2022

Challenges of digital privacy in banking organizations

Okechukwu Innocent Ogudebe
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Okechukwu Innocent Ogudebe

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Gary Griffith, Committee Chairperson, Information Technology Faculty
Dr. Habib Khan, Committee Member, Information Technology Faculty
Dr. Alan Dawson, University Reviewer, Information Technology Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2022

Abstract

Challenges of Digital Privacy in Banking Organizations

by

Okechukwu Innocent Ogudebe

MS, University of Maryland University College, 2019

MS, University of Maryland University College, 2018

BS, University of Maryland University College, 2015

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

2022

Abstract

As the information and technology age becomes more advanced, digital privacy flaws have become more challenging. Information technology (IT) security managers, chief information security officers, and other stakeholders in banks are concerned with identity-based authentication attacks because identity-theft attacks cause data breaches. Grounded in the protection motivation theory, the purpose of this qualitative pragmatic study was to examine strategies IT security professionals working on internet banking platforms use to mitigate identity-based authentication attacks. The study participants comprised five IT security professionals currently working in the online banking industry from the northeastern United States with at least 5 years of experience handling digital banking platforms. Data were collected from interviews with five IT security professionals and publicly accessible documents such as NIST documents and industry standards. Data were analyzed using thematic analysis. Five major themes emerged from the analysis: comprehensive user authentication, importance of data encryption, system audits, intrusion detection systems, and comprehensive user policies. A key recommendation is to train all users on secure usage of the bank’s digital transaction platform by providing mandatory privacy protection training and security awareness to users before they successfully create or access financial accounts. The implications for positive social change include the potential to increase the number of users to effectively use cybersecurity policies, techniques, tools, and training designed to protect their online banking accounts from identity-based authentication attacks.

Challenges of Digital Privacy in Banking Organizations

by

Okechukwu Innocent Ogudebe

MS, University of Maryland University College, 2019

MS, University of Maryland University College, 2018

BS, University of Maryland University College, 2015

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

2022

Dedication

I dedicate this doctoral research study to the Almighty God, who gave me the vision, direction, and strength to conduct it. I thank and dedicate this research study to my late grandmother Chinyere Lucy Ogudebe for her sacrifices in raising me to ensure I have a good education. She encouraged and motivated me to further my studies, and without her, I would not be the person I am today. Grandma, I want you to know that no day passes without me thinking about you since you passed away. You will always remain a reference in my eyes due to your hard work, dedicated role, modesty, and kindness. I acknowledge you, grandma, for striving to show me the spirit of hardwork, honesty, and self-effacement in every aspect of my life. I also thank and dedicate this doctoral research study to my mum Bernice Obiageli Ogudebe and my aunt Izukanne Nnubia for their help in raising me.

Acknowledgments

First, I thank my committee chair, Dr. Gary Griffith, for his fantastic mentorship, guidance, and prompt constructive feedback throughout the demanding lengthy process of writing this research study. Dr. Gary Griffith, your great guidance and support toward my research study strongly motivated me to do the right research in all my study phases. Second, I thank Dr. Habib Khan, Dr. Gail Miles, Dr. Alan Dawson, and Dr. Rose Gold for their great support during my research study. Third, I thank all the participants in this research for their time and input that made this research study a success. Finally, I thank my family, friends, and colleagues for their kind encouragements, especially during the difficult moments when this research study seemed unattainable.

Table of Contents

List of Tables v

Section 1: Foundation of the Study 1

Background of the Problem 1

Problem Statement 2

Purpose Statement 2

Nature of the Study 3

Research Question 5

Interview Questions 5

Conceptual Framework 6

Definition of Terms 7

Assumptions, Limitations, and Delimitations 9

Assumptions 9

Limitations 10

Delimitations 11

Significance of the Study 11

Contribution to Information Technology Practice 12

Implications for Social Change 12

A Review of the Professional and Academic Literature 13

Protection Motivation Theory 14

Protection Motivation Theory with Other Theories 18

Key Assumptions of PMT 20

Protection Motivation Theory in Identity-based Attacks 21

Protection Motivation Theory in Digital Privacy 24

Inconsistencies with The Protection Motivation Theory 26

Supporting Theories 28

The Theory of Planned Behavior (TPB) 29

Theory of Reasoned Action (TRA) 30

Unified Theory of Acceptance and Use of Technology (UTAUT) 32

Digital Privacy and Digital Banking 36

Transition and Summary 44

Section 2: The Project 46

Purpose Statement 46

Role of the Researcher 47

Participants 49

Research Method and Design 51

Research Method 51

Research Design 53

Population and Sampling 55

Ethical Research 58

Data Collection 60

Instruments 60

Data Collection Technique 64

Data Organization Techniques 66

Data Analysis Technique 68
Reliability and Validity 70
Introduction 70
Reliability 70
Validity 71
Dependability 72
Credibility 72
Transferability 73
Confirmability 74
Transition and Summary 74
Section 3: Application to Professional Practice and Implications for Change 76
Overview of Study 76
Presentation of the Findings 76
Theme 1: Comprehensive User Authentication 79
Theme 2: Importance of Data Encryption 98
Theme 3: System Audits 105
Theme 4: Intrusion Detection systems 114
Theme 5: Comprehensive User Policies 117
Applications to Professional Practice 126
Implications for Social Change 128
Recommendations for Action 132
Recommendations for Further Study 136

Reflections 136

Summary and Study Conclusions 138

References 138

Appendix A: Interview Protocol 173

Appendix B: Interview Consent Form 176

List of Tables

Table 1. Major Themes Emerging From the Data Collection 78

Table 2. Subthemes Under Comprehensive User Authentication 80

Table 3. The Application of Information System Security Procedures and Policies in User Authentication 81

Table 4. Interview Participants Who Have Implemented NIST Frameworks to Protect Their Online Banking Platforms 81

Table 5. Interview Participants Who Have Implemented NIST Frameworks on the Use of OTP 83

Table 6. Subthemes Under the Importance of Data Encryption 99

Table 7. The Application of Encryption Procedures in Digital Banking........................ 100

Table 8. Interview Participants Who Have Implemented NIST Frameworks to Protect Their Online Banking Platforms 100

Table 9. Subthemes Under the Importance of Carrying Out System Audits.................. 108

Table 10. The Application of System Audits in Digital Banking.................................. 107

Table 11 108

Table 12. Subthemes Under the Importance of Comprehensive User Policies 117

Table 13. The Application of Comprehensive User Policies in Digital Banking........... 118

Table 14 119

Section 1: Foundation of the Study

Background of the Problem

The evolution of digital banking has come a long way since the days when transactions could only be conducted in brick-and-mortar financial centers. Today, customers can virtually access all banking services over the internet. Online banking encompasses all electronic payment systems that enable users to carry out internet-enabled financial transactions (Oertzen & Odekerken-Schröder, 2019). Online banking offers users round-the-clock access to financial services, enhanced transaction processing speed, and reduced transaction fees. It is estimated that the integration of digital banking services results in a 20% reduction in a bank's operating costs (Ananda et al., 2020).

Online banking's popularity has contributed to an increase in fraud, which has contributed to substantial financial losses recorded globally (Carminati et al., 2018). Fraudulent attacks against digital payment platforms are perpetrated through cyberattacks, malware injection, phishing scams, and identity-based authentication attacks. As consumers continue to demand increased support for digital freedom, identity theft cases have continued to rise. Identity-based authentication attacks may be categorized into two distinct groups: identity theft and identity fraud (Gies et al., 2020). The two crimes involve compromising an individual's right to digital privacy to facilitate financial fraud. The most common identity verification techniques used by online banking platforms consist of user credentials such as login ID and password (Sinigaglia et al., 2020). However, these tools are considered ineffective at fool proofing digital banking platforms against identity-based authentication attacks.

Problem Statement

As the information and technology age becomes more advanced, major flaws affecting digital privacy have become tougher to deal with (Akanfe et al., 2020). A crime-based survey found that 46.5% of the identity-based crimes reported to financial organizations targeted high income earners (Green et al., 2020); between $1.5 trillion and $2.8 trillion was lost worldwide by financial institutions because of identity-based crime (Raza et al., 2020). The general information technology (IT) problem is that identity-based authentication attacks threaten the integrity of digital privacy on digital payment systems. The specific IT problem is that some IT security professionals working on internet banking platforms lack strategies to mitigate identity-based authentication attacks affecting digital privacy in online banking.

Purpose Statement

The purpose of this qualitative pragmatic study was to examine the strategies IT security professionals working on internet banking platforms use to mitigate identity-based authentication attacks affecting digital privacy in online banking. The target population for this qualitative pragmatic study was IT security professionals working in online banking industry in the northeastern region of the United States. The results of this study may contribute to a positive social change by offering techniques to protect bank customers and employees' digital payment systems from identity-based authentication attacks and threats. In addition, the findings from this research may be used to guide IT security professionals in other organizations with appropriate digital privacy strategies to proactively prevent identity-based authentication attacks for online users' security.

Nature of the Study

I chose a qualitative method to examine my research topic. Using the qualitative methodology, investigators can explore their topic of interest using a naturalistic approach and build an in-depth understanding of the social problem (Hamilton & Finley, 2019). The qualitative methodology is generally an ideal investigation tool for researchers seeking to examine, describe, and explain a problem using non-quantifiable data collection techniques or sources. Since the primary data collection technique is mostly conversational, qualitative researchers can gain first-hand data regarding identity theft and digital banking (Lo et al., 2020). Conversely, a quantitative method is used to provide valid points through comparative analysis (Huarng et al., 2018). Quantitative method approach lets researchers use statistics to measure an individual's experience; the quantitative method tests relationships between variables by collecting and analyzing numerical data (Lo et al., 2020). In this study, I did not collect statistical data, as it was not appropriate for this study; hence, I did not use the quantitative method. Statistical data only portrays a study's findings using a single perspective. In the mixed-method, an investigator is required to incorporate both quantitative and qualitative methodologies within one study (Ivankova & Wingo, 2018). Because I did not study the relationship between variables and test hypotheses, mixed method was inappropriate for my study. Since I needed a deeper understanding of the research study participants' views, quantitative and mixed methods were not suitable for my study.

I chose the qualitative pragmatic study design to analyze the complexities caused by identity-based authentication attacks on digital banking platforms and their impact on the user's privacy. The pragmatic research design is use in answering scientific questions using existing evidence and how the solutions can accelerate impact on the general population's equity (Holtrop & Glasgow, 2020). The pragmatic research approach is valuable to information system (IS) researchers exploring a field that has not received enough attention by other researchers (Ramanadhan et al., 2021). Moreover, a pragmatic approach also addresses IS-specific questions with rigor and breadth by processing the influencing factors (Auernhammer, 2020; Teece et al., 2021). The multiple-case studies are empirical inquiry tools used to explore concepts, ideas, and problems within their real-life context using an explicit framework (Gallagher, 2019). Case studies are used to investigate scientific problems with lingering uncertainties. The multi-case study design has provided researchers with groundbreaking insights towards investigations requiring extensive analysis (Hoorani et al., 2019). I did not choose the multiple-case study approach due to its subjective real-life analytical method. The phenomenological approach explores using people's lived experiences on a phenomenon (Hamilton & Finley, 2019). The phenomenological design attempts to view the problem from the participant's view (Hamilton & Finley, 2019). I did not choose the phenomenological research design as I did not intend to focus on understanding the meaning of the participants' lived experience. In this study, my interest was not to understand the IT security professionals' lived experiences; therefore, the phenomenological design was not an ideal investigation approach. An ethnographic approach is designed to describe a phenomenon from a cultural point of view (Vasilev et al., 2018). However, digital privacy strategies and policies are designed to protect society. In ethnography, researchers use a cultural lens to study the social organization of a group of people. I did not use ethnographic design because the study would not engage in group culture observations; therefore, ethnographic design was not suitable for my study. Consequently, the qualitative pragmatic approach was best suited for my research topic. Since my goal was to investigate strategies used to mitigate identity-based authentication attacks on digital banking platforms, a qualitative methodology was appropriate for this study.

Research Question

What strategies do IT security professionals use to mitigate identity-based authentication attacks affecting digital privacy in online banking?

Interview Questions

1. What strategies have you implemented to support digital privacy?
2. What strategies have you implemented to ensure users comply with digital privacy rules when registering or using online payment platforms?
3. What strategies do you use against data breaches?
4. What procedures have you used to conduct internal compliance audit to protect users' privacy?
5. How do you deal with identity-based authentication attacks?
6. What is involved in following up identity-theft cases on your network?
7. What type of information is typically lost in identity-based authentication attacks?

8. What policies are in place to improve the information security awareness by end-users?
9. What procedures are involved in resolving identity-based authentication attacks cases?
10. How would you describe your proficiency in handling identity-based authentication attacks on your network?
11. How often do you update digital privacy policies?
12. What type of mitigation techniques have you integrated into your protection strategies against identity-based authentication attacks?

Conceptual Framework

I used Rogers's (1975) protection motivation theory (PMT) to investigate how fear-based security policies elicit unconditioned avoidance behavior in individuals. PMT was originally created in 1975 by Ronald Rogers and conceptualized the implementation of fear-arousing stimuli to initiate protective responses by individuals (Rogers, 1975). The philosophy behind the PMT model was modified to include external stimulus; response efficacy; self-efficacy; and social influence as fear appeal components (Johnston & Warkentin, 2010). Nonetheless, the PMT approach may be used to enhance the efficacy of information security policies in the context of data breach (Giwah et al., 2019). Additional features of the PMT methodology may be used to motivate users to share knowledge and solutions within cyberspace (Wu, 2019).

Rogers' (1975) PMT may be applied as the foundation for my examination of the strategies used to mitigate identity-based authentication attacks affecting digital privacy in online banking. The modified PMT theory may be applied in the formulation of security policies to prompt response efficacy to threats (Johnston & Warkentin, 2010). By integrating Wu's (2019) PMT framework, it may improve knowledge sharing on identity-based authentication attacks. In this study, IT security professionals working on internet banking platforms may create strategies to mitigate identity-based authentication attacks. By applying the PMT approach, user compliance may increase to practical information security policies (Giwah et al., 2019). The theories will help design persuasive messages from the perspective of IT security professionals by indicating the dangers of identity-based authentication attacks on online banking platforms.

Definition of Terms

Cybercrime: Refers to the use of computers and other digital devices to carry out illicit activities or potentially harm other individuals (Donalds & Osei-Bryson, 2019). Cybercrimes are considered global offenses as they transcend geographical boundaries and may be perpetuated through technology. It is a holistic view of computer-related crimes.

Cybersecurity: Encompasses a broad range of governance and protective measures designed to enhance the security of network communication (Veale & Brown, 2020). It covers technically focused data security protocols designed to prevent accidental and deliberate misuse of digital tools.

Digital banking: Refers to the provision of financial services via the internet. It is a service-oriented architecture that enables banks to offer traditional services using online mechanisms such as web platforms and mobile applications (Megargel &

Shankarararman, 2020). It is the use of digital channels to facilitate economic transactions (Son et al., 2019). Digital banking promotes efficient personal banking services accessibility compared to self-service channels such as ATMs. Digital banking is reshaping the world of banking. The term may be used interchangeably with online banking.

Digital privacy: Advocates for the protection of an individual's privacy rights while using electronic systems. In essence, it refers to the protection of personal information for individuals using networked computing devices (Elueze & Quan-Haase, 2018). Online privacy is acknowledged as a basic human necessity and phenomenon. Privacy breaches arise from cyberattacks, cybercrime, and compromise of digital media.

Identity-based authentication attacks: Refers to attacks seeking to compromise user authentication services used to identify an individual (Kumar et al., 2020). Identity-based authentication security uses personal identifiers such as username, password, fingerprint, or facial recognition to offer a secure and reliable user account verification. Identity-based authentication attacks attempt to compromise current user verification on computer systems and other electronic devices (Cui et al., 2018). These attacks impact user identification, tracking, and privacy control. Examples of such attacks are password guessing, spoofing, eavesdropping attacks, insider attacks, and masquerading attacks.

Identity theft: A form of cybercrime that happens when a person impersonates another and uses their information to commit fraud. It happens when an adversary gains access to electronic records and uses them to conduct a wide range of crimes (Piquero et al., 2021). It involves the deception and illegal access of IT services for economic gain.

The crime occurs when an adversary steals your login credentials, social security number, credit card details, bank account records, or any other personal identifiers to gain access into a victim’s online banking platform (Vučković et al., 2018). It may effect a negative psychological and economic impact for the victim.

Information technology (IT): The use of computing devices, physical devices, or infrastructure to process, create, store, exchange, or secure electronic data (Khuntia et al., 2018). It also refers to the development, use, and preservation of digital systems, networks, and software in the exploration and exploitation of data (Benitez et al., 2018). In the business context, IT offers a platform for consumers to share knowledge and solve business problems.

User authentication: Computing devices and systems employ user authentication techniques to identify and validate a user (Solovyev, 2020). User authentication prevents illegal access to computing resources and attempts to harden network resources. Authentication strategies predominantly employ access control tools to limit illegal access of resources and maintain system security.

Assumptions, Limitations, and Delimitations

Assumptions

An assumption is a proposition that scholars believe to be the true without evidence (Ertefaie et al., 2018). It may also be a premise that a researcher believes to be valid, an unmeasured belief. There are various aspects of this study I assumed to be true. One assumption is that a population comprising of IT security professionals would contribute in reliable and high-quality data regarding banking data security practices. I assumed that there would be no issues accessing contact information of the participants. In addition, I assumed IT security professionals from social media platforms such as LinkedIn in the northeastern region of the United States would agree to participate in my study. The second assumption was that the interviewees would offer their honest feedback during the semi-structured interview session.

Limitations

Every study encounters various hurdles that may be beyond the researcher's control and they may influence its findings. Typical shortcomings of a study include flawed methodology, unavailability of resources, and insufficient sample population (Greener, 2018). Flaws within a study prevent a scholar from truly addressing the topic under investigation. Chang et al. (2020) argued IT research may sustain several limitations. First, the IT policies around a technology may affect the quality of data obtained. Secondly, rapidly changing technology and innovation pose risks to information security. Identity-based authentication attacks and cyberattack models evolve within a relatively short time. A technique used 2 years ago may be outdated and offer invaluable information to my study. There are various limitations that I encountered as I progressed with my study. The main limitation was confined to the geographical region I collected my study's data. Since the participants were from the same region, their input may not mirror data from the general population. The National Institution for Standards and Technology (NIST) guidelines for information security may be prohibitive in analyzing data security standards in banking organizations (Rose, 2019). NIST guidelines provide a comprehensive overview of security and privacy protocols designed to protect the end-user. The organization implements new changes to its information security regulations to protect its users.

Delimitations

Study delimitations encompass the decisions made by the scholar to define boundaries. They include factors and variables that are not to be included in the study as they limit the scope (Bergström et al., 2019). In essence, delimitations describe the boundaries of a study and outlined for practical reasons such as lack of time or limited finances. The limiting factors of this study included (a) legally accessing bank records highlighting cases of identity-based authentication attacks (b) interviewing IT security professionals with at least 5 years of experience (c) the implementation of cybersecurity protocols to counter identity-based authentication attacks, and (d) selecting participants that support digital banking platforms. Moreover, IT security professionals are not the only technical specialists responsible for banking IT systems.

Significance of the Study

The purpose of this study was to examine the strategies IT security professionals working on internet banking platforms use to mitigate identity-based authentication attacks affecting digital privacy in online banking.. The research findings could assist IT security professionals and IT directors protect digital banking platforms from identity-based authentication attacks. To IT organizations, the study could provide insight on ways they can appropriately mitigate identity-based authentication attacks affecting digital privacy in online banking platforms. This study could aid chief information security officers (CISOs) and chief information officers (CIOs) develop better digital privacy strategies integral at deterring identity-based authentication attacks. The mitigation strategies proposed by this study may assist IT practitioners in other organizations, both in and out of academia, remodel, replicate, and implement effective digital privacy environments that secure users and organizational data from identity-based authentication attacks. The identified mitigation strategies may be instrumental in reducing instances of identity-based authentication attacks targeting digital platforms, individuals, financial institutions, and local economies.

Contribution to Information Technology Practice

This study may help IT professionals in early detection, reduction, and prevention of identity-based authentication attacks on online banking. Aboobucker and Bao (2018) observed that internet banking services are prone to identity-based authentication attacks due to the financial incentive behind a successful system exploit. Consequently, cybercriminals target E-banking platforms and banking databases due to their wealth of information (Kiljan et al., 2018). Putting in place cybersecurity strategies to address digital privacy based on the results of this study may compel IT security professionals to effectively design, establish, and improve the existing digital privacy strategies and deter identity-based authentication attacks. In addition, the results may be used to properly ensure IT security professionals catalog each security incident experienced by the banks and enhance digital privacy on online banking platforms.

Implications for Social Change

The results of this study may contribute to a positive social change through the effective development of cybersecurity policies designed to protect online-banking users from identity-based authentication attacks. The results of this study may prove to be effective to individuals looking to protect themselves from identity-based authentication attacks. The results of this study may mitigate banking fraud exploits targeting the elders, illiterates, people with disabilities, and youths from identity theft, thus protecting their privacy. The findings of this study may contribute to a positive social change in the proper use of security tools and technology by bank employees. Employee behavior plays a great role in the failure of a security chain of a system (Syniavska et al., 2019). For instance, a bank employee may share their system authentication credentials with third parties and inadvertently compromise the bank's IS. Bank employees and employees in other organizations may use the study's recommended techniques to effectively manage and update their passwords. With technology rapidly evolving, the bank's employees need to incorporate complex password management.

A Review of the Professional and Academic Literature

Using Ulrichsweb and Walden University Thoreau database search tools, I carried out searches to locate related articles published by other scholars and researchers highlighting the strategies used to mitigate identity-based authentication attacks affecting digital privacy in online banking. To further locate factual results related to the research topic under investigation, I used the following phrases in my search string: *identity theft, digital privacy, online baking platforms, identity-based attacks, and protection motivation theory (PMT) online banking.* To keep my study's findings up-to-date, I used articles not older than five years ago, and the articles must have been peer-reviewed. The IT industry is fast evolving, which means older research material tends to lose its relevance within a short period. In essence, practices within IT and cybersecurity change very fast. Consequently, I had to ensure that I locate current relevant articles to exhaustively explore my research topic. My initial search only yielded 70 peer-reviewed articles. I also identified extra journals by reviewing other academic databases and search engines. The online libraries included Google Scholar, Proquest, EBSCO, IEEE, and Inspec. I used the study's research question as a query, which was instrumental in locating more articles. In total, I gathered 100 different journals for the literature review, 96% of the articles are peer-reviewed. The analysis of the literature review section is driven to find appropriate answers based on my research topic. The literature review is broken down into several sections designed to conclusively discuss identity theft, online banking platforms, digital privacy, cybersecurity, data governance, and protection motivation theory. The literature review section will offer a full explanation of the privacy motivation theory (PMT), its evolution, and compare it to other theories in regard to digital privacy in online banking platforms.

Protection Motivation Theory

Rogers introduced the protection motivation theory (PMT) in 1975 to demonstrate how fear appeals may be used as a stimulus to mediate attitude change in an individual. His proposition offered an explanation on the use of fear-arousing stimuli to alter response patterns and produce aversive actions. Rogers (1975) expected the adoption of PMT to diversify over time and his assertions have lived up to his expectations. The responsibility of persuasive communication is based on "true" and "just" information delivery (Wieder, 2019). Rogers' (1975) pointed out that three key variables of fear appeal were integral in designing a persuasive messaging model: the intensity of noxiousness of an outlined event, the likelihood of that event occurring, and the effectiveness of the proposed preventative action. Earlier analyses of the fear arousal demonstrated that several packages were needed to adopt the communicator's message to evoke preventative action.

Fear appeal is a multifaceted stimulus and a major component of persuasive communication. For years, scholars and IT security professionals have illustrated that human behavior is a major impediment to the security chain (van Bavel et al., 2019). Using Rogers proposed fear-based security stimuli, the efficacy of a security chain may be enhanced through protective response. Historically, fear has been conceptualized as stimuli trigger against danger. Intake input assists an individual to decide the course of action to follow. Conditional responses may be achieved by subjecting an individual to associative emotional responses (Boddez et al., 2020). Several meta-analyses have demonstrated that the perception of danger triggers a high response rate amongst a population. Fear a psychological reaction triggered by noxious events (Luchkina & Bolshakov, 2018). It triggers the basic survival mechanism forcing an individual to respond to a causative agent. However, the effects of fear are not maintained in the long run and are usually disregarded after the organism has successfully evaded the fear trigger. In addition, Rogers characterizes fear as an intervening variable against adverse conditions forcing an organism to keep away from a noxious event.

The decision on whether an individual engages in protective behavior is governed by two distinct cognitive processes, which are threat appraisal and coping appraisal (Kim et al., 2021). In psychology, individuals address threat appraisal factors first. Threat appraisal assesses maladaptive behavior to determine if the individual is in immediate danger. Maladaptive behavior includes physical inactivity, substance abuse, overeating, and self-harm (Snider et al., 2019). In threat appraisal, the individual looks at extrinsic and intrinsic rewards to determine the course of action they take. Essentially, rewards may contribute to the enhancement of maladaptive behavior, whereas consequences may reduce maladaptive behavior (Gazendam et al., 2020). The coping appraisal is addressed later by an individual as its effect is not immediate. It is an assessment of adaptive behaviors, which can be characterized by rules, healthy eating, and cleaning. Coping appraisal compares response efficiency and the associated decision cost when interpreting a decision (Wall & Warkentin, 2019). In essence, an individual holds the belief that a coping action will purge the threat. The two meta-analyses of the traditional PMT cognitive processes are largely used in the health domain.

The perception of a high severity and vulnerability act as a trigger making an individual engage in risk-preventative behavior. The perceived threat attribute makes up the core elements of PMT (Rogers, 1975). For individuals to undertake preventative actions, a positive evaluation of the threat has to be determined. In essence, individuals are likely to take adaptive actions when coping appraisal conditions are met. Boddez et al. (2020) stated that fear-based rewards, whether intrinsic or extrinsic, are believed to be essential in an individual's thought process. The effects of the two appraisal processes make people consider the negative consequences (severity cost) before taking an appropriate course of action.

Johnston and Warkentin (2010) in their study evaluated the relationship between fear appeals and persuasive messaging in the context of information security behavior. Persuasive messaging includes an element of fear to facilitate action. While every message is encouraged to include all the elements of ethos, pathos, logos, and clear storytelling, a persuasive message is discussed in terms of reason versus emotion (Wieder, 2019). Dupuis and Renaud (2020) warned that fear appeals may overlook certain ethical concerns making the approach inappropriate in message passing. The authors also note that there are varying opinions on the use of fear appeals in security messages. Schuetz et al. (2020) stated that fear appeals have emerged as a key tool for improving information security over the past few years. The use of persuasive messaging has promoted health-protective behaviors against diseases caused by lifestyle choices such as AIDs and lung cancer (Hurst & Stern, 2020). Due to its effectiveness in health-related threat messaging, scholars are exploring ways to integrate fear appeals into the IT sector. Persuasive arguments can be used to modify a person's attitude, intentions, and behaviors (Johnston & Warkentin, 2010). Attitude changes triggered may be permanent or temporary depending on the circumstances.

There is good evidence that PMT strategies are generally effective at initiating behavioral change (Johnston & Warkentin, 2010). However, the efficacy of positive emotional appeals, such as humor, is still not clear (Zhao et al., 2019). Moreover, the integration of targeted emotional appeals may have not received the appropriate attention in prevention research. One explanation for the mixed attention of emotional appeal messaging is the subtle difference in user context of the research. In their research, some scholars apply fear appeals to personal messages while other target corporate users (Schuetz et al., 2020). Various explanations have investigated the extent to which a message may be used to generate fear and alter behavior. Johnston and Warkentin (2010) determined that an individual's behavioral intention is influenced by three crucial factors, namely, self-efficacy, response-efficacy, and social influence. The pair conceptualized the fear-appeal model (FAM) and used it to find factors determinant to behavioral change in PMT. They found out that social influence had a determinant role in aiding behavioral intent. The FAM model studied the threat effects of various end-users and the functionality of privacy within a decentralized IT environment. The mutual collaboration of response efficacy and social influence has translated to safer behavior.

Protection Motivation Theory With Other Theories

PMT is a flexible framework and has been used in conjunction with other theories to explore varying topics. Scholars may augment components of PMT and other theories to explain behavioral biases exhibited by a population (Jansen & van Schaik, 2019). The PMT relies on the principle of fear-appraisal in decision-making. Its usage has expanded and may be used to inform studies on self-protective strategies towards a perceived threat. To fill research gaps, investigators compare a study's knowledge using different conceptual models to monitor user behavior from different perspectives (Wu, 2019). Zhang et al. (2019) used the theory of planned behavior (TPB) and PMT in a complementary manner to investigate and validate their study on mobile health service adoption in China. TPB has been extensively used to predict the behavior of individuals in various information system studies (Johnston & Warkentin, 2010). TPB and PMT may be used to complement each other in developing different perspectives in qualitative research. Pang et al. (2021) sought to investigate the influence of purchase intentions amongst consumers as a result of the adoption of organic food in Malaysia. The team also applied the TPB and PMT in investigating the structural relationships within consumer purchase intentions (Pang et al., 2021). The conceptual models helped determine which perceived factors greatly impact consumer decisions. Wu (2019) in his study implemented the PMT and theory of reasoned action (TRA) to investigate information non-sharing behavior within the digital environment. Information sharing has been a fundamental pillar of the internet. However, as internet adversaries rise, there is a growing attitude towards information withholding. The two theories were used to investigate ways information withholding behavior may be reduced in cyberspace.

Chen et al. (2019) applied the PMT and construal level theory (CLT) to analyze the tourist's behaviors towards environmental mitigation methodologies. The researchers examined the relationship between environmental knowledge and behavioral intentions in regard to climate change. Findings from the study would be integral in developing better climate change mitigation behaviors in tourists. Factors such as threat appraisal and coping appraisal are essential at informing the study's actions. Furthermore, Srivastava et al. (2021) investigated the impact of COVID-19 on the adoption of contactless payment platforms. Threat conditioning caused by COVID-19 has forced people to avoid physical contact and inculcate social distancing practices. The researchers integrated PMT and unified theory of acceptance and use of technology (UTAUT) to investigate how people have become accustomed to contactless payment models. The COVID-19 pandemic has truly transformed the consumer perspective on digital transactions on payment. The disease acts as a fear agent motivating users to adopt contactless transaction modes. While PMT concepts may be applied to other studies and complement other research theories to investigate topics, this study will only use PMT to evaluate the research question. PMT was used to identify the security strategies used by IT security professionals in mitigating the impact of identity-based authentication attacks on digital transaction platforms.

Key Assumptions of PMT

PMT assumes its concepts may be applied to any scenario involving the use of fear as a prerequisite for behavioral change (Vedadi & Warkentin, 2018). The model was first developed for health-related messages, but was later integrated into the Information technology field, finance field, and social studies. Scholars integrating PMT methodologies into their studies assume that an individual will experience the minimum level of threat and concern about the causative agent. Secondly, the PMT model assumes that an individual will feel motivated to minimize the impact of the potential risk. According to Rogers (1975), fear appeals attempt to exert attitude change in an individual by arousing the protective stimuli through cognitive appraisal. Psychologists apply the conceptual theory to enable purposive behaviorism in an individual.

There are six associative conditions that an individual takes into account to elicit the subsequent behavior and reason to protect oneself. Essentially, one must believe that the threat is severe; they are unprotected against the threat; there are protective measures one can implement; one must be capable of performing evasive procedures; there are rewards associated with evasive procedures; and there are costs associated with the protective behavior (Jansen & van Schaik, 2019). The conceptual model usually refers to coping mechanisms associated with cognitive measures. Evasive responses may also be affected by one's emotional state.

Consequently, prior interactions with a threat may minimize an individual's fear appeal. PMT predominantly assumes the subject has not faced the threat before (Good & Hyman, 2020). For instance, if a system user has been attacked by a computer virus, their fear of computer viruses may be diminished. Therefore, future persuasive messages targeting such individuals may not induce the required responses. Fear-appeal manipulation may also result in static responses. In Information systems (IS) security, static responses may not be quite effective at safeguarding an individual's identity. For example, a persuasive security message may result in short-term evasive exercises. PMT assumes that an individual's fear-response will result in long-term behavioral changes. The conceptual model assumes the individual will complete a rational decision-making process. Humans are prone to cognitive bias when subjected to threats (Daniel et al., 2020). Anxious individuals may interpret fear-appeals as socially threatening to result in inaccurate decisions. Instances of cognitive bias may reinforce maladaptive behaviors.

Protection Motivation Theory in Identity-Based Attacks

Today, researchers such as Rahi et al. (2018) are keen on integrating the PMT framework to explore topics based on Information Technology and Cybersecurity. As of consequence, PMT has become one of the most applied theories used to explore IS behavioral studies (Srivastava et al., 2021). PMT offers scholars important insights into

IS breaches and cybersecurity attacks. The psychology behind the fear-appeal model offers organizations a better perspective into identity-based authentication attacks, which can be used to design effective intervention techniques. To gain a better understanding of the cognitive processes involved in cyber-attacks, researchers use the framework to make well-informed decisions. Internet users are considered the weakest link in the effective implementation of cybersecurity methodologies (De Kimpe et al., 2021). Identity-theft attackers use simple attack vectors to compromise systems. For instance, phishing attacks directly target individuals by circumventing measures used to offer user authentication (Blackwood-Brown et al., 2019). Email users are highly susceptible to phishing attacks and therefore need a better understanding of protective measures (Meske et al., 2019). Maladaptive user behavior plays a great role in exposing individuals to phishing attacks. To reduce instances of maladaptive user behavior on cybersecurity, PMT interventions may assist educators to inform the public about IS security behavior.

According to Johnston and Warkentin (2010) cases of security incidents, such as system infiltration, insider system abuse, and other forms of unverified system access continue to increase in magnitude and sophistication. Interestingly, organizations tend to maintain a low profile when hit with such attacks. Technology specialists have indicated that the end-users play a crucial role in winning the war against cyberattacks (Wang et al., 2019). IT security professionals, to a degree, align system infiltration with the end-users. Identity theft primarily exploits an individual’s behavior. For example, people often dump their old documents into dumpsters without shredding them. By simply dumpster diving into an academic institution’s garbage bin, a perpetrator may end up collecting hundreds of intact documents with vital student information. Identity theft, unlike other crimes, is not immediately evident to the victim (Ylang, 2020). It is a difficult form of theft as the victim only detects its impact much later. Identity theft tarnishes the victim's reputation and leads to financial loss. The reliance on a routine activity timeline greatly exposes an individual to identity-theft perpetrators. The concepts of PMT are designed to assist individuals to break away from routines. PMT instead encourages individuals to adopt a protective behavior when one is sharing or dumping their personal information.

Li et al. (2019) integrated PMT's threat appraisal and coping appraisal concepts to scrutinize an individual's awareness of their cybersecurity behavior. The scholar's goal was to analyze how modern system attacks take advantage of employee complacency to exploit networks. The study's findings were essential at mitigating computer networks against attacks. They hypothesized that insider threats caused by employees posed a great danger to an organization's corporate networks. As the use of the internet continues to increase in volume and complexity so have cyberattacks. However, organizations continue to stick to archaic data practices, which expose an organization's valuable data to adversaries. Using the PMT methodology, Hooper and Blunt (2019) aimed to develop new perspectives into cybersecurity by defining the domains of employee system security behavior. The PMT conceptual model was used to develop security behavioral constructs and create awareness. They found that peer behavior was to blame for employee organizational security laxity. Furthermore, the researchers complemented their study Health Belief Model (HBM). The model was used to investigate preventative behavior amongst employees and cybersecurity procedures. The PMT theory best captures individual behavior and best illuminate's cybersecurity principles.

Protection Motivation Theory in Digital Privacy

As society transitions into the new digital age, new concerns have emerged about the future of the internet ecosystem. The banking sector has recorded phenomenal growth in the usage of computer networks. In the modern marketplace, private data is regarded as the ultimate resource by website operators (Bornschein et al., 2020). Consequently, website operators have implemented invasive data collection tools on their platforms. Increased interconnectivity has introduced risks regarding privacy risks and data misuse risks. PMT was integrated into digital privacy studies to enhance digital privacy. Akanfe et al. (2020) conducted a privacy-risk study for digital payment systems. The scholars based their research on the country-level markers. Various factors were affecting consumer confidence in digital privacy. They found out that country-level risks greatly affected cross-border consumerism. The threat posed by a specific country's data laws often makes consumers avoid taking part in cross-border consumerism. Akanfe et al. (2020) identified factors such as political climate, credit rating, financial security, cyberattack prevalence, and protection practices that were used as risk indicators by consumers. Bornschein et al. (2020) also carried out a study assessing consumer outlook on information privacy practices. Online business entities rely on private data to enhance the consumer experience. This factor has forced organizations to adopt invasive monitoring techniques on their clients, namely, cookies, web scripts, and offline tracking apps. However, governments across the globe have been keen on protecting their citizens from digital exploitation. Various regulations have been put in place to discourage website operators from illegally tracking their users (Bornschein et al., 2020). Consumer monitoring practices may be viewed as threats using PMT in the context of digital privacy. Essentially, governments and policymakers viewed consumer tracking as a threat that needed to be quickly addressed.

Policymakers were also concerned about the extreme behavioral changes that individuals would exhibit as a result of privacy invasion. Zhang et al. (2019) carried out a study analyzing the negative influence of data sharing practices implemented by medical health services (MHS) in China. To optimize medical service provision in China, a selected number of medical centers implemented mobile health digital networks to facilitate information sharing. However, patients utilizing the services of the select centers were reluctant about information-sharing practices adopted by the hospitals. According to the study, the integration of MHS resulted in the risk of privacy invasion. Using PMT, Zhang et al. (2019) investigated the relationship between user-perceived behavior and the loss of privacy as a result of the privacy invasion. They found out that patients were worried about having their digital details shared by multiple medical institutions. Fear-appraisal triggered the loss of privacy considerably affected the patients. The researchers also noted the patient’s behavioral intentions also led to health status deterioration. They hypothesized the health status may be negatively affected by the relationship patients exhibit towards MHS.

Wu (2019) conducted a study seeking to determine why users were withholding their knowledge while interacting on digital platforms. According to the study, cases of counterproductive knowledge behaviors have been on the rise recently. However, the internet was initially created to facilitate information sharing (De Matos et al., 2020). The premise of increased interconnectivity is to enhance knowledge sharing amongst individuals. The conceptual study blames the rise of digital privacy policies for the decline of knowledge sharing practices. Secondly, factors such as fear, emotion, time pressure, distrust, relationship conflicts, and social identity are contributing to the reduction of data sharing (Kiljan et al., 2018). Moreover, the dark aspects of digital privacy are affecting information sharing (Mani & Chouk, 2019). These aspects include cyberbullying, knowledge infringement and privacy violations are increasing user fear severity on digital platforms. In regard to cyberbullying, knowledge hiding behavior was attributed to six fear variables: losing power, isolation, losing face, exploitation, contamination, and opportunism. Digital privacy threats continue to affect knowledge-sharing behavior (Wu, 2019). Using PMT, individuals may be educated on the dangers presented by the internet and therefore enhance their trust in digital privacy methodologies. Historically fear has been used to condition individuals. Fear attributed to the invasion of digital privacy may be used to enhance an individual's perception of the practice (Vedadi & Warkentin, 2018).

Inconsistencies With The Protection Motivation Theory

Some scholars have expressed their dissatisfaction with PMT as an investigation tool (Srivastava et al., 2021). First, PMT persuasion messages do not adhere to guidelines of effective communication. In communication, the messenger should adhere to the ethos, pathos, and logos principles governing effective communication (Wieder, 2019).

Aristotle’s Rhetoric outlines how people should have the ability to view each case clearly and identify the available persuasion. While every person has their preferences on how they receive information, the use of persuasion certainly affects information exchange. PMT tampers with communication ethos. Ethos identifies the credibility of the communicator and message. For instance, showing empathy radiates credibility and enables individuals to make trustworthy decisions. However, PMT messaging model integrates fear into its messaging model, which negatively influences people’s judgments. Wieder (2019) also attributes a positive first impression as an integral component of affirming emotional conversation. Communicators should use their influence as an opportunity to positively influence others. However, fear appeals tend to negatively influence an individual’s decision-making process.

On the contrary, Srivastava et al. (2021) found out that coping appraisal and threat appraisal positively influence an individual’s response to perceived threats. PMT encourages protective behavior amongst individuals. The researchers also stated that the PMT model has been integrated and validated in enhancing protective behavior amongst internet users. Fear appeals have also been instrumental in enhancing self-efficacy and response efficacy in the context of online harassment, anti-spyware software usage, and mobile healthcare programs. Boerman et al. (2018) found out that PMT is integral at enhancing protective behavior towards digital privacy. Today, individuals are more concerned about their privacy and are also more likely to engage in protective behavior. However, individuals with less knowledge about privacy threats are more vulnerable to privacy threats. The researchers stated that digital skills are fundamental to the protection of data. On the other hand, Ylang (2020) stated that simple self-protective measures against identity theft are ineffective. Therefore, individuals should develop lifelong self-protective measures against identity theft. By taking the necessary proactive steps, individuals can minimize or prevent cases of identity theft. Poorly educated individuals are more likely to share their data without following due diligence on the organization. Online privacy has become a fundamental component of our daily lives (Boerman et al., 2018). There is a need for people to understand the role of protective behaviors when it comes to the internet.

Supporting Theories

According to Aurigemma and Mattson (2018), there is no universally accepted correct theory that expounds how individuals should enhance information security behaviors. Information security control is a voluntary act and there is a need to motivate people to protect themselves. The authors noted that various researchers focusing on information security integrate different theories into their studies. Researchers have used theories such as the theory of planned behavior (TPB), Theory of Reasoned Action (TRA), general systems theory (GST), technology acceptance theory, general deterrence theory (GDT), social cognitive theory, and unified theory of acceptance and use of technology (UTAUT) to explore information security research questions. Srivastava et al. (2021) use UTAUT dimensions together with PMT to assess the impact of COVID-19 on the acceptance of digital payment systems. Boerman et al. (2018) also agreed that different theories may be used to explore topics on digital privacy and online banking. Blackwood-Brown et al. (2019) also demonstrated various techniques may be used to educate the elderly on effective cybersecurity skills. Assessing cyber threats requires a hand-on approach and is a requisite skill in today's digital society.

The Theory of Planned Behavior (TPB)

TBP has been extensively integrated into IS studies and used to explain people's outlook on data security. According to Zhang et al. (2019), TPB utilizes a three-factor methodology to determine an individual's behavioral intention, namely, perceived behavioral control, attitude, and subjective norm. Attitude highlights an individual's internal emotional outlook towards an issue or threats. The perceived behavioral control describes an individual's perception of factors affecting a behavior, and the subjective norm outlines the environmental factors that may impede or promote an action. Rajab and Eydgahi (2019) also stated that awareness can be used to outline one behavior in TPB. Rajab and Eydgahi (2019) explored how conceptual frameworks affect an individual's intentions to comply with information security policies. Numerous researchers have evaluated the influence of TPB on regulation compliance in IS. Sommestad et al. (2018) deemed an individual's behavioral intentions as a result of predetermined beliefs on security compliance behavior. The authors were testing how employee perception on IS security affects compliance. The team of researchers tested the theory in relation to a group's general behavioral outlook. They found out that an individual's behavioral intention had a higher impact on IS security negligent behavior by employees. A person's intentions had more control on their behavior.

The use of digital banking platforms greatly depends on a user's emotional intention to adopt such solutions. In the current digital era, non-cash payment technologies are seen as the future (Srivastava et al., 2021). Digital payment platforms enable users to make transactions without physical contact requirements or compromise proximity guidelines essential in the COVD-19 era. The TPB approach may be used to independently assess belief influences on the acceptance of digital payment platforms. Verkijika (2018) used PMT and TPB to analyze smartphone security behaviors. The researcher used a modified PMT conceptual model to positively assess an individual's vulnerability and their behaviors. The modified PMT used TPB principles to study security intentions and behaviors. Their dual analysis approach yields improved information critical for decision-making. PMT takes into account more behavioral factors when evaluating research topics. Zhang et al. (2019) in their study analyzed the adoption of user intentions using the two approaches. As a consequence, they developed an in-depth perspective into technology acceptance and also addressed other goals within their study. PMT components may be used to assess behavioral intentions in TPB. However, TPB is not an ideal analysis model for risky behavior and therefore not ideal for this study. I did not select this theory as it did not fit into my research question.

Theory of Reasoned Action (TRA)

TRA was created to evaluate and predict human behavior. Wu (2019) carried out a study seeking to determine information withholding is counterproductive to combating cyberattacks. According to the scholar, internet users and governing bodies are increasingly concerned about reduced knowledge sharing behaviors. Knowledge hiding has significant ramifications in combating digital threats. The researcher believes that campaigns focusing on internet privacy have changed user behavior when it comes to data sharing. To some extent, privacy rules have altered social interaction, self-presentation, and internet norms. To investigate the inhibiting behavioral factors driving information withholding, the researcher analyzed user behavior using PMT and TRA. The theory proposes individuals make rational decisions after carefully assessing the situation and when they are in complete control (Wu, 2019). Behavioral intentions in TRA are a result of an individual's readiness to perform a certain action. In PMT, individuals are subjected to fear-appeals and persuasion. However, in TRA, the population under investigation is given the opportunity to make rational decisions under their own volition. TRA reduces the likelihood of individual's developing a negative bias towards a subjective norm. The conceptual model uses an intuitive and open approach to explain human behavior. Therefore, it is highly ideal in investigating social functions. In IS, information sharing should be voluntary to encourage rational behavior in individuals.

Hooper and Blunt (2019) used PMT, TRA, and the deterrence theory to assess IT employee behavioral outlook on information security. The pair of researchers were interested in evaluating the influence factors causing IT employees to lightly take into account data security. A lot of behavioral studies tend to focus their attention on non-IT staff members when evaluating cybersecurity topics. Researchers believe that attention to security is a fundamental trait for IT members (Syniavska et al., 2019). In addition, much research has also been dedicated to organizational policy compliance and often neglects IT employees. The intentions of IT members may affect an organization's security standing. Using TRA, they determined the cues of action, which influence individual behavior towards IS security. TRA attempts to predict attitudes and therefore is not ideal for investigating identity-theft cases. The methodology also attempts to predict attitudes. Its limiting factor is the individual's attitude towards a behavior.

Branley and Covey (2018) also used TRA in understanding the factors that make a subset of social media users engage in risky online behavior. The pair conducted a quantitative study evaluating the activities of more than 1200 users. Using TRA and TPB they determined the willingness of the users to engage in risky digital activities. Their study's findings would be instrumental at identifying why some digital bank users tend to engage in risky digital behaviors. For instance, an individual may use their banking details to purchase items from an unverified online platform. Such willingness to share their information puts and exposes them to adversaries. Furthermore, Esmaeilzadeh (2020) used TRA to analyze patient trust on Health Information Exchange (HIE) platforms. Using TRA, the researcher examined the perceived transparency of data privacy policies implemented by HIE. A patient's willingness to share data across medical platforms could potentially expose them to attackers. Using the theory of reasoned action (TRA) the scholar developed an empirical testing model to assess user trust. The study's findings would identify factors that may be used to improve patient willingness to share their data across health information platforms.

Unified Theory of Acceptance and Use of Technology (UTAUT)

Unlike PMT, UTAUT attempts to explain an individual's usage behavior and intent towards a particular technology. UTAUT conceptual model fuses eight behavioral models to analyze an individual's behavioral patterns. The behavioral concepts include technology acceptance model, protection motivation theory, theory of reasoned action, theory of personal computer utilization, theory of diffusion innovation, social cognition theory, and theory of planned behavior (Srivastava et al., 2021). It uses a mix of strategies in evaluation of the strategies needed to enhance the innovation adoption. The theory has been used to explore the social acceptance of new technological developments. It investigates the user's behavioral intention of new scientific development and its usage. Srivastava et al. (2021) used the model to evaluate user acceptance of digital payment platforms as result of the COVID-19 pandemic. COVID-19 has forced individuals to social distance and reduces physical contact to minimize the disease's spread. The use of hard cash was unsuitable in tackling the pandemic. Users perceive the disease as a health threat. The researcher used both PMT and UTAUT to evaluate the social influence caused by the pandemic. As a result, people have been forced to embrace the use of contactless payment models. COVID-19 is perceived as a threat, which has forced more people to switch to digital payment platforms. However, self-efficacy issues still plague user behavioral intentions on the technology. The scholars found out that more users exhibited willingness to learn about the online payment systems.

Another concept that may be investigated by UTAUT is the strategies used to improve user reception of digital banking utilities. Rahi et al. (2018) used UTAUT to explore the adoption of internet banking methodologies in Pakistan. The researchers in their study use four emotional indicators to analyze user reactions towards new innovations, namely, effort expectancy, facilitating conditions, social influence, and performance expectancy (Rahi et al., 2018). The team used a quantitative approach to examine user acceptance of the internet banking tools. Using the various dimensions of UTAUT, they evaluated how individuals perceive internet banking platforms in the mentioned country. They found out that users viewed internet banking as an easy transactional medium. Furthermore, the population stated that they have a high expectancy towards internet banking platforms. User's intentions towards the new technology revealed that they are likely to adopt the new technology. The opinions of the individual's friends, relatives, and anonymous reviews reaffirmed their belief in the technology. However, when it comes to data privacy, users are more inclined to respond to threats. Social influence has little effect on the user's intentions or behavior. Therefore, PMT is an ideal in the reinforcement of protective measures rather than technology acceptance.

Donmez-Turan (2019) used the UTAUT methodology to investigate user acceptance of the incremental integration of new technological infrastructure in the society. Ordinarily, the transition to new systems tends to affect an individual's perceptions and attitude. In essence, people at first find it hard to accept new technology and in extreme cases they may reject the technology altogether. For researchers, predicting these factors has proven quite difficult. The implementation of new technologies is often dealt a blow by user rejection, which in turn increases the workload. However, end-users still reserve the right to reject meaningless technologies (Donmez-Turan, 2019). The scholar's goal was to evaluate why individuals exhibit resistance to change and how they can overcome anxiety. The implications of the study's findings would translate to better adoption readiness by manufacturers and an attitude change towards technologies by individuals. User anxiety is a great impediment to positive behavior and affects performance expectancy. Therefore, PMTs use of threats would prevent uptake of new technologies. The PMT may be used to understand user motivation towards new technologies.

The use of information systems to facilitate digital record management by modern public administration is on the rise. Public institutions are utilizing electronic document management systems to enhance service delivery. Ayaz and Yanartaş (2020) sought to determine the public acceptance of digital systems. Users are expected to have positive intentions with a new technology for it to be successfully implemented. The UTAUT model was used to assess user intentions on the digital systems. First, users may be skeptical of a digital record management system as it exposes their information to attackers (Ylang, 2020). Secondly, many users are concerned about compatibility issues related to new technology. The performance expectancy of a new system has a significant impact on user trust. On the other hand, PMT uses fear-appeals to win user trust. PMT uses its components to reassure the intention of the system. In essence, threat appeals may enhance user expectancy in a new system. PMT integrates a systematic culmination to invoke interest and manipulate other variables crucial in the implementation of a system (Rogers, 1975). Fear is a motivational intervening variable and is aroused in response. PMT may be used to invoke a learned drive in individuals towards new technologies. However, Srivastava et al. (2021) emphasized on a positive influence when it comes to technology uptake. Their study revealed that response efficacy and intention towards a new technology affected technology uptake. Threats may affect an individual's outlook on a technology. People first consider any underlying threat on a system and how to counter it. Their motivation to secure a technology boosts the innovation's uptake. To boost the adoption of digital record management systems users must be motivated to protect themselves. Intention motivation eliminates user bias against a tool.

Digital Privacy and Digital Banking

A Brief History of Digital Privacy

The introduction of personal computers may be regarded as the tipping point of digital privacy. The emergence of household computers created new grounds for digital content brought about by the convenience of new technology. Personal computers (PC) with all their future variants offered individuals an interface to connect with the outside world and also eroded our right to privacy. Operating systems standardized information exchange between computer networks. The internet was invented after the arrival of personal computers. The World Wide Web helped connect standalone PCs and facilitated data sharing. At its infancy, stealing of information was a rare occurrence. However, as the internet became easily accessible amongst the general public so did data theft. The exponential growth of the web increased data exchange between institutions, people, and governments (Giwah et al., 2019). At its infancy, internet users transmitted data using unsecured protocols and methodologies. HyperText Markup Language (HTML) the flow of unguarded information on the web attracts individuals interested in undermining other people's privacy. As electronic devices evolved to laptops, smartphones and tablets, the principles of digital privacy began to encompass all these devices, which were now capable of accessing the corporate or work network (Meske et al., 2019). Computers play a key role in digitizing an individual's life and along with it came the digital issues associated with sharing personal information on the internet. Hacking was soon to become a security issue as data became the new source of wealth.

The continuous presence of people on the internet leads to the realization that technology may be integrated into the context of private lives (Losavio, 2020). Above all, organizations also took advantage of the technology. To boost implicit trust, company employees could access the internet and enhance workplace productivity. Most companies initially insisted that their employees must use only corporate networks to connect to the internet network. Pew Research Center report that indicates a dramatic rise in the use of social media networks by American workers (Snyder & Cistulli, 2020). While this posed a security threat, most organizations did not stop the employees as they found out that when they worked on the devices they are used to. Most employees registered higher productivity, and it also meant the company was to exploit the new user generated data. The shift to digital data sharing practices has increased data sharing principles. Access to digital data platforms has also exposed organizations that encouraged social media use within their premises.

Internet-mediated communication and social media use opens up new avenues for data exploitation and data surveillance. Adams (2020) algorithmic data surveillance has become quite rampant on the web. Terminologies such as big data and data mining are now normalized by web users. In the long run, there is a need for a balance between privacy and surveillance. Information societies across the globe recognized the need for comprehensive data privacy. An individual's right to privacy is a fundamental pillar of modern society (Wang et al., 2019). People also have a right to access information. The demarcation between private and public data has become vague. For instance, between a social media user and a social media organization, who has the right to manage information published on the social media platform. However, privacy preservation is a prerequisite of modern technology (Vasilev et al., 2018). The dynamics of data privacy have triggered governments, financial institutions, and societal organizations to develop stringent data laws.

Risks and Vulnerabilities of Digital Privacy

The continued reliance on digital communication presents a challenge to consumers. Data breaches and data violations have demonstrated that current protection methodologies implemented on the internet are not completely secure. The media reported widespread data privacy misconduct cases (Byrne et al., 2019). Social media organizations implemented unethical data mining techniques such as user tracking and cross-site surveillance scripts to collect information about the users. Internet organizations readily collect, and store information logged by users. Digital surveillance is viewed as a crucial utility in the creation of business utilities. While tracking an individual's data may assist the creation of efficient sales and marketing analytics. Violations associated with email breaches within the workplace also tampers with employee privacy (Snyder & Cistulli, 2020). Digital surveillance is considered as an invasion of privacy. Internet-based crimes are largely intangible making them harder to resolve.

The digitization of personal data presents various problems to the end-user. Today, internet users may not hide the digital footprints. For instance, a person sending an email is not completely aware that the message leaves a digital footprint such as internet protocol (IP) address, browser version, timestamps and more. These details may be stored for decades in the host organization's server and may be used as evidence by law enforcement agents (Losavio, 2020). Encryption weaknesses may expose an individual's data as it is on transit to the recipient. Cyberattack approaches such man-in-the-middle attacks sniff user data exploiting shortcomings present in data transmission protocols (Fuller, 2019). In the internet of things, inappropriate use of telecommunication devices negates any protective countermeasure integrated into a computing device. The distinctive nature of electronic communication presents many challenges to security practitioners. New digital privacy threats keep on emerging as technology becomes the core of modern communication.

Most internet users are least concerned about their online privacy or unaware of the risks associated with poor privacy techniques. Internet sites log visitor data using temporary browser cache files called cookies. Web cookies can track an individual's browsing behavior, clicks, and system details, so as to advertise to the consumer in a more targeted way (Bornschein et al., 2020). However, the data collected may put the consumer at risk or inhibit future behavioral intentions. Consequently, individuals face the following major digital privacy threats

Spying threat: An individual's internet activity is spied on by a number of surveillance tools such as online trackers, scripts, and cookies. Internet surveillance tools are primarily used to improve the consumer's shopping and browsing experiences. However, cybercriminals are known to inject dubious web scripts to mine user data and carry out illegal activities (Sommestad et al., 2018). Governments have also been known to monitor their citizen's online activities.

Information misappropriation threat: Recently, social media organizations have been accused of selling their user logs to third party organizations. Furthermore, poorly encrypted websites may expose an individual's data to cybercriminals (Dia et al., 2020). Online banking has been accused of paving the way to attackers. The financial reward associated with e-business and digital banking exploits and attracts all manner of cybercriminals.

Location tracking threat: Modern computing devices track an individual's geolocation data. The same data tech firms used to analyze an individual's activities and determine the most ideal products to push to the individual (Harvey et al., 2018). Geolocation trackers log an individual's real time location.

Identity theft threat: Today, identity-based authentication attacks have become one of the fastest growing digital crimes. Identity theft is one of the fastest growing digital crimes (Maitlo et al., 2019). Hackers are frequently abusing computer networks and accessing sensitive user information. The theft of user identities has proven to be quite lucrative. Cases of identity-based crime grew by 125% from the previous year in the U.S. (Maitlo et al., 2019). Major challenges associated with identity-based authentication attacks are the disruption of the individual's financial life, result in psychological difficulty, and lead to credit problems. There is a need for improved security solutions and awareness on identity theft.

Digital Privacy and Digital Banking

The progressive advocacy for digital transactional channels has changed the relationship between consumer and bank interaction. The adoption of online banking models has been accelerated by the adoption of digital technologies. Mobile banking has had a disruptive force on modern banking (Son et al., 2019). The shift to mobile banking may be attributed to the ever-evolving user demands. Traditionally, bankers had to physically visit financial centers in order to receive the much-needed banking services. The recent technological, social, political, and media had a profound effect on how people view technology (Trevisan et al., 2019). In essence, the digitization of banking services has changed consumer perception on digital transaction platforms. Furthermore, the improved use of information technology has increased user confidence on new digital transaction platforms.

Studies are showing that users have confidence on online transaction platforms. Bankers are also attracted to lower transaction costs associated with e-banking platforms (Mbama et al., 2018). Digital channels reduce instances of barriers commonly linked to banking halls. For instance, e-bankers can flexibly switch between banking applications in an instant. However, an individual planning to transact via different platforms will be required to physically visit the banks. Physically visiting banks is time consuming and tedious (Oertzen & Odekerken-Schröder, 2019). Melnychenko et al. (2020) carried out a study on the theoretical generalizations associated with digital banking platforms. Using qualitative, quantitative, and correlational analysis, the scholars investigated the relationship between volume of transaction against the performance of the banking system in use (Teece et al., 2021). The goal was to determine the dominant factors forcing users to transition to digital banking platform tools (Melnychenko et al., 2020). Srivastava et al. (2021) carried out a study seeking to evaluate the impact of COVID-19 on the uptake of contactless payment systems. By integrating PMT and UTAUT, the investigators found out that the pandemic's perceived threat and coping behaviors enhanced user trust on digital banking platforms. Using a quantitative approach, 387 Indians participants gave their feedback on the pandemic's perceived threat factor. COVID-19 had a significant role at encouraging users to shift to a cashless transaction approach.

Kaur et al. (2021) carried a qualitative investigation seeking to evaluate the emergence of digital banking platforms in India. The investigation underlying factors cause in-branch customers to shift to mobile banking technologies (Kaur et al., 2021). They used in-depth semi-structured interviews to gain better insight into the consumer's sudden behavioral shift. The study's population was the bank's executives. According to their findings, customers in India had gained more trust on digital banking platforms. Furthermore, the banks had met the required cultural and organizational changes needed to convince users that the digital payment platforms were secure. Ananda et al. (2020) explored the factors affecting the adoption of digital banking in the retail sector. The researchers used the extended technology acceptance model to determine the relationship between retail consumers and digital banking platforms. The study revealed that web technologies had a positive influence on the adoption of the technology.

The use of Rogers (1975) PMT has offered significant insight on user behavioral attitude towards identity-based authentication attacks affecting digital privacy in online banking. Some of the existing digital payment platforms do not offer their users sufficient protection (Cao & Zhu, 2019). Digital banking platforms such as Alipay and Paypal fail to offer their users the much needed anonymity tools. As a result, users may shun online banking platforms with poor privacy security measures. Financial data leaks tend to include transactional details on amount sent, spending location, user data and goods purchased (Reis et al., 2019). Fuller (2019) was cautious of digital privacy transactional platforms. The researchers conducted theoretical and empirical studies to find out if the general market was convinced by the new technologies. The scholars carried out a qualitative study seeking to determine whether members of the public were willing to pay for full digital privacy tools. It emerged that digital firms were interested in offering paying customers online anonymity. However, the population sampled expressed minimal interest in paying more for additional privacy features. It is reported that over 85% of young adults prefer little digital tracking (Fuller, 2019). Privacy-related limitations affect the current digital society. In the context of privacy risks related to digital banking utilities, Aboobucker and Bao (2018) investigated the impact of internet banking on user privacy. The researchers noted that there are various factors inhibiting the proper integration of digital banking platforms. Increased interconnectivity brought about by the internet has stimulated growth within the banking sector. However, constructs such as privacy, security, perceived trust, perceived risk, and platform usability still affect the implementation of web technologies (Green et al., 2020). By addressing these issues, user confidence may be stimulated into trusting digital transaction platforms.

Transition and Summary

In section 1, I analyzed the background of identity-theft and how it affects the adoption of digital banking platforms. The goal of this research is to investigate which strategies would be effective at handling identity-based authentication attacks. The conceptual framework used in this study is the protection motivation theory. A detailed review of the peer-reviewed articles was performed involving a descriptive data analysis approach. The Protection Motivation Theory was developed to integrate fear as an intervening variable in modern studies. I first began by providing a brief breakdown on the conceptual framework's use of fear-arousing stimuli to modify an individual's behavior. Using PMT's fear-arousing model, IT security professionals may design effective strategies to mitigate identity-based authentication attacks. The nature of the study focuses on stimulating individuals to change their attitude towards the internet and digital privacy in order to mitigate cases of identity theft. I provided a comprehensive breakdown of the PMT's assumptions and how they might interfere with this study's findings. I proceeded to give a brief breakdown of PMT with other theories. I provided a comparison of PMT against similar behavioral assessment conceptual models. I then demonstrated how the different authors integrated PMT with other methodologies into their studies. Finally, I compared studies analyzing identity theft and digital theft. The findings of the studies may be used to compile mitigation strategies against identity theft and digital privacy in online banking.

Section 2 of this study investigated the strategies used by IT security professionals to mitigate identity-based authentication attacks in the respective banking institutions. The section also focused on investigating the role of digital privacy guidelines in enhancing mitigation strategies. Furthermore, the section outlined the researcher's role, research method, population sampling methodology, data collection techniques, and data analysis. I also outlined how the data was collected, analyzed, and validated. In section 3, I provided qualitative study overview, presentation of the findings, application to professional practice, the implications for social change, recommendations for action, recommendations for further research, reflections, and conclusion.

Section 2: The Project

In this study, I sought to examine mitigation strategies for identity-based authentication attacks affecting digital privacy in online banking. Section 2 of this project outlines in detail the methodology and investigation process I integrated into the study. I also describe the role of the researcher, expound on the participant selection process, highlight the research methodology and design, and explain the population sampling approach that I used. Importantly, I also explained how the study follows ethical research guidelines. Other areas covered in this section include the selected data collection process, data organization technique, data analysis methods, reliability, and validity.

Purpose Statement

The purpose of this qualitative pragmatic study was to examine the strategies IT security professionals working on internet banking platforms use to mitigate identity-based authentication attacks affecting digital privacy in online banking. The target population for this qualitative pragmatic study is IT security professionals working in the banking industry in the northeastern region of the United States. The results of this study may contribute to a positive social change by offering mitigation techniques to protect bank customers and employees' digital payment systems from identity-based authentication attacks and threats. In addition, the findings from this research may be used to guide IT security professionals in other organizations with appropriate digital privacy strategies to proactively prevent identity-based authentication attacks for online users' security.

Role of the Researcher

In qualitative research methodology, the investigator is the main data collection instrument. Using the skills and academic knowledge I have acquired through the years, I collected qualitative research data for this study. Researchers have a mandate to broaden the scope and breadth of the topic under investigation (Alexander & Smith, 2018). An investigator sets up the stage for the topic's future explorations. However, researchers are dissuaded from integrating their personal biases into academic literature. In descriptive studies, it is critical to establish credibility in the study (Hilger et al., 2018). One way to achieve this is by ensuring credibility, observing ethical guidelines, and guaranteeing the participants' wellbeing. Ethical conduct in research solely lies on the researcher (Cumyn et al., 2018). Therefore, how one perceives and acts throughout the research process is paramount to the study's overall credibility. The qualitative method puts an emphasis on proper behavioral and ethical conduct. I observed professional research conduct and ethical standards. There are many ways a researcher may interfere with the efficacy of the study such as bias, poor research methodologies, tampering with evidence, and more. According to Glegg (2018), qualitative researchers may introduce bias due to the beliefs they hold. However, a researcher may minimize instances of bias by establishing preventative measures that safeguard participant identities and promote transparency and research ethics. The interview data methodology is highly prone to bias (Taylor et al., 2021). I acknowledged that differences exist within the study. I observed bias-free language guidelines while conducting the study. In qualitative research, bias may occur in the dissemination of the study (Haven & Van Grootel, 2019). The interview process may contaminate the data collection process by introducing bias. By avoiding leading questions, a researcher may minimize bias in their studies. Instead, I strictly adhered to the interview protocol and did not ask any leading questions. I avoided bias by ensuring that I did not have any personal relationships with the study participants. A more reliable qualitative research process was achieved by following the same interview protocol throughout the study (Aguinis & Solarino, 2019). My role as a researcher in this study requires me to adhere to the interview protocol. I ensured that each participant was subjected to a similar set of semi-structured interview questions. For this study, I examined the strategies IT security professionals working on internet banking platforms use to mitigate identity-based authentication attacks affecting digital privacy in online banking. Qualitative investigations are highly inquisitive and therefore the researcher needs to maintain utmost integrity (Becker, 2019). In essence, I searched for meaning within the data. I carried out an exhaustive data analysis process and ensure my sources are valid. Secondly, I used data triangulation within the study to find meaning. I ensured that my participants are credible and experienced in the cybersecurity field. To ensure study reliability, I used a systematic data analysis approach. As a researcher, I adhered to the principles set in the *Belmont Report.* The *Belmont Report* outlines an ethical analytical framework consisting of (a) respect for persons, (b) beneficence, and (c) justice (Schupmann & Moreno, 2020). I also did not contact my study's participants before receiving IRB's approval. Furthermore, it was crucial that I observe ethical guidelines set to protect the human subjects. A researcher's role extends beyond the scientific scope of the study (Hilger et al., 2018). As the primary research instrument, I ensured that I did not influence the choices made by the study's population. I used an open communication approach when interacting with the study's participants. I actively listened and engaged my participants throughout the research process.

Participants

Before beginning a research study, scholars are encouraged to come up with criteria and principles that will guide them in participant selection (Liu et al., 2019). The scholar will evaluate the research findings, as well as the transferability, using the relevance of such criteria and principles (Liu et al., 2019). When a researcher uses a specific participant selection criterion, they create a more reliable and accurate system for identifying and describing study participants (Team et al., 2018). The participant selection process should also protect the selected population. As a result, in order to protect study participants, I monitored the research criteria. I recruited five IT security professionals from LinkedIn. The participants comprised of IT security professionals working in the banking sectors with at least 5 years of experience. I asked potential participants to contact me using the same email address as in the email correspondence. I contacted the participants via email and they indicated their willingness to take part in the study. According to McEvoy et al. (2019), a researcher must communicate with study participants in order to build confidence and mutual trust. Also, open communication between the researcher and the study participants ensures confidentiality (LaDonna et al., 2018). This is significant because study participants who have faith in the researcher will be more honest in their comments, resulting in more believable study results. Interview questions can be answered in many different ways. Open-ended questions allow participants to express themselves without being restricted to the responses that multiple-choice questions may offer (LaDonna et al., 2018). In close-ended questionnaires, the participant can only respond using the set of predetermined answers. A close-ended questionnaire achieves its objective without taking into account an individual's unique response. Essentially it can limit responses, especially one that most participants would have chosen. Open-ended research may miss important aspects of the study's design. In this study, I used open-ended structured interview questions to allow for unexpected responses from the interviewees. There was no need to use close-ended questionnaires because the participants' responses may not be included in the choices on the questionnaire. It is possible for the interviewer to elicit more information by asking open-ended questions. The structured interview will allow the interviewer to focus on a narrow range of topics by using established questions (Becker, 2019). The study's participants may be accessed in several ways. Call-Cummings et al. (2018) noted that participants may be contacted via emails and telephone calls. I reached out to the study's potential participants using emails, text messages, and invitations. It is also vital that a researcher uses credible and reliable participant selection processes (Christensen & Miguel, 2018). During the interview phase, I asked questions to gain deeper insight from the participants. In interviews, the answers given often include details that would be missed in surveys or questionnaires (LaDonna et al., 2018). I developed a professional relationship with the interviewees. With qualitative interviews, the questions and discussions will differ from interview to interview. In research, participants may not provide consistent results to the researcher (Strickland & Stoops, 2019). Overall, it is important that the study's participants feel confident with the interview process. I notified my participants that they could withdraw from the interview process at any time. Winning the participant's trust is vital in obtaining credible answers.

Research Method and Design

Research Method

I used the qualitative method to investigate mitigation methodologies that may counter identity-based authentication attacks and enhance digital privacy. Qualitative research method examines new ideas as to answer the why or how a phenomenon occurs (Richard et al., 2020). Therefore, it emphasizes understanding why themes make the qualitative method suitable for exploring social problems. In IT, the cybersecurity field is plagued with tons of social problems (Wiafe et al., 2020). The qualitative methodology allows a researcher to focus and collect complete data from the participants' perspective and real-life experience, as well as explore the participants' subjective knowledge of the study issue (Stenfors et al., 2020). The qualitative method may be used to investigate the cause-effect factor motivating cyberattacks. Furthermore, the qualitative research method is necessary to determine the underlying social factors affecting information security. Qualitative research methods can help identify influential and non-numerical elements that may influence a user's decisions or actions (Richard et al., 2020). The qualitative method is ideal at determining which steps the victim could have taken to prevent an attack or a repeat attack. I selected the qualitative approach for this study because it may be integrated into PMT and be used to develop effective countermeasures against identity based-authentication attacks. To gather information from IT security professionals about their impact on implementing cybersecurity methods, a qualitative research method was appropriate for this study.

According to Kelley-Quon (2018), the quantitative approach measures the outcomes of an event using numerical data. The quantitative methodology is a data-oriented investigation technique and transforms data into usable statistics. The statistical data uncovers patterns and facts. In my study, I did not collect any numerical data. According to Gill (2020), probability and statistics form the foundation of quantitative research. The approach attempts to evaluate variables using a structured approach. In this study, I did not evaluate variables or analyze the magnitude of a phenomenon. Additionally, the quantitative methodology is ideal for large datasets (Maxwell, 2019; Richard et al., 2020). By identifying patterns within the data, the quantitative method compresses the findings to make meaningful comparisons. I did not attempt to compare variables or phenomena within my study since my goal is identifying strategies to mitigate identity-based authentication attacks.

The mixed methods approach uses multiple forms of inquiry to answer research questions (Alam, 2020). It is an emergent methodology that systematically integrates quantitative and qualitative data to answer an inquiry. The mixed-methods research was not appropriate for this study as it combines quantitative and qualitative procedures in one study. A mixed-methods technique is best suited for inductive and deductive examination of a research issue and hypotheses (McGrath et al., 2018). Nonetheless, my study goals were to focus on the perspectives of participants. Therefore, I only used the inductive approach to analyze my data. A mixed-methods strategy combines qualitative and quantitative approaches, or data gathered using one method is converted and evaluated using the other method (Maxwell, 2019). Because I would not study the relationship between variables and test hypotheses, mixed methods were inappropriate for my study. However, I collected non-numerical data from interviews and reviewed documents. Since I needed a deeper understanding of the research study participants' views, quantitative and mixed methods were not be suitable for my study.

Research Design

In this study, I chose a pragmatic design as the best suitable for the investigation. Ethnography, phenomenology, pragmatic, and case studies are a few examples of qualitative research designs (Gill, 2020). In terms of the research data, problem, data analysis, questions, and reporting results, these methodologies are similar to traditional research. Each of these research designs implies that the researcher uses various data collection methods (Soilemezi & Linceviciute, 2018). For example, while studying people and cultures, the ethnography research design is commonly used. The researcher obtains an effective way and technique for format through ethnography. The researcher must study the subjects while they are in their natural environments in order to fully comprehend their perceptions, experiences, creation, and socialization (Crick, 2020). The ethnographic researcher collects data in a real-life context using a variety of evidence sources (Cypress, 2019). I did not use ethnographic design because the study would not involve group culture observations. Phenomenology is a study method that focuses on exploring the meaning of lived experiences by a person or a community. Researchers that use phenomenology attempt to identify a concept as it appears from the standpoint of a single person. Phenomenological studies have fewer participants than other qualitative designs, although they tend to use lengthier interviews with each respondent to understand the true meaning of the experience (Taylor et al., 2021). I did not use the phenomenological design because the goal of this study was not to learn about the respondents' real-life experiences to mitigate identity-based authentication attacks affecting digital privacy in online banking.

Pragmatic design strategically combines various established approaches to meet the needs of a study. The pragmatic approach is not new to information security and often viewed as a rigorous tool in describing a situation (Ramanadhan et al., 2021). The pragmatic perspective is informed by the researcher's understanding of an event or methodology (Clarke & Visser, 2018). The methodology uses a range of strategies to answer the research question. In essence, it is a multi-methodology approach that attempts to sensibly answer a question. I collected exhaustive data pertaining to the research question through interviews and other data collection tools. An inductive approach was used to align the study's aim and produce new understandings. When no new ideas emerge from study interviews, the researcher assumes that data saturation has been achieved (Aldiabat & Le Navenec, 2018). The pragmatic approach benefits the researcher by broadening data while setting a high sensitivity bar (Carhart-Harris et al., 2021). According to Aldiabat and Le Navenec (2018), qualitative researchers may interview more people until they achieve data saturation. When qualitative researchers realized that more participants are not providing fresh information on the topic under investigation, they may consider ending their interview sessions.

Population and Sampling

For this study, I used the purposive sampling approach. In the purposive sampling methodology, the investigator intentionally selects participants who meet a set criterion. The purposive sampling methodology lets the scholar select individuals who will inform the study (Butler et al., 2018). The approach lets one identify information rich subjects using an evidence-based approach. I selected participants well versed in information security or cybersecurity. The study population comprised of IT security professionals working in the banks. An organization's cybersecurity implementation can be influenced by a sample of employees. People who choose or install security measures must have a considerable impact on their implementation (Gruschka et al., 2018). The effectiveness of an organization's cybersecurity protection can be influenced by the organization's senior leadership, information technology staff, and other employees. It is up to senior management to make decisions and set the tone for the entire company's culture. This information is needed to understand how each employee's motivation might affect the effective implementation of cybersecurity methods across the organization. I did use the snowball sampling technique. The snowball technique is a chain participant referral process whereby the respondents also assist in recruiting more respondents (Mawhinney & Rinke, 2018). I was the main research instrument that performed the selection process. A non-probability participant selection process may yield better results. The participant selection is integral in the overall study's findings (McEvoy et al., 2019). I chose participants with experience in online banking and information security.

The goal of purposeful sampling is to select information-rich samples (Butler et al., 2018). In qualitative research, purposive sampling may contribute to data saturation. Each topic tends to be examined by the researcher using various methodologies and also by employing exhaustive data collection techniques. Stakeholders find it difficult to make sense of such voluminous data. Research syntheses are therefore as important as primary research in terms of ethical representations and methodological rigor (Crick, 2020). According to Jain (2021), the appropriate sample size for a given study is determined by a number of criteria, including the individuals and groups participating in the investigation. In this study, the research question, research goal, and data saturation to estimate the best sample size.

I selected participants from various IT security backgrounds working in banks in the northeastern region of the United States. IT security professionals working in banks also make suggestions to the organization's senior management on other significant topics related to strategy like cybersecurity and other concerns. In this pragmatic inquiry, I chose banking organizations as the reference point because I want to see what strategic methods they used. I chose banking organizations as the study’s point of reference because I want to see what strategies banks used to adopt the PMT. The pragmatic approach provides researchers with sensible and practical methods to answer a given research question (Clarke & Visser, 2018). I began my search for participants for the sample by looking through online digital directories. Limiting the search to the northeastern region of the United States guarantees that only participants who met the study's population criteria will be contacted and drive the data saturation effort. To choose the sample size for this investigation, I used three guiding concepts. These guidelines included thinking about the research topic, reflecting on the study's objective, and emphasizing the need of data saturation.

I attempted to find as many participants working in the banking sector. As a crucial part of my work, I targeted data saturation. I reached data saturation when the research participants provide no new information. I conducted interviews with as many participants as possible until the data saturation was reached. Cronje (2020) explains why a qualitative researcher needs to evaluate a phenomenon in the real world. The pragmatic design allows researchers to utilize different approaches in analyzing a problem (Levitan et al., 2018). To improve rigor and validity, I advised participants to choose their preferred interview settings. A comfortable interview atmosphere encourages participants to openly answer interview questions and ask questions if they do not understand something (Taylor et al., 2021). In essence, the participants felt more at ease, calm, and safe in deliberating on their points of view while openly talking with me. I conducted the interviews in a quiet area, away from potential distractions and automated bias. This aided in achieving the required privacy for the participants as well as the interview process. I used questions from the interview methodology to elicit responses that reflect the participants' overall understanding. I used Zoom to conduct the interviews.

At the end of the interview, I also enabled participants to ask questions, which provided an extra opportunity for gathering additional information. Richard et al. (2020) argued why a qualitative researcher is needed to evaluate a phenomenon's real-world context. The pragmatic approach relies on collaborative research methods in identifying user experiences towards a phenomenon (Sebele-Mpofu, 2020). Alam (2020) claimed that in a relaxed interview situation, participants are encouraged to freely react to interview questions and ask questions if they do not understand something. As they become more experienced with the interview procedure, the participants felt more at ease, calm, and safe in deliberating on their points of view while openly talking with me.

Ethical Research

In today's research, the ethical treatment of human subjects in study is viewed as an integral credibility factor. In the early days, scientists would test harmful substances or unethical procedures on human test subjects. This was demonstrated by Nazi doctors and scientists who conducted horrific experimental research on human subjects during World War II (Kolman & Miller, 2018). The Declaration of Helsinki was enacted by the World Medical Association as a model for the ethical principles or codes that researchers must follow when conducting studies involving human subjects (McKenna & Gray, 2018). The researcher has a moral and ethical obligation to ensure that the participants do not suffer any harm as a result of their participation in the study. Informed consent ensures that participants are completely informed about the research, understand the risks and rewards, are competent and clear in making choices, and participate voluntarily without any manipulation (Fernando & Bandara, 2020). In order to establish trust between the researcher and the participant(s), I presented a consent form to the interview participants. I also included a copy informed consent form in the appendix. This form has information about the study, the procedures that the participants asked to follow and a statement that participation is completely voluntary. According to Kellam and Cirell (2018), even after obtaining written informed consent, participants are still free to withdraw from the study at any point in time, with no need to give a reason or an explanation for their decision.

Participants in this study can also opt out of the study by contacting the researcher by phone or email and stating their desire to be removed from the study. In qualitative research, it is integral for the researcher to protect their respondent's identities (Cumyn et al., 2018). I used pseudonyms to protect the participant's details and also track their input. As a recruitment strategy, incentives are used in a variety of ways in various studies. While money can be used to reimburse research-related expenses, compensate time and inconvenience, provide an incentive to overcome a lack of interest and show appreciation, caution must be taken not to introduce coercion or create undue influence or inducement (Zapata-Barrero & Yalaz, 2020). The participants did not received any gift or reward in order to prevent participation from being motivated or influenced. Research participants' data must be protected by all researchers, no matter where they are based.

The clinical trial guideline, an international and ethical standard, requires de-identification and processing of participant data for ten years in an off-site secure facility (DuBois et al., 2018). I used participant coded numbers instead of names to keep the participants' identities safe. Thereafter, all records have been stored in a lockbox for five years, and will be shredded or deleted after five years. Due to the fact that no personally identifiable information was collected, the proposed research poses a minimal risk to participants. As part of the research, Google Drive may be used to store the data collected (Team et al., 2018). The least privilege principle may be used to secure access to the data collected as part of the study (Paradis & Varpio, 2018). This means that no one other than the researcher and the mentor have seen the collected data.

Five years after the study is published, the data I collected and stored in cloud servers will be released or destroyed. The research interviews started after all participants accepted the consent form. I will delete the collected data after the retention period has expired. Individuals who opt to participate in research studies are aware about the information that will be collected and often give permission to the researcher to collect that information (Xu et al., 2020). During the interview, the participant's identity was protected by confidentiality. Raw data was shared with those who have a legitimate need to know, thanks to the privacy laws in place. Any study participant's rights was not violated by the researcher. Information about study participants should never be compromised by the researcher (Becker, 2019). Ethics issues can arise at any point in the research process, including when defining the problem, stating the research objectives, reviewing literature, choosing the research design, analyzing data, discussing conclusions and future recommendations, and citing sources (Pallisera, 2019).

Data Collection

Instruments

For this study, I took up the role of the primary data collection instrument since I am tasked with the duty of collecting study's data. Hagues (2019) stated that selecting an appropriate data collection technique is integral for knowledge transfer. In qualitative studies, data collection should be pursued in a systematic approach (Ibrahim et al., 2019). Collecting qualitative data focuses on finding data that will answer the why and how of the issue at hand. Furthermore, data collection involved continuous interaction between the researcher and the study's participants (Jain, 2021). During the data collection process, I ensured that I examined participants within their natural settings. In qualitative studies, the researcher's main aim is to gain an in-depth perspective of the social phenomenon within its natural surroundings or setting (Wolnik et al., 2018). When investigating a social phenomenon, the researcher must establish trust with the study's participants so as to obtain credible information. The experiences of the population give the researcher a broader perspective of their motivations, opinions, interests, and feelings towards the topic under investigation (Jain, 2021). As the data collection instrument, I was thorough while pursuing the project.

A qualitative inquirer may obtain data for their study using semi-structured interviews, observation, surveys, visual analysis, and textual analysis. Qualitative data collection methods and designs contribute to the development of the study and support future development (Perchoux et al., 2019). Interviews are grouped into three fundamental domains, which are unstructured, semi-structured, and structured (Glegg, 2018). I conducted my study using the semi-structured interview approach so as to draw out crucial details of the participants' experiences. Semi-structured interviews are an interactive form of data assortment tools that offer a more personalized exchange of information (Jain, 2021). Furthermore, during the interview process, the interviewer may observe and reflect on the participant's behavior and personality (Hagues, 2019). In an interview, other influential factors give the interviewer a glimpse of the participant's thinking. I used the open-ended questions included in the study to gain a better insight into the research phenomenon. I believed the questions are highly interactive and had a significant impact on the progress of this study. The qualitative research design elicits deep reflections by the participant, which is vital at guiding the progress of the study (Glegg, 2018; Jain, 2021). Critical interviewers are often reflective and reflexive, that is why I opted for an open-ended semi-structured interview approach. The semi-structured interview process caters for a fluid and flexible research approach.

To ensured that my semi-structured interview stays on track, I integrated an interview protocol in Appendix B. I formulated a set of 12 open-ended interview questions to assist me in collecting data concerning my research topic. The semi-structured research interview is an ideal strategy for collecting valid data for qualitative studies (Call-Cummings et al., 2018). The semi-structured research interview may incorporate both open-ended and closed-ended research questions to enhance the study's clarity. In general, the researcher utilizes a general structure that is devoid of bias (Wolnik et al., 2018). I designed the interview guide to comprehensively assess the various aspects affecting my research topic. Apart from the interview questions, I analyzed publicly available information such as NIST and industry standards to gain a better validity to the study. Also, I analyzed public accessible documents such as newspaper articles, journals, and reports associated with banking security. Both the interview questions and document analysis processes was primarily focus on generating secondary evidence needed to improve the quality of my findings. In the document analysis, I integrated both existing and prospective data to generate conclusive results. I utilized already published results, archived research data, and publicly accessible databases. Qualitative researchers should be keen on the quality of data they integrate into the study (Christensen & Miguel, 2018). In addition, I cross-checked the interview's responses with the participants to develop an accurate theme and ensure consistency.

Each participant in the interview submitted differing answers and their input was replicable. In qualitative research, the data collection process should yield similar results in the instance different populations are sampled (Hagues, 2019). Finding replicability is a contentious issue in qualitative studies. A study's replicability is examined using three distinctive criteria: (a) exact replication, (b) conceptual replication, and (c) empirical replication (Aguinis & Solarino, 2019). Replication reduces instances of errors within the study. However, in qualitative studies, it is quite difficult for a scholar to achieve exact result replication (Glegg, 2018). I used a transparent interview process to enhance the reliability and replicability of my study. Also, I recorded my participants' views so as to cross-reference their input later. However, I notified them and requested their permission before recording their input. Finally, I concluded my interview session by notifying my interviewees that their safety has been guaranteed and they have a right to withdraw their statements. In investigative reports, the participants' identities should stay anonymous to prevent public victimization (Gunsalus et al., 2018). Researchers have a central role in protecting the identity of their participants.

Research consistency is considered a key pillar of scientific studies. By focusing on transparency and openness, researchers can reduce instances of misleading content (Christensen & Miguel, 2018). Notably, I ensured that my personal biases do not interfered with the study's findings. I synthesized the study's materials using a deductive approach. Furthermore, a methodological triangulation technique was used to provide the researcher with various perspectives on the topic. The methodological triangulation process uses a convergence approach to enhance the confidence of the study's findings (Saks, 2018). In essence, methodological triangulation uses various multiple approaches to rigorously analyze data and identify common themes. The rationale for using the methodological approach is finding out the data's consistency, truth-value, and applicability (Natow, 2019). Social scientists integrate various methods into their studies when faced with uncertainties. I employed the methodological approach to accurately synthesize the data. I am interested in the truths within the data and also minimizing instances of research bias. Utilizing a combination of data strategies makes the information more understandable.

Data Collection Technique

My primary data collection technique obtained from semi-structured interview approach. The interview questions were highlighted at the end of this paper (Appendix A). The interview process utilized already predesigned interview questions that assisted me in staying consistent. Interviews are viable and highly utilized by qualitative researchers as a data collection tool (McGrath et al., 2018). Semi-structured interviews may be used to investigate a broad spectrum of research questions. The semi-structured interview approach lowers the participants' chances in giving well-choreographed feedback. It permits the respondents to give original answers that enhances a study's validity (Aguinis & Solarino, 2019). I selected the semi-structured interview approach to enhance the study's flexibility. The interview protocol contained open-ended questions.

The interview protocol included at the end of this research (Appendix C) and broken down into three sections, which are the pre-interview, main interview, and post-interview.

The interview process has its advantages and disadvantages. Its advantages are: it is a highly flexible research technique, has a better response rate, may be non-verbal, the interviewer has control over questions, and is conducted in a serene environment (Jain, 2021). The disadvantages of the semi-structured interview approach are: it may be costly, potential respondents may decline, interviewer bias may affect the study, and may be time-consuming (Glegg, 2018). On the other hand, researchers may use structured interviews to collect data on the research topic. I did use the structured interview approach, as it is quite rigid. In addition, qualitative researchers may use the unstructured interview approach to gain more insight into the topic under investigation. The unstructured interview may contain one predetermined question (McGrath et al., 2018). However, I had multiple predetermined questions in the study.

I synthesized data from publicly accessible documents. The data obtained from the semi-structured interview will be cross-referenced against data obtained from publicly available cybersecurity organization documents retrieved from the internet. I used peer-reviewed articles. Utilizing external sources enriches the evidence-based synthesis approach (DeVaney et al., 2018). A broad and rich data analysis process improves the reliability and validity of the research (Flemming et al., 2018). By merging multiple data collection and evaluation approaches, I obtained emerging themes occurred within the study. The main disadvantage of utilizing publicly available documents is that they may be prone to bias (Jain, 2021). Newspaper articles may contain biases that affect the study's validity.

I performed member checking after the interview and after I transcribed the participants information to enhance the research's validity and minimize instances of bias. Member checking is common practice in qualitative research used to assess whether the participants demonstrate an understanding of the research phenomenon (Caretta & Pérez, 2019; Iivari, 2018). It is a technique used to determine if a researcher has captured participants' information correctly. Member checking also ensures that the participants do not collectively construct assumptions that interfere with the study's validity (Caretta & Pérez, 2019). By carrying out member checking, I strengthened the study's accuracy and strengthened its results. It is a recursive process and crucial to ensuring the study is not homogenous. To minimize instances of participant collaboration, I used a random and non-heterogenous participant selection process. I used a randomized interview questioning approach.

Data Organization Techniques

In qualitative studies, researchers often collect a lot of information on the topic of interest. In essence, qualitative research is a data-intensive investigation methodology (Cepeda et al., 2019). In every step of the pragmatic inquiry, the investigator tries to align their study by accumulating as much data as they could. Too much data within a study may lead to information saturation and also cause the study to be disjointed. Qualitative researchers integrate several strategies to ensure their paper is organized and coherent (Edwards & Holland, 2020). Data organization within a study may take a systematic, thematic, or deductive approach. Organizing data offers efficient access for the researcher and improves interpretation accuracy. There are simple ways the researcher may organize their data for easy retrieval. I used logs, notes, and memos as a simple way of organizing my data. To ease file access, I created dated folders and sub-folders that assisted me in tracking my research process. Data attributed to the interview process ha been archived on my computer and copies kept uploaded into private cloud servers. I used a journal to track the progress of my study.

I used alphabets and numerals to track my transcripts and interview logs submitted by each participant. Field notes are also essential at tracking my study's progress and also recording key events within the interview process. Interview data validity is also another integral component at enabling researchers to get acquainted with the study. I jotted down short notes on the respondent's overall tonal variation in my journal. Tracking the interviewee's minute details is a good research practice (Maher et al., 2018). In addition, I transcribed the respondents' input so as to have a digital copy of the interview.

Qualitative software analytic tools will also be used to triangulate and analyze digital data collected. The selected software for this study is NVIVO software. I ensured the research's data is stored for the next five years in an encrypted drive. Furthermore, I created a backup cloud drive. The data uploaded into the cloud drive were encrypted. Physical files attributed to the study have been stored in a private and secure safe. The data will be shredded after the five years.

Data Analysis Technique

According to Lester et al. (2020), many researchers are unfamiliar with qualitative data analysis techniques. The research design seemingly limitless data collection approach is partly to blame. Most investigators assumed that learning the basics of qualitative studies will equip them with enough skills to perform comprehensive content analysis techniques. To generate quality qualitative studies, one must take time to learn the various data analysis approaches (Srivastava & Hopwood, 2018). Researchers must understand their study's primary audience should guide them in selecting an appropriate research design. The thematic analytical method has been conceptualized to be applied in a vast number of studies. I used the thematic data analysis approach on the data collected in the study. In essence, the data during the interview, observation, document synthesis, member checking, journal entries, and short notes were evaluated for themes. In addition, I used a recurrent data analysis technique to ensure that I do not omit or fail to notice patterns within the data. First, I used Nvivo to transcibed the data into a raw format suited for thematic analysis. I ensured that all the data analysis fits into the qualitative research design format. This means I converted all the data obtained in the interview data collection process into an ideal format. I created a roadmap for thematic analysis. It is useful for researchers to set up an appropriate landscape for the thematic analysis process.

My main goal in carrying out the data analysis process was to appraised the common themes and patterns occurred in the data collected. I used NVivo software to analyze the recurrent themes. Several common approaches often yield consistent themes within the study (Lester et al., 2020). The first step in data analysis was to find the codes in the data. First, I affixed codes to the field notes I collected and also on the observations. Attaching codes to the data assists in tracking down the patterns within the study. Secondly, I noted down remarks recorded in the margins and affixed themes to the data. The third step was sorted and sifted through the data to identify similar phrases used by the interviewees, the relationship between the themes, patterns, noted down the distinct differences with the data, and grouped the sub-groups. Maintaining an analytical perspective is essential in identifying the emergent themes (Saks, 2018). In the fourth step, I isolated the emergent pattern and processes within the data. The commonalities and differences assisted in creating new data collection patterns.

After identifying the patterns, I grouped the recurrent factors into small sets of generalized codes. By discerning the patterns, one may discover the consistencies and inconsistencies within the data (Srivastava & Hopwood, 2018). I analyzed the generalizations occurring in the study. These generalizations informed my topic and body of the research. I constructed theories associated with the study. Finally, I compiled a comprehensive report that either validates or invalidates my findings.

The final report should correlate the concepts of PMT and identify strategies used to enhance data security in online banking platforms. The findings should have a significant impact on data security (Alam, 2020). Identifying emergent themes is integral in promoting protective behavior needed to deter digital banking platform users from engaging in risky behavior. In addition, the emergent themes were critical in creating strategies needed to secure bank networks. IT security professionals need to embrace a protective role in minimizing the cases associated with account infiltration within the banking setting.

Reliability and Validity

Introduction

To guarantee the study was of high quality, I integrated strategies that observed reliability and validity in the study. According to Christensen and Miguel (2018), from the ontological perspective, a study must exhibit desirability of replicability. In essence, researchers aim to create studies whose results can be easily replicated. Every investigation must yield similar results when subjected to similar conditions. Therefore, investigators must be as transparent in their research approach as possible. Transparency is gained by ensuring the study is trustworthy. When assessing a study for credibility, scholars often assess a study’s dependability, credibility, confirmability, and transferability. Salarvand et al. (2020) presented a four criteria model of trustworthiness utilized in qualitative studies, which are dependability, credibility, confirmability, and transferability.

Reliability

Reliability in qualitative studies refers to the ability of a study achieving consistent results when carried out by different researchers and subjected to an alternative population (Rose & Johnson, 2020). In humanist qualitative research, reliability is a core element in increasing a study’s trustworthiness. According to Poe et al. (2018), scholars often view reliability as the reproducibility of results. In this study, member checking was used to ensure the findings are correct and reproducible. To achieve this, I provided the participants with an opportunity to verify my interpretation of views. I shared briefs and summaries from the study with the participants to build a positive rapport with them. Moreover, member checking is one way of achieving study reliability (Caretta & Pérez, 2019). The approach was used to ensure the participants are in mutual agreement with the study's findings. I stored the data collected to ensure that other researchers are in a position to replicate my findings. Essentially, I used different data sources to verify my suppositions and research questions.

Validity

According to Rose and Johnson (2020), validity refers to the quality or legitimacy of a study. In qualitative studies, validity is used to determine the worthiness of a study within social sciences. The concept of trustworthiness is a core pillar of qualitative inquiries, and most researchers advocate for it strongly. By integrating comprehensive data collection methods, researchers may strengthen the trustworthiness of their findings (Caretta & Pérez, 2019). I used a recursive data collection and analysis process to improve the study's validity. Moreover, validity may improve the accuracy of the data and build a consensus in the study. I utilized member checking to ensure the study's validity. Deficiencies in validity within a study may produce erroneous results (Rawson & D'Arcy, 2018). However, member checking may enhance the validity of a study. I also used data triangulation to bolster the study's external and internal validity. External and internal validity are used to strengthen a study's confidence in the generalization of the results (Crano, 2019). All the assumptions within the study were outlined and backed by scientific findings.

Dependability

In scientific research, dependability is achieved by replicating the study's findings when the variables are subject to the same conditions and yield the same results (Aguinis & Solarino, 2019). To ensure study reliability, I used systematic triangulation process and member checking. Natow (2019) suggested that triangulating patterns occurring within the study is achieved by analyzing data from various sources. Therefore, I located the recurrent themes within the study and compare my findings with available public records. Also, dependability gets rid of any bias within the study (Maher et al., 2018). I compared the interviewees' input against publicly available documents and organizational documents to confirm research reliability. I also subjected the study to a rigorous coding process. The emergent themes were compared to patterns occurred in the public documents. Secondly, I performed member checking to ensure the study's results are captured correctly. According to Caretta and Pérez (2019), researchers often exhibit a problematic tendency of summarizing findings, which introduces bias to studies. However, through member checking, the researcher restates their data gathering process in order to capture the data correctly and establish consensus. I cross-referenced the participant's transcribed input against their interview data.

Credibility

For this study, I used the member checking approach to enhance credibility. Credibility is used to demonstrate a study's transparency and win an audience's trust (O'Connor & Joffe, 2020). Member checking lowers the chances of research's respondents from collaborating their feedback. I conducted interpretive research using pragmatic design and also collected data from interviewees and quality secondary sources such as NIST documents and industry standards. Iivari (2018) noted that member checking helps mitigate subjectivity within the study. In addition, I used a rigorous screening process to enhance the study's trustworthiness. I also used data triangulation techniques to improve the study's credibility levels.

Transferability

In qualitative research, transferability alludes to the ability of the research findings or suppositions may be replicated into a larger population (Maher et al., 2018). In data security, transferability is essential in guaranteeing that the policies created may be instrumental in safeguarding a larger population. Triangulation may be used to improve transferability score of a study (McGrath et al., 2018). I analyzed publicly available data and participants' organizational data to ensure my findings may apply to a larger population. In my research, I did not rely on assumptions or generalizations in order to improve research transferability. I used a methodological triangulation approach to improve transferability. According to Natow (2019), the methodological triangulation approach integrates various methods to enhance a study's confidence. In essence, multiple methods are used to arrive at a similar conclusion thus eliminating instances of confusion. I used triangulation to obtain my results from the interviews, NIST documents, and other scholarly sources. Reviewing archival documents of internet security practices assisted in improving the study's transferability.

Confirmability

Confirmability is the criterion used to verify a study's trustworthiness (Haven & Van Grootel, 2019). It also alludes to the degree other scholars may agree with the study. Member checking is an ideal way of guaranteeing that the study's data is highly trustworthy. Secondly, I exhaustively analyzed every aspect of my study. Furthermore, I used high quality and credible sources within my study to improve its credibility. Finally, data triangulation processes used to ensure that my findings mirror the results of prior qualitative studies.

Transition and Summary

The use of online banking platforms has grown exponentially over the years. More users are now using digital platforms to carry out their financial activities. However, due to a lack of awareness, users are easily duped by attackers into revealing their credentials needed to access online banking solutions. This qualitative study assessed various ways adversaries gain access to user credentials using identity-based authentication attacks and the approaches to mitigate such processes. Data from the study may also assist financial organizations to counter identity-based authentication attacks.

Section 2 started by restating the research's purpose and justifies the reason for exploration. I also highlighted the research problem and defined the research methodology. The section 2 provided the details regarding the data collection, participant selection, and population sampling approach that were used. Using the qualitative pragmatic approach, I assessed the research's topic validity and exhaustively evaluate the research topic. The study's population comprised of IT security professionals working in banking organizations. I used a purposive sampling approach. In Section 2, I evaluated the major elements that are integrated into this study. I expounded on the study's population and also highlighted the role of the researcher. I also demonstrated that I am the study's primary data collection tool and highlighted the interviewing protocol that I utilized in this study. I used a semi-structured interview approach to gain better insight into the research topic. I included the various sub processes needed to collect data and determined its reliability. I used NVivo software to transcribed interview data and identify themes within the study. In section 3, I provided qualitative study overview, presentation of the findings, application to professional practice, the implications for social change, recommendations for action, recommendations for further research, reflections, and conclusion.

Section 3: Application to Professional Practice and Implications for Change

Overview of Study

The purpose of this qualitative pragmatic study was to examine the strategies IT security professionals working on internet banking platforms use to mitigate identity-based authentication attacks affecting digital privacy in online banking platforms. The study's target population consisted of IT security professionals with experience working in online banking from the northeastern region of the United States. The recruitment process was done via LinkedIn. A total of five participants were recruited for this study. Each participant's identity was encrypted to ensure the study maintains its integrity. The participants were interviewed via Zoom. After each interview, I conducted additional member-checking interviews to confirm the accuracy of the findings and gave the participants an opportunity to point out errors I made in my interpretation of the data collected.

Presentation of the Findings

The overarching research question of this study was, what strategies do IT security professionals use to mitigate identity-based authentication attacks affecting digital privacy in online banking? My process for responding to this research question entailed conducting in-depth semi-structured interview with IT security professionals with at least 5 years of online banking experience. In the semi-structured interview, my goal was to understand the various strategies used by banks to protect their customers, employees, and society from identity-based authentication attacks, how often they update their security policies, and how they handle suspect cases of identity theft within their banks. I reached data saturation when the data collected from the participants during the interview became repetitive and no new data were collected after the fifth interview. I also reviewed over 53 cybersecurity documents retrieved from governmental databases, newsletters, banking journals, and other publicly available records.

The participants were required to give their consent before beginning with the research study interview. I also notified them that their identities would be protected. I assigned each of the five participants a code to protect their identities: participant 1 was assigned P1, participant 2 was assigned P2, participant 3 was assigned P3, participant 4 was assigned P4, and participant 5 was assigned P5. Moreover, if the participants felt that I was asking intrusive questions they had the liberty to skip the question or leave the research study interview. I recorded each of the interviews in an audio format and took notes during the interview. I used NVivo to transcribe and analyze the data collected during the interviews. NVivo was used to identify the common occurring themes, identify subthemes, and check for their consistency. This study's conceptual framework was the PMT. Out of my analysis, there were five major themes that emerged: (a) comprehensive user authentication. (b) importance of data encryption (c) system audits (d) intrusion detection systems, and (e) comprehensive user policies. Each of the major themes comprised of other subthemes that I used to contextualize the main theme. Each of the major themes comprised of other subthemes that I used to scrutinize the main theme. I will cover the subthemes occurring under each theme. Table 1 highlights the major themes and the percentage occurrence rate.

Table 1

Major Themes Emerging From the Data Collection

	Participants		Documents	
Major themes	Count	% of response	Count	References
Comprehensive user authentication	5	100%	19	53
Importance of data encryption	5	100%	15	34
System audits	5	100%	19	51
Intrusion detection systems	5	100%	8	21
Comprehensive user policies	5	100%	11	24

In the analysis below, I cover all the five major themes; describe how they are linked to the literature, and explain how they are linked with the study's conceptual framework. Veale and Brown (2020) argued that cybersecurity covers a broad range of technical and social issues that must be put into consideration in order to protect networked IS. The major themes mentioned above seek to bolster the security of networked computing assets and minimize incidences of identity-based cybercrime. A comprehensive cybersecurity solution is comprised of a collection of tools, policies, concepts, risk management, and safeguards that can protect the assets. Many of the organizations that are actively digitizing their components fail to put in place security measures vital for long-term cybersecurity success. Using the PMT conceptual model, organizations can establish digital security mechanisms that will ensure long-term success. This study's findings were aligned with Section 2's literature review of this paper. In the sections below, I analyzed the five themes using the lens of the conceptual framework.

Theme 1: Comprehensive User Authentication

The first central theme identified was the importance of having comprehensive user authentication mechanisms. P1, P2, P3, P4, and P5 reported that there is a need for a thorough user verification process. P1 explained that it is paramount that bank platforms integrate the best data security practices such as user authentication to support digital privacy. P2 stated that banking platforms need to implement comprehensive authentication processes to secure their customer's bank accounts. P2 further explained that a holistic authentication mechanism can be achieved by streamlining the bank's external and internal processes. P3 pointed out that by implementing a comprehensive authentication protocol ensures that only the actual bank clients are accessing the bank's IS. P4 explained that they use comprehensive user authentication processes such as multi-factor user verification to enhance user protection. P4 further explained that tools such as machine learning and big data analytics are used to evaluate user behavior and protect the online banking user privacy. P5 pointed out that a comprehensive user authentication system should ban the use of common passwords. P5 also noted that legacy authentication systems should not be incorporated into banking systems as they introduce security vulnerabilities that may expose the users' digital privacy. P5 explained that user accounts with high privileges should have split responsibilities to minimize the chances of such accounts from being attacked.

Digital banking applications offer their users a convenient platform to transact with just a single click of a button, and it is crucial that these platforms keep unauthorized users from gaining access into protected resources. Shah and Kanhere (2019) described user authentication as the process in which a person's identity is verified as they attempt to gain access to a computing resource. User authentication is almost present in all human-to-computer interactions and is essential in safeguarding computing resources. Teh et al. (2019) pointed out that user authentication is the first line of defense of any computing system and is achieved via a knowledge-based verification mechanism. Basically, authentication technology grants a user access to system resources by confirming the user's credentials match those stored in the database. The vast proliferation of web-based devices in our society has driven the demand for more robust verification techniques. Typically, the process of user authentication is comprised of three critical tasks: identification process, verification process, and resource access authorization. Common resource access authorization methods to computer systems in use include password authentication (memorized secret) and the use of personal identifier numbers (PINs). However, these simple login mechanisms have their shortcomings and easily expose computer networks to external threats. More complex user authentication methods are needed to safeguard digital banking platforms against identity theft cases. P1, P2, P3, P4, and P5 suggested that enhanced login techniques could be integrated into digital banking platforms to counter identity-based authentication attacks. The following subthemes emerged in the data regarding the development of comprehensive user authentication methods. The sub-themes included one time passwords, time-based access control, identity detection and response, and multi-factor authentication.

Table 2

Subthemes Under Comprehensive User Authentication

Subthemes	Participants response	% Of Response
One time password	3	60%
Time-based access control	5	100%
Identity detection and response	4	80%
Multi-factor authentication	5	100%

Table 3

The Application of Information System Security Procedures and Policies in User Authentication

Data source	One time password	Time-based access control	Identity detection and response	Multi-factor authentication
Participants	3	5	4	5
Documents	7	7	7	7

The documents listed in Table 4 were used for triangulation and were downloaded from government-approved databases (www.nist.gov).

Table 3 shows that P1, P2, P3, P4, and P5 supported the use of multifactor authentication and time-based access control as policies to safe guard user authentication. P2, P3, P4, and P5 endorsed the use of identity detection & response and P2, P4, and P5 supported the use one-time passwords. Table 3 and 4 show seven documents support the sub-themes mentioned above.

Table 4

Interview Participants Who Have Implemented NIST Frameworks to Protect Their Online Banking Platforms

Government framework	Participants	Document page count
NIST 800-63B	P2, P4, P5	78
NIST 800-106	All	17
NIST 800-132	All	18

NIST 800-140E	All	9
NIST 800-218	P1, P2, P3, P5	36
NIST 800-214	All	45
NIST 800-210	All	53

The participants listed in Table 4 above used NIST frameworks 800-106, 800-132, 800-140E, 800-214, and 800-210 to improve user authentication policies and make sure the secured their digital banking platforms. They reported that they provided user training on safe authentication guidelines to their users at the beginning of their usage of the digital banking platforms. They also confirmed that the NIST guidelines improved system security by 99% by enhancing user authentication guidelines. Based on the data analysis, the following sub-themes were found to be essential in all of the participants application of the comprehensive user authentication guidelines.

One Time Passwords

P2, P4, and P5 emphasized on the use of one-time passwords at enhancing the security of digital banking applications. One-time password (OTP) is a verification mechanism that relies on the generation of a unique verification code that is sent to the user via their cellphone number. OTP scheme takes advantage of a two-factor authentication approach, making it difficult for attackers to access a computer asset. However, NIST classifies OTP as a single factor authentication tool that relies on the issuance of symmetric keys to a trusted third-party platform. OTPs rely on the use synchronous dissemination of tokens between the client and server to achieve device authentication (Sharma & Nene, 2020). OTP's verification process's primary goal is to establish trust between the service provider and the transacting entity. The recipient's key can only be accepted if it matches the sender's key and its time limit has not expired (Grassi et al., 2018). OTP's ease of implementation makes it an ideal user verification mechanism for banking platforms. Various modifications can be done to the OTP authentication scheme to enhance the mechanism's security. According to P2, "security strategies such as the implementation of OTP protection systems offer a holistic way of securing internal organizational infrastructure and external processes from malicious entities."

On the other hand, P4 said that they had adopted the use of OTPs to prove transactor's identity. P5 reported on the importance of personal identifiers in the implementation of user verification processes. OTPs issue out short block ciphers that act as authenticator tokens for computer networks. The authenticator code may be a 6-digit alphanumeric code that should changes after a set time period has expired. NIST has classified the implementation of OTP authenticators based on the integration technique. Table 4 below shows how the participants' input agreed with NIST's use of OTP authenticators.

Table 5

Interview Participants Who Have Implemented NIST Frameworks on the Use of OTP

Government framework	Participants	Document page count
NIST 800-63B	P2, P4, P5	78
NIST 800-106	All	17
NIST 800-132	All	18
NIST 800-140E	All	9

P1, P2, P3, P4, and P5 confirmed that they have integrated NIST 800-63B, NIST 800-106, and NIST 800-132 guidelines in their integration of OTP schemes to secure banking digital platforms. They reported that they suggested the use of OTPs to non-compliant financial institutions and sensitized their users on the importance on enabling OTPs on digital banking platforms. The participants also confirmed that OTPs are part of the core strategies in securing banking platform. They also aligned the application of the OTP strategies with NIST and other governmental data security guidelines.

The security of online banking platforms is critical to the wellbeing of a nation's financial stability. Weak digital financial safeguards can compromise a country's financial security in various ways (a) undermine the integrity of financial makers; (b) cause economic distortion; (c) lead to loss of revenue; (d) reputational damage; and (e) affect the control of money markets. Hence, there is a need for comprehensive verification protocols in the banking sector to protect a nation's financial wellbeing. Digital banking tools can integrate simple authenticator techniques to minimize cases of identity theft and thwart system infiltration by complicating access to digital resources. The study literature review supports this study's findings. Using the PMT theory, Vedadi and Warkentin (2018) argued that fear is a necessity when eliciting for behavioral change. Fear-based messages may be used to encourage the users of digital banking tools to enable OTP verification systems. Having weak authentication mechanisms exposes networked systems to external threats. Rogers (1975) stated that fear appeals exert attitude change in individuals and acts as protective stimuli. Teh et al. (2019) stated that the OTP authentication process involves four key parties, which are user, server, authenticator, and an attacker. PMT's fear-based messaging model may be used to ensure users are careful when engaging the authenticator platform thus minimizing the chances of successful system intrusion. IT security professionals may use fear-based messaging to coerce users into enabling OTP verification on their digital banking applications. The above literature review and study's finding align with the fear-based model of the PMT conceptual framework of this research.

Time-Based Access Control

In digital banking applications, access control is an essential component of security management. The bank's application needs to track the user activity during the session and restrict system access in case the user is inactive. Time-based access control systems allow for network management based on the user's access time or day. Time-based access control systems are implemented by specifying the time window or time range in which a user can carry out specific functions (Wang et al., 2019). The specific access duration is set by the IT security professionals by defining the time attributes users can be granted access into the bank's network. In addition, a time-based access list may be used to define the number of actions the users can execute during a particular window of time. For instance, IT security professionals may set conditions that prevent users from transacting large sums of money after midnight till morning. P2 stated that "The introduction of timed delays is essential in inhibiting cases of failed logins. Time delays are important because they thwart illegal system access in the event an attacker succeeds to exploits a user's password." Time-based access control systems utilize granular enforcement rules in permitting or preventing access to system resources to mitigate the risk of system breaches (Hu et al., 2018). Using P2 scenario, timed delays may prevent system intrusions by enforcing timed system delays. P2 further confirmed that IT security professionals restrict access to computer resources using time-based controls. In the event an attacker gains access into the system, the administrator receives an alert after the system flags illegal system session.

P3 reported that the bank may institute procedures that allow IT security professionals to assess the timeliness of internal controls. Evaluating the timeliness of transactions lets IT security professionals flag illegal access to system resources and streamlines control mechanisms in the bank. Nakamura et al. (2020) pointed out that authorized system users and applications may manipulate system resources when left ungoverned. Time-based access controls limit the freedom of authority, which authenticated devices possess when accessing system resources. Access controls enforce rule-based actions that are only valid at a specific time window. There are various variations of time-based access controls such as capability-based access control and traffic-based access control. In the two variations of time-based access schemes, the control systems prevent the illegal flow of information in the network by its users. In the event users exceed the predefined number of transactions set or system usage metrics, they are denied further access into the bank's network for a set period of time. Freezing access into the system lets the bank's IT security professionals review the flagged sessions and identify suspicious activities. Alternatively, a time-based operation interruption (TBOI) protocol may be enforced to prevent illegal flow of information. Nakamura et al. (2020) stated that TBOI protocol evaluates the flow of information and issues interruptions to late transactions. The protocol may be embedded in the bank's database to restrict access to information. The TBOI protocol provides better control of the time-based access system inputs that have been put in place.

P5 suggested that limiting access to system resources can reduce the severity of an attack. The participant stated that by allowing 1000 workers to have equal rights to access the database puts the system security at risk. In such a scenario, the 1000 users may be categorized as 1000 potential instances of vulnerabilities. To reduce the threat levels, the database administrator may limit access to the database by allowing a set number of users to access system resources. For instance, if only 10 people can access a system resource at a particular time, threat levels posed to the database application diminishes by 99 percent. P5 stated that access control is a pivotal system in protecting the bank's digital application from data breaches. P4 also noted that by setting up network access points may limit cases of system infiltration. Hu et al. (2018) reviewed the pros and cons of using time-based flow scheduling to optimize inter-data center communication. The researcher noted that access points may optimize data center inter-data exchange, which is vital for data hungry applications and customers. Service providers may deploy dedicated access control mechanisms to exclusively service system requests using time-based coefficient. Furthermore, a deadline-based model enables tenants to utilize the network resources based on a set-time frame. A completion time-based model decreases an application's functionality based on a set timeframe. For instance, when the user logs into the bank's digital platform and completes a number of actions, the application will automatically log out of the session forcing the user to log in again. A completion time-based model calculates the probability the user has concluded their activity and restricts further operations. Bank IT security professionals could utilize time-based access controls to optimize system security. Users flouting the bank's time-based measures may have their access rights restricted. In addition, the bank IT security professionals may issue strict time-based protocols design to improve information security. Giwah et al. (2019) stated that a growing of security problems are caused by the users failing to adhere to the best mobile data security practices. Limiting user access is one way of dealing with malignant user behavior. A time-based access control is an effective way of taking special measures against unauthorized system access. Users who fail to observe their time allocation to system resources will be blocked from utilizing the platform. This sub-theme aligns with the concept of issuance of threats, which is an integral part of the protection motivation theory.

This study's findings mirror the concepts included in the above literature review section. Giwah et al. (2019) explained that PMT conceptual model provides clarity to the user by using fear appeals. The theory encourages the use of persuasive communication to mediate behavioral change. Users change their behavior by perceiving threats from their surrounding and look for ways to mitigate threats. van Bavel et al. (2019) explained that IT security experts and researchers noted the greatest hurdle to effective cybersecurity administration is user behavior. Rogers proposed that fear may be used as stimuli to institute behavior change. In this case, fear-based messages used in the time-based access model can invoke associative emotional responses making users to be increasingly cautious while using digital banking platforms. Nakamura et al. (2020) noted that time-based access controls may allow IT security experts to manipulate resource utilization. The researchers agree that system warnings may force users to change access behaviors from the system's tenants. Warnings cause the users to become increasingly careful when accessing system resources thus resulting in fewer data breaches. Findings on the implementation of time-based access control systems may be use in the digital banking platforms. P2, P3, P4, and P5 recommended the implementation of the NIST 800-63B framework in access control as part of the user authentication policy. The literature review and study's findings are aligned with use of persuasive messaging attribute of the PMT conceptual framework.

Identity Detection and Response (IDR)

Detecting compromised identities is a major challenge digital banking platforms face. The detection of fake identities happens in real world verification and in the virtual environment. The use of fake identities has become quite rampant as more users look to protect their identity. Today, the creation of fake accounts is mainly viewed from an economic perspective such as money mules, money laundry, phishing, and spamming (Monaro et al., 2018). Considering the weaknesses of online security, the issue of fake identities becomes increasingly complex to resolve. User authentication approaches can be easily bypassed in case a system user personal information fall into the wrong hands. If problems shrouding identity detection are not addressed, then it becomes increasingly difficult to ascertain a user's true identity. Different studies have shown that true system users can be distinguished from users using faked identities by analyzing truth features in their responses (Monaro et al., 2018). For example, a person using a faked profile may have trouble answering personal questions and will always give shorter answers compared to original accounts. With the proliferation of fake accounts, banks are increasingly embracing the use of identity detection and response systems.

Identity detection and response is a security strategy that involves on the use of identity-related information to protect critical infrastructure against infiltration, system compromise, and detecting attackers. IDR does not focus its efforts solely on user authentication, but serves to protect the user's credentials, system entitlements and system management (Bernerth et al., 2021). Financial platforms such as banks and ecommerce platforms periodically request their users to upload verification documents to detect compromised profiles. IDR OnDemand request for verification documents integrates techniques such as the request for a selfie with the user holding current newspaper, current bill, rent notice, or tax return forms responses (Monaro et al., 2018). The request of sensitive details helps organizations detect, mitigate, and recover from advanced persistent threats. NIST has issued cybersecurity measures and guidelines that incorporate the best practices in the request for best data (Moreira et al., 2021). NIST 800-135 guidelines provide management standards in the management of data to protect the user's confidentiality, integrity, and availability in resilient systems. NIST 800-157 provides additional guidelines for the verification of personal user identities credentials. It offers organizations with technical guidelines for setting up interoperable and secure public key infrastructure (PKI) in processing user credentials. These guidelines are instrumental in protecting the usage of personal identity verification documents by organizations.

P1, P2, P3, P4, and P5 argued that requesting for identification documents is a vital approach they used in mitigating cases of identity-based authentication attacks. P1 explained that both the customers and bank officials are required to verify their identities in order to carry out transactions with the bank. In addition, the verification process applies to customers utilizing both online and legacy transaction systems. The dual identity verification approach is among the five paramount security practices adopted by the bank. Participant also pointed out that the bank regularly informed the customers when introducing new security policies and measures. Monaro et al. (2018) pointed out that consistent communication with the customers is an instrumental approach in detecting faked identities. Truth analyzing techniques may be integrated into identity detection features to detect deviant responses. For instance, perpetrators typically give shorter answers when they are being interrogated, whereas truth tellers give longer responses. Criminals purposefully give short answers to prevent the observer from detecting their lies. A cognitive-based lie detector system can capitalize on this technique to detect fake profiles.

P2 stated that bank users are required to submit identification documents for verification. The banks verification process does not stop after the initial document request, but users are also required to provide additional information regarding the source of the funds. The request for additional information arises after the bank’s system flags an account’s activity. Moreover, P2 educates bank customers why the financial institution keeps on requesting for additional verification information. NIST 800-85B and NIST 800-85B-4 guidelines emphasized that organizations must educate end-users on the importance of the personal identification and verification process. Enlightened users are increasingly willing to share personal data after understanding the benefits of such practices. Özmen and Yucel (2019) pointed out that the emergence of online platforms has dramatically changed people dilemma for information usage. More people are interested in the intricate details pertaining information usage. People are demanding for concrete proof in their search for information. Conversely, bank users are more likely to investigate the bank's data usage sharing practices. Transparency is key in promoting user confidence. P2 suggested that informing the consumers about their institution's request for personal data is essential in combating cases of identity-based fraud. Educated users are more likely to comply with the bank's request for verification documents.

P3 mentioned that they have integrated identity exposure (IVE) and identity detection and response (IDR) systems to guarantee data security in their banking platform. IDRs and IVEs systems create comprehensive databases containing personal identifiable information to combat identity-theft (Monaro et al., 2018). These systems use a variety of techniques to secure corporate systems against fake profiles. Monaro et al. (2018) noted that techniques such as keystroke analysis, cognitive-based lie detectors, autobiographical implicit association test (aIAT), and Concealed Information Test (CIT-RT) are used to evaluate a user's memory detection and flag fake user identities. According to the study's results, people with faking identities will have a hard time beating the memory-retention techniques mentioned above. IDR systems analyze a user's metadata and use control questions to flag profiles. Integrating IDRs and IVEs may be used as a fear-arousing tools to deter identity theft and associated attacks.

P4 explained if a customer's identity is compromised, the customer is notified and recovery measures are instituted in the said account. Account recovery measures mainly require the afflicted party to verify their identity. Moreover, participant P4 pointed out that their bank's digital platform users are required to prove their identities before they are allowed to transact on the platform. Consumers who fail to comply with the bank's platform are not allowed to transact with the bank. Such statement can be viewed as a fear-invoking message. Essentially, consumers who cannot verify their identities are not allowed to use the platform. Participant P5 stated that they review their customers and employees' registration using an ID verification process. P5 also explained that they use a combination of facial and identity authentication technologies to ascertain the users' identities are not compromised. A real-time identity verification process has been implemented to deter attacker from infiltrating the organization's systems. P5 also encourages users to create a financial-only email address to optimize the identity detection process. A financial-only email address will reduce the user's digital footprint minimizing the exposure to phishing attacks.

The findings on identity detection and response (IDR) subtheme supports the integration of self-protective strategies adopted by users in handling threats. Identity verification is an evasive strategy implement by financial organizations to deter system intrusion. The persuasive messaging integrated into identity verification processes used by banks cause users to be extremely protective of their credentials. Ogbanufe and Pavur (2022) pointed out why individuals maladaptively and adaptively respond to the threat of identity theft. An individual's reflection on the negative events associated with identity-theft cause the individual to be increasingly motivated in protecting their credentials (Ogbanufe & Pavur, 2022). The anticipated regret associated with identity-theft is effective in reducing maladaptive coping responses the individual may exhibit. Bax et al. (2021) explained that in threat appraisal, an individual assesses the perceived threat and their perceived vulnerability to it. The individuals also reviewed the perceived reward associated with not taking evasive measures against the threat to determine the seriousness of the situation. The seriousness of falling victim to phishing attacks forces users to be highly invested in the identity verification process (Shahbaznezhad et al., 2020). According to Korać et al. (2021), the security management of user identities by digital systems is improving user security behavior. IT security professionals are educating their users on the importance of user authentication and verification. Consumers should always take the appropriate steps to protect the identities at all times. The literature review for this research study and participants contribution on identity detection and response were aligned with the attributes of the PMT conceptual framework.

Multi-Factor Authentication (MFA)

P1, P2, P3, P4, and P5 emphasized on the importance of enabling multi-factor authentication methods on digital banking platforms. The participants were able to assess the security flaws present in legacy authentication systems and recommended the use MFA as a great defense system. They further described how legacy authentication systems may led to the loss of customer data in digital banking system. P1 explained that online banking systems require at-least a two-factor authentication system to verify the identity of the consumers or employees accessing the bank's digital resources. The need for comprehensive user verification is a pertinent issue in the banking security. Mehraj et al. (2021) stated that users commonly forget their passwords and are forced to reset them by websites. Typically, the password retrieval process is straightforward with user responding to a security question or submitting the details for an alternate email address. Mehraj et al. (2021) pointed out that such a multi-factor authentication system is vulnerable to attacks and is ineffective. The researchers explain that MFA practices should take advantage of PMT's adaptation technique to institute stronger authentication techniques. Adaptation assessment of the MFA should focus on building user confidence. P2 MFA authentication mechanism attempts to reinforce user confidence by requiring both consumers and employees to use multiple layers of security in verifying their identities.

P2 reported that they have implemented multiple strategies to protect user privacy at the financial institution they work with. One strategy is enabling the use of multiple methods of authentication for users accessing the online banking platform. MFAs are user authentication approaches that require the use of two or more independent verification techniques. Examples of MFAs include captcha tests, user smartphone's verification action, fingerprints, biometrics, facial recognition, and voice recognition (Wu et al., 2019). Ometov et al. (2018) pointed out that as the world becomes increasingly interconnected, organizations must embrace the use of multi-factor authentication methods. Multiple methods of authentication or MFAs have become a much more flexible and secure way of verifying user authentication. MFAs can be categorized into three distinct groups, which are knowledge factor, biometric factor, and ownership factor. According to Ometov et al. 2018, in knowledge factor, the verification process tests for something the user knows. Biometric MFA checks the user’s biometric data or behavioral patterns. In ownership MFA factor, the verification uses a third-party device that has been proven to belong to the user such as phone, card, or electronic device. P2 stated that their digital banking platform utilizes the above strategies to improve user access security. PMT offers users a hypothetical structure for analyzing the protection of end-users. Individuals have the responsibility of determining the most important predictors of their security.

P3 described the strategies they have put in place to enable digital privacy in their organization. P3 stated that they have implemented the multi-factor authentication protocol to ensure that only the bank’s actual clients have access to their banking information. Additionally, the system only allows users to setup their passwords in an Alphanumeric format. The integration of the two security techniques makes it difficult for attackers to compromise user accounts within the bank. Mousavi et al. (2020) demonstrated that privacy and data security concerns have a significant impact on the user’s coping appraisal. MFA and the usage of complex passwords have an effect in immediate emotional state. PMT further discouraged individuals from engaging in risky behavior such as having a weak password or using a weak authentication mechanism as their bank accounts only safeguard. By combining the two protocols, participant reassures the bank’s customers of their safety.

P4 also disclosed that they have developed and integrated digital security systems that utilize the multi-factor user authentication protocol. The participant further described that machine learning and big data analytics tools have been integrated into the authentication protocol to evaluate consumer behavior and enhance user privacy. Ng et al. (2021) highlighted the importance of PMT in resolving security-related motivation. As an increasing number of banks experiencing cyberattacks, it is imperative that IT security professionals motivate their users to embrace the use of secure authentication protocols. P4 approach of integrating MFAs and data analytics approaches is crucial in creating security awareness against cyberattacks. P4's data analysis approach may assist them to evaluate the individual reactions to maladaptive rewards. Moreover, they can evaluate an individual's coping appraisal process and behavioral changes to cybersecurity threats. Insights from the data analytics may be instrumental in encouraging the adoption of security behavior.

P5 explained that they work as an IT security engineer and oversee the use of multifactor authentication systems to grant users access into their digital banking platform. The participant described how the enforce MFA integration into their system. Users are required to answer security questions and have the option of creating dual accounts for users with high system privileges. According to P5, higher privileged account holders need multiple accounts to reduce the chances of such accounts falling into the hands of hackers. Lower privileged accounts will be used to handle simple administrative tasks such as replying to emails and less critical work. People exhibit some level of cognitive bias when subjected to threats resulting in long-term behavioral change

(Daniel et al., 2020). Therefore, P5's use of fear appeals ensure C-suite users use different accounts to carry out our administrative tasks. The instances of MFAs cognitive bias will force users to make significant system usage.

My literature review support's this study's findings. Using the PMT conceptual theory, Mehraj et al. (2021) stated that MFAs fear appeals may be used to boost the trust levels people have on computer networks. The five participants encouraged user's trust levels on digital banking by enforcing MFAs as the primary authentication mechanism. They suggested that MFAs practices can be used in collaboration with other data security practices to improve digital banking data practices. Users who fail to integrate MFAs on their accounts are highly susceptible to attacks. This use of fear appeals seeks to change the perspective of bank clients on digital and encourage users to adopt the use of multiple authentication approaches. The above literature review and study's findings aligned with the fear-arousal and use of evasive procedures of the PMT conceptual framework of this research study.

Theme 2: Importance of Data Encryption

The importance of data encryption was the second theme arising from the data analysis. Stewart and Jürjens (2018) noted that most financial institutions are under extreme pressure from the customers and governmental bodies to secure their data. The researchers further pointed out that banks have adopted disruptive technology to optimize lending mechanisms. However, in order to continue exploring technology-based opportunities, banks need to reassure their customers that their data is safe. The process of adopting FinTech has to be in compliance with modern data security trends. NIST has created guidelines to promote data security, such as the NIST 800-11 guide for storage encryption technologies for end-user devices. P1, P2, P4, and P5 described the approaches to ensuring data security through data encryption. Two subthemes arose from the input, which are database encryption and encryption of communication channels.

P1 explained that one of the strategies they use to protect their platforms against security breaches is through the use of encryption tools. P1 noted that data breaches are a dreaded occurrence in the world of digital banking. It is important that IT security professionals protect their systems by implementing encryption technologies on their platform. P2 noted that data encryption is a preventative strategy against data breaches. According P2, encryption makes data unusable to the attacker in the event of a data breach. P4 stated that they use encryption protocols such as AES symmetric encryption as a defense mechanism against data breaches. P5 pointed out that they regularly update their encryption protocols to secure customer data and transaction records.

The P1, P2, P4, and P5 feedback on the use of preventative measures above aligns with the PMT theory. Hackers act as external threat stimuli seeking to exploit a bank's networks and steal consumer data. By enforcing evasive measures such as encryption tools, IT security specialists minimize the negative impact of data breaches. Implementing encryption protocols may be viewed as a response to fear appeals, which aligns with the evasive actions of the PMT conceptual model.

Table 6

Subthemes under the Importance of Data Encryption

Subthemes	Participant Response	% Of Response

Database Encryption	4	80%
Encryption of communication channels	4	80%

Table 7

The Application of Encryption Procedures in Digital Banking

Data Source	Database Encryption	Encryption of communication channels
Participants	5	4
Documents	5	5

The documents listed in Table 8 were downloaded from government-approved databases (www.nist.gov), and were used in the triangulation process.

Table 8

Interview Participants Who Have Implemented NIST Frameworks to Protect Their Online Banking Platforms

Government Framework	Participants	Document Page Count
NIST 800-38G	All	54
NIST 800-66 Rev 2	All	17
NIST 800-111	All	18
NIST 800-140E	All	9
NIST 800-214	All	45

P1, P2, P3, P4, and P5 reported in Table 8 that they used NIST guidelines that specify the use of encryption protocols in their digital banking platforms. They reported that encryption protocols improve the security of their platforms and confirmed that the systems were 95% less susceptible to cyberattacks. Their encryption procedures aligned with NIST framework.

Database Encryption

It is also referred to as data-at-rest encryption. Stewart and Jürjens (2018) pointed out that data-at-rest within a bank's infrastructure poses complex security risks to the bank and end-user. Cyberattacks can be viewed as intelligence gathering missions, and data-at-rest is easy to exploit. The most reputable approach to securing such data is through the application of encryption technologies. NIST 800-38G, NIST 800-66 Rev. 2, and NIST 800-111 provide guidelines for the application of data encryption principles on databases. Ng et al. (2021) stated that compromised personal data and violations of the individual's privacy are some of the security threats that should make IT security professionals to change their data protection behavior. As a result of the threat appraisal process, IT security professionals should enforce strict data-at-rest encryption techniques.

P1 mentioned in the interview that they ensure all digital databases are encrypted to establish a secure banking infrastructure. P1 further explained that data encryption is also an effective strategy against data breaches as it safeguards all the data stored by the bank. The application of data encryption was aligned with NIST 800-111 framework. P1 expounded on the importance of encrypting the customer's data as it makes it harder for hackers to utilize the data in the event of a successful data breach. Stewart and Jürjens (2018) stated that data breaches are common in FinTech. Encrypting databases safeguards the information in case it falls into the wrong hands. P2 explained that one of the strategies they have put in place is the encryption of the database. P2 further stated that encryption is a security measure that makes data unusable to the perpetrator unless they have the encryption key. P2 continued to expound that some attackers are predominantly interested in sabotaging organizations. Data encryption fools proofs the bank's database against data corruption techniques. Checksum techniques embedded in encryption algorithms guarantee data integrity in databases (Jung et al., 2019). NIST 800-38G guideline also specifies the application of encryption to ensure data protection. Taking protective measures is in line with the PMT motivation theory.

P4 mentioned that they use different encryption techniques as preventative strategies against data breaches. For instance, P4 has implemented the advanced encryption standard (AES) symmetric encryption model to encrypt data within the organization. P4 also monitors the network for intrusions and enforces preventative measures to protect the customers' data confidentiality. According to Jung et al. (2019), modern data encryption algorithms offer file-level and data-level data integrity protection. P4's approach to integrating the AES approach maximize data recovery approaches in the event of data breaches. P5 also stated they request to update the encryption system utilized by the organization regularly. By constantly updating the bank's encryption techniques, the organization manages to seal data leaks that may be presented by the use of a weak encryption algorithm.

This study literature review supports the study's findings. Johnston and Warkentin (2010) mentioned that response efficacy is a critical characteristic of the PMT conceptual model. The existence of external stimuli such as hackers force IT security professionals to adopt data encryption as a strategy against data breaches and guarantee the customer's digital privacy. The PMT theory has been effective in enhancing the efficacy of security strategies enforced by IT security professionals. P1, P2, P4, and P5 are motivated to protect their user's data at rest by implementing database encryption principles. Jung et al. (2019) noted that algorithms such as data encryption standard (DES), advanced encryption standard (AES), and data encryption standard extended (DES-X) offer high-performance cryptographic tools to IT security professionals. Stewart and Jürjens (2018) pointed out that the adoption of mobile financial technologies into the banking sector presents significant risks to users. The application of a data-at-rest encryption algorithms such as AES and DES helps win over the consumer's trust (Matta et al., 2021). By responding to fear appeals, IT security professionals are utilizing the philosophy behind the PMT conceptual model. The literature reviewed for this study and the findings of this study are aligned with the conceptual model of the PMT.

Encryption of Communication Channels

End-to-End encryption is mainly applied data security principle in data communication. End-to-end encryption ensures data on transit maintains its confidentiality, integrity, and availability (CIA) properties during transmission. As the volume of big data continues to grow, IT security professionals must ensure their consumers' right to privacy is observed. The NIST 800-11 guide for storage encryption technologies for end-user devices has created a comprehensive guideline that guarantees CIA properties. As the demand for digital applications grows, organizations must ensure they comply with the NIST 800-11 and ISO/IEC 27000 data privacy guidelines. P1, P2, P4, and P5 demonstrated that their institutions support data-on-transit policies currently enforced by the government and other standardization bodies.

P1 pointed out that their bank's application utilizes various encryption techniques to protect consumer data against data breaches. P1 reported that their company uses algorithms to hash information on transit and aligns with the NIST 800-11 end-to-end communication encryption guidelines. P2 explained that hackers are interested in corrupting the bank's data in some instances. P2 stated they use data encryption techniques to maintain the integrity of the data-on-transit. Data-in-transit is highly susceptible to user manipulation. For example, a hacker may rebuild the contents of a message by using network listening tools to intercept unencrypted data packets. P2 stated that by encrypting communication channels, hackers will have a harder time interfering with the bank's communication channel. P2 reported that firewall software is used to protect their institution's network. Moreover, the firewall applications may be used to filter out illegal users accessing the bank's system. Kamoun-Abid et al. (2021) explored the techniques utilized by firewall software to make cloud-based communication more secure and block incoming intrusions. The researchers noted that firewalls employ end-to-end encryption technologies to filter out malicious data requests by unverified applications. P2's application of firewall applications aligns with the NIST 800-11 encryption guideline. P4 pointed out that they had taken the appropriate steps to secure their networks by implementing data security principles. Furthermore, the network is monitored to detect any instances of data breaches. In their study, Jung et al. (2019) stated that end-to-end encryption tools can be used to monitor networks to reveal patterns, trends, and associations in regard to user behavior and interaction by security experts. Analyzing user patterns and trends may be integral in the application of the PMT theory. P5 explained that they have put an encryption system to secure transaction data in place. Bank network communication is highly susceptible to man-in-the-middle attacks. Enforcing end-to-end data encryption minimizes the chances of an attacker deciphering the bank's communication.

End-to-end data encryption skills are associated with the PMT theory. According to Johnston and Warkentin (2010), taking evasive measures is a component of the threat and coping appraisal process. Enforcing data security principles on the bank's network is designed to motivate users to communicate with the application. Digital banking customers are more likely to trust a NIST 800-11 and ISO/IEC 27000 complaint platform than unsecured currency exchange platforms. Projects on newer and more robust data encryption technologies are currently being finalized. For example, the influence of end-to-end encryption in blockchain technology is transforming digital finance. The implication of this theme is that more users gain trust and transition to digital banking platforms. The above literature review for this study is aligned to the adaptive and maladaptive changes in user behavior present in the PMT theory.

Theme 3: System Audits

Given the impact of data breaches, it has become critical for financial institutions to manage the risks associated with digital banking platforms. Carrying out system audits is integral to security awareness in the banking sector. Security audits help banks secure their data, identify security loopholes, identify gaps in their policies, and evaluate the effectiveness of a security strategy. IT security professionals understand that conducting regular audits can help ensure that the bank employees and other system users are following the set security practices. In addition, security audits determine the compliance levels a system has in regard to information regulations. Security audits assist organizations and IT security professionals evaluate the effectiveness of their security strategies.

P1 explained that they perform internal audits to assess their organization's compliance to user privacy guidelines. P2 pointed out that results obtained from the audits enables senior management find ways to strengthen the bank's data privacy such as the purchase of security software. P2 stated that their firm uses security audits to ensure their organizations follow laid out data governance guidelines. P2 also pointed out they use security to determine the system user's roles and how they may create conflict or trigger breaches. P3 explained that they use an audit checklist to evaluate the adequacy, reliability, and effectiveness of the bank's system internal controls. P3 noted that security audits are necessary in maintaining a risk-free, compliant, and streamlined IT environment. P4 pointed out that they use ISO standards as an audit guideline that assists their organization determine weaknesses within the system. P4 explained that in the event the system exhibits vulnerabilities, security patches are applied to the system. P4 pointed out that they use computer-assisted audits to determine their bank's compliance levels with payment data security standards used by financial institutions.

Audits offer financial institutions a proactive way of addressing potential threats present within the system. Essentially, audits give IT security professionals a different focal point for assessing unknown agents who pose a significant danger to the organization's IS. The use security audits align with PMT's conceptual model on use of adaptive response mechanisms to invoke protective measures. Ogbanufe and Pavur (2022) noted that adaptive response to threats is an essential component of the PMT model. The above literature review aligns with preventative measures of the PMT model reviewed in this study. The security audit them had two subthemes occurring, which included internal audits and compliance audits.

Table 9

Subthemes Under the Importance of Carrying Out System Audits

Subthemes	Participant Count	% Of References
Internal Audits	5	100%
Compliance Audits	3	60%

Table 10

The Application of System Audits in Digital Banking

Data Source	Internal Audits	Compliance Audits
Participants	5	3
Documents	3	3

The documents listed in Table 11 were used for triangulation and were downloaded from government-approved databases (www.nist.gov).

Table 10 shows that P1, P2, P3, P4, and P5 agreed that they perform internal audits on their digital banking platforms using various NIST frameworks. P2, P4, and P5 also review their systems using NIST compliance documents. Table 10 and 11 show that 3 NIST documents support the sub-themes above.

Table 11

Government Framework	Participants	Document Page Count
NIST 800-53 Rev 5	All	70
NIST 800-123	P1, P2, P4, P5	44
NIST 800-115	All	68

Table 11 above shows us that P1, P2, P3, P4, and P5 used NIST framework 800-53 Rev. 5 security and privacy controls for Information Systems. The NIST document provides a comprehensive control list for IT audits. It provides security catalog for organizations auditing their assets, individuals, other systems, and governmental services from a diverse set of risks and threats. P1, P2, P3, P4, and P5 used NIST 800-115 technical guide to Information security testing and assessment as part of system auditing process. Moreover, ISO 19011 guidelines were also used in the IT infrastructure audit process adopted by the IT security professionals. ISO 19011 contains instructions for IT security experts evaluating management systems.

Internal Audits

Cybercrime can have detrimental effects on the stability of a financial organization. The direct economic impact a financial organization experiences due to data theft, asset misappropriation, disruption of services and legal fees may cripple the bank's operations (Slapničar et al., 2022). Consequently, cybercrime can indirectly impact the status of a financial institution's information system, leading to the disclosure of sensitive information, affecting the implementation of internal policies, and reducing consumer trust in the banking platform. Steinbart et al. (2018) noted that carrying out internal IT audits helps organizations identify potential vulnerabilities and mitigate an attack's impact. Internal audits act as a risk management mechanism and safety control mechanism. Using the PMT conceptual model, internal audits can be compared to the threat appraisal process. IT audits also improve efficiency levels in service provision within the bank. They help create awareness of the status of the IT infrastructure. All the participants suggested that they conduct internal IT audits to optimize digital privacy within their organizations.

P1 reported that they use audit trails as a digital privacy implementation strategy. In data security, the act of reviewing data logs sequentially is referred to as audit trailing. Audit logs typically arise from transactions carried out within the IT infrastructure. The chronological process of analyzing records or the source of records helps document evidence of any attacks or malpractices within the organization. NIST framework 800-53 Rev. 5 contains a comprehensive outline that assists IT security professionals conduct system analysis. The sequential nature of the audit trail helps determine if two security-related events resulted from a related event. For instance, financial organizations are easy targets of denial-of-service (DOS) attacks. An audit trail may determine which IP addresses the attack originated from and the details from the analysis used to prevent a similar attack (Slapničar et al., 2022). Audit trails furnish the reviewer with the progressive buildup of events, thus indicating where the infringement occurred. P2 explained that they carry out internal audits to determine user responsibility and roles in their organization. IT administrators typically split user roles within their systems to minimize instances of data breaches. Moreover, splitting user roles reduces conflicts in user management. P2 pointed out that their internal audit process involves reviewing the data using top-down and bottom approaches to determine the condition of the organization's system. P3 reported that they verify if internal procedures adopted by the bank are in accordance with an internal checklist. P3's audit process involves checking the organization's internal controls' adequacy, reliability, and effectiveness. The participant's internal review process is in accordance with NIST 800-53 framework. In addition, P3 said that if the internal controls have discrepancies, they usually streamline the rules to satisfy external data guidelines. P3 further stated that the role of an IT security professional is to maintain risk-free and efficient IT infrastructure.

P4 said that they conduct regular system audits to ensure their IT infrastructure meets data security standards. P4 further explained that they monitor the network to detect any attacks and check if any successful breach has impacted their organization. If their system yields information of an attack, they notify the bank's users and take corrective measures. P4 also explained that they ensure their users' privacy by observing international data compliance standards such as international organization for standardization (ISO) and NIST 800-11 data security guidelines. P4 also stated they review current security procedures to ensure their staff follow the laid-out guidelines. Preventing internal data breaches is vital in maintaining the network's integrity. Yen et al. (2018) reported that the effectiveness of internal controls of an IT system plays an essential role in preventing data breaches. Ineffective data auditing methods often attract external agents, thus introducing additional information risks. The threat of an external audit review forces IT security professionals to be thorough with their analysis (Pedrosa et al., 2019). P5 explained that they use computer-assisted auditing techniques (CAAT) to establish a robust review process. P5 reported that the CAAT reports help them determine if the bank is adhering to ISO data privacy and security practices. P5 also ensures their digital platforms are following payment card Industry data security standards (PCI DSS) guidelines. In the event the organization fails to meet the set guidelines, then P5 patches the system to ensure it satisfies the laid-out guidelines.

The findings of the internal auditing process support the notion of an individual reacting in a self-protective manner towards a perceived threat. Johnston and Warkentin (2010) stated that risk avoidance is an integral component of the PMT conceptual model. By conducting internal system audits, the IT security experts evaluate their digital payment platforms for flaws and determine the risk levels present in the system. When risks within the system are noted, the IT security professionals can rectify the mistake before attackers take advantage of the exploit. A pragmatic approach requires professionals to address problems or issues with rigour and vigour. Steinbart et al. (2018) in their study highlighted the importance of extensive system audits. The researchers pointed out that investigators should use multiple perspectives to analyze problems to develop definitive solutions and improve internal controls. IT managers use internal audit processes as a non-formal measure of compliance. The literature review for this research is aligned with the self-protective attribute of the PMT framework.

Compliance Auditing

Compliance auditing was the second subtheme that highlighted the importance of system auditing. As the demand for digital financial applications grows, it is crucial that IT vendors ensure their solutions are stable, well maintained, and use the relevant data security applications. Rikhardsson et al. (2019) explained the importance of standardized technology integration in the financial sector. Technology-based solutions are subject to governmental regulations in order to protect the consumer from exploitative practices adopted by private firms. With IT vendors incorporating a wide array of technologies into their applications, it is vital that digital solutions are subjected to market regulations to allow for fair treatment of consumer data. According to Antunes et al. (2022), compliance regulation is an evaluation technique that establishes whether a product meets predefined standards set by the government or standardization bodies. ISO 27001 and NIST SP 800-53 Rev. 5 are some of the significant compliance guidelines focusing on the integration of digital technology into the banking sector (Weil, 2018). These documents propose predefined controls and the corresponding mitigation techniques.

P1 said that audits were performed to evaluate the safety and reliability of the information data storage and processing systems. The results of the compliance audits are then shared with the senior management to discuss areas the bank needs to strengthen or make interventions. The IT security team also performs compliance audit when the organization upgrades its information system or integrates a new security solution. P2 explained that they conduct compliance audits to ensure that their organization follows data governance principles. Compliance audits performed by P2 determine the information system's accuracy, limitations, and data protection standards. Participant P2 takes the appropriate steps to ensure they have secured their client's data. P2 confirmed that they implemented NIST SP 800-53 Rev 5 and ISO 27009 standards in their organization. P3 reported as an IT security professional they are tasked with the mandate to ensure that their online banking platform adheres to existing banking regulations. P3 expounded that they make sure new technology implemented by the bank satisfies a set checklist involving the application's adequacy, reliability, and effectiveness. Their goal is to ensure digital technologies present a minimal data security risk to banks and consumers. P4 reported that they use standards set by the international organization for standardization (ISO) and payment processors to determine the bank's digital platform's compliance levels. Participant P4 carries out additional penetration testing to assess their information system's areas of weakness. P5 stated that they use computer-assisted logging techniques to evaluate their bank's compliance levels. All five participants confirmed that they had applied the above mentioned guidelines while inspecting their information systems for compliance. The application of these guidelines is vital for the successful risk management of the bank's IT infrastructure.

Evaluating an information system for compliance is a necessary threat appraisal process that aligns with the PMT framework. The PMT theory is comprised of two fundamental dimensions, which are threat appraisal and coping appraisal. In other words, an individual's protection motivation behavior is influenced by fear (Srivastava et al., 2021). Security breaches in the financial sector affect a firm's operations and trigger financial losses. Conducting compliance audits assists financial organizations to protect themselves from common attack vectors plaguing the information security industry (Steinbart et al., 2018). Therefore, compliance testing is an ideal threat appraisal process that assists digital payment platforms to secure their systems or reducing the severity of an attack. A compliance audit helps an organization evaluate the perceived vulnerability and severity an attack poses. Srivastava et al. (2021) stated that the threat appraisal process modifies an individual's response efficacy and self-efficacy. By conducting compliance tests, IT security professionals can quickly determine a system's weak points and can counter cyberattacks targeting the system. The literature review and participant responses on carrying out compliance auditing align with the threat appraisal and coping appraisal attributes of the PMT conceptual framework.

Theme 4: Intrusion Detection Systems

Having defensive tools to detect and prevent cyberattacks was the fourth theme found in the participant's responses. Advances in technology coupled with growth in the global digital payments have stimulated the demand for means to detect cyberattacks and other protective measures. Agarwal and Hussain (2018) explained that the rise of web-based applications such as e-banking, e-commerce, and social networking platforms has necessitated comprehensive web security applications. These applications deal with sensitive user data and operations, it is imperative that they are protected. For attackers, exploiting these applications seems easy and ideal targets to perform their unlawful acts. Bland et al. (2020) stated that information systems security officers can minimize vulnerability to cyberattacks by implementing the right defense strategies. Vasilomanolakis and Mühlhäuser (2018) noted that intrusion detection systems (IDS) and intrusion prevention systems (IPS) offer a sophisticated way of detecting and countering cyberattacks. These systems make use of a plethora of monitor and shield computer networks.

NIST 800-123, NIST 800-95, and NIST 800-39 are comprehensive guidelines that assist IT security managers in managing information system risks and integrating middleware. The guidelines significantly reduce the complexities associated with the integration of IDS and IPS systems. P1, P2, P3, P4, and P5 pointed out that they have implemented intrusion detection systems into corporate networks to improve data security. P1 reported to have implemented security protocols such as firewalls to protect the bank's internal IT infrastructure from external threats. According to Agarwal and Hussain (2018), web application firewalls (WAF) are organizations' most popular defense mechanisms to protect their IT systems after deployment. Firewalls operate by rules and defend applications against sequential attacks. For instance, a firewall application will quickly detect a denial-of-service (DOS) attack and quickly filter out the IPs used by the attackers. P2 stated that they use firewall applications to control network traffic and restrict illegal system access by allowing only authorized system users. IDS use signature-based authentication and anomaly-based techniques to detect abnormal user behavior. For instance, cybercriminal may attempt to access the bank's database and copy confidential information within the organization. In such a scenario, the IDS system will report the illegal system access and block the user from further downloading sensitive files. P3 pointed out that they have integrated identity detection and response tools to prevent unlawful system access as an illegal system utilization strategy. In the event of an attack, P3 blocks compromised accounts from further transacting. P4 explained that they use machine learning and big data analytics tools to analyze consumer behavior in order to detect data breaches. Bland et al. (2020) noted that cyberattacks are becoming increasingly complex, and the integration of machine learning tools can assist IT security experts detect attack build-ups. P5 reported that they had integrated access protocols such as internet message access protocol (IMAP), messaging application programming interface (MAPI), post office protocol (POP), and simple mail transfer protocol (SMTP) to prevent system intrusions. The participant application of these protocols is in accordance with the NIST 800-123, NIST 800-95, and NIST 800-39 guidelines on middleware integration.

Over the years, IT security professionals have noticed an increase in the complexity of IT infrastructure attacks. Hackers have become increasingly patient with their attacks, making it harder to detect their activities. This has necessitated the formulation of intrusion detection systems. IDS systems form an active defense system against immediate and prolonged attacks. These systems monitor suspicious activities and alert responders when system anomalies are detected (Agarwal & Hussain, 2018). Mousavi et al. (2020) suggested that users' coping appraisals are vital in implementing threat avoidance mechanisms. The conceptual model of this research was the PMT, and it emphasizes on the use of threat avoidance mechanisms to protect the end-user. The integration of IDS systems assists IT security experts ensure system security and improving privacy protection. P1, P2, P3, P4, and P5 demonstrated that PMT threat avoidance attributes were integrated into the application of IDS systems. The application of IDS and IPS systems aligned with the coping appraisal attributes of the PMT conceptual framework.

Theme 5: Comprehensive User Policies

A system's security is only as strong as its users. User policies fulfill a vital role in the effective management of an information system. Having policies ensures the system's users know what is expected of them. They determine a clear boundary between actions that are acceptable and not acceptable to the system. Moreover, well-enforced user policies minimize the digital banking platform's liability if an employee or customer misuses the organization's resources. Creating comprehensive was the fifth theme that arose from the coding process. This section contains two subthemes, which are evaluating end-user needs, and user training and enforcing best security practices.

According to P1, user policies are essential at enforcing the bank's digital procedures. Both customers and bank employees are required to follow the institution's digital privacy guidelines. Users who flout security policies set by the bank can be suspended, dismissed or prosecuted in a court of law. P2 noted that providing users with adequate policies and education regarding data protection is important in mitigating cases of data breaches. P3 noted that enforcing user policies was part of the bank's efforts to follow existing bank adherence levels to data security. P4 pointed out that they review security logs to determine their staff's compliance levels to user policies. P5 stated that as an IT security officer they ensure that the train users and IT staff members to be compliant with the organization's internal policies.

Policies are essential in safe guarding a bank's IT infrastructure. To improve the efficacy of system policies, a fear-based messaging model may be used to improve user compliance to the bank's security mechanisms. The use of policy documents aligns with the PMT conceptual model. The literature review and participant responses on enforcing user compliance align with the threat appraisal and coping appraisal attributes of the PMT conceptual framework.

Table 12

Subthemes Under the Importance of Comprehensive User Policies

Subthemes	Participant Count	% Of References
User training and enforcing best security practices	5	100%
Evaluating End-user needs	3	60%

Table 13

The Application of Comprehensive User Polices in Digital Banking

Data Source	User training and enforcing best practices	Evaluating End-user needs
Participants	5	3
Documents	3	3

Table 13 shows that P1, P2, P3, P4, and P5 reported that user training and enforcing of the best security practices was part of their comprehensive user policies. P1, P2, and P4 pointed out that evaluating their user's needs was part of their user policy compliance review. Table 13 and 14 shows that 3 NIST documents supported the sub themes mentioned above.

The documents listed in Table 14 were used for triangulation and were downloaded from government-approved websites (www.nist.gov).

Table 14

Government Framework	Participants	Document Page Count
NIST 800-50	P1, P2, P4, P5	70
NIST 800-39	All	60
NIST 800-114	All	80

P1, P2, P3, P4, and P5 reported in Table 14 above that they used government-approved guidelines in formulating user policies for their internet banking platforms. P1, P2, P3, P4, and P5 reported they provide comprehensive user policy reports for their subscribers and regularly update the document. Data security guidelines and the system use document are updated bi-annually by the users. Moreover, user training is offered to the users to enhance system usability and security. The participants also confirmed that their guidelines are aligned with ISO standards.

User Training

User training is a crucial component of information system (IS) implementation security management. With more and more organizations transitioning to online-based solutions, it is imperative that the users are made aware of the system's core functions and how to protect themselves. A study carried out by Kaspersky found that users older than 55 years are not well-versed with cybersecurity principles (Ricci et al., 2018). The study further pointed out that older people are more trusting and thus more vulnerable to social engineering attacks. A secondary report by Symantec found that digital-native and overconfident millennials are more susceptible to cybercrime. Therefore, internet banking organizations must train their users on the dangers of poor internet security.

P1 reported that they train both employees and customers on the principles of digital privacy and ways they can protect their information from hackers. P1 further stated they train their employees on the risks of data breaches and how to handle cyberattacks. P1's training approach takes into account that the company employees will be the primary users. By training the system's primary users, the IT security professionals significantly diminish the chances of a data breach occurring due to user negligence. User complacency is a significant driver of system attacks. P2 explained that they had trained their customers on how to identify malicious websites and defend against phishing attacks. Ricci et al. (2018) pointed out that the best intrusion detection system will not protect users from phishing attacks. Users who do not understand the application or system they are using pose the most significant security danger. P2's user training model is crucial for averting security threats. P4 reported that they train their employees on IT safety and created awareness on the use of the latest cryptographic tools as mitigation techniques against identity-based authentication attacks. P4 noted that they warn their customers against sharing their credentials with others. P4 further explained that they encourage the bank's customers to change their passwords regularly. Updating one's password is a precautionary safety measure that reduces the risk of exposure. P5 explained that they regularly host cyber security webinars for their customers. The webinars assist to spread awareness on how users can secure their accounts, avoid common security pitfalls, and operate online applications. P5 further explained that they are responsible for the employee training session. The organization's workers are not left behind when it comes to user training on data security.

User training is an integral cybersecurity measure. Stafford et al. (2018) noted that a successful awareness program requires a motivated teacher to achieve the program's demands. Educated and motivated trainers are a firm's most effective deterrent against data breaches. Training is of no use if the educator cannot pass on information on effective data security measures. PMT's fear-based messaging model is well suited for user training programs. Mousavi et al. (2020) noted the effectiveness of using threats in messages makes users avoid engaging in risky behavior, thus promoting protection. For educators, the user training message needs to observe three important PMT rules (1) the severity of the threat's damaging outcomes; (2) probability of the threat occurring; (3) the effectiveness of the protective message influence. P1, P2, P4, and P5 agreed that they use NIST Framework 800-111 user training manual. Good and Hyman (2020) pointed out that the PMT conceptual model is ideal for formulating IS security strategies. The PMT conceptual model increases a message's efficacy, making it a perfect model for user training. The findings of this sub-theme align with the PMT conceptual framework.

Evaluating End-User Needs

Despite significant progress being achieved in cybersecurity, most efforts seem to have been aimed at the security system's computing assets. An organization's effectiveness of cybersecurity measures is often determined in the wake of an attack. Therefore, cyber security experts are encouraged to pay closer attention to human components when designing security policies. Dupuis and Renaud (2020) noted that the internet belongs to the users, and IT security experts are encouraged to adopt a human-centric approach when implementing cybersecurity solutions. Failure to account for the human factors leads to the complete failure of cybersecurity strategies (Creese et al., 2021). Policies adopted by banking organizations should establish boundaries on what is humanly possible and what is not. For instance, an ATM card should not be required to create an alphanumeric PIN as it affects the process's efficacy. NIST 800-70 Rev 4 provides a comprehensive guideline for user management for IT products. These guidelines are essential for optimizing system usage by encouraging a user-centric management approach.

P1 reported that it is quite challenging for their organization to ensure that their customers will be following the institution's digital procedures and safety policies. However, the participant reported that they ensure they sensitize and educate customers about the bank's laid-out digital security guidelines and user policies. It is difficult for cybersecurity experts and IT security professionals to ensure external parties are adhering to data laws. Barth et al. (2022) noted that IT system users always engage in system-compromising activities. For instance, in bank applications, users share passwords with other parties. Having poor privacy-related attitudes puts the user in compromising situations. P1 noted that digital banking platforms should consider end-user negligence in the formulation of training programs. P2 explained that they integrated KYC (Know Your Customer) strategies to ensure their banking platform understands the customer's needs and improves user compliance with digital privacy guidelines. P2 pointed out that they educate the users of their platform to improve service provisioning by the organization. A typical verification process requires the user to submit some identification documents. However, P2 use KYC principles to promote compliance among the users. Grobler et al. (2021) stated that the three U's of cybersecurity are the user, usage, and usability. Therefore, IT security professionals must create a healthy rapport with the users to enhance system security.

P3 pointed out that they use a checklist document to streamline services in the bank. P3 said that they conduct awareness programs to assist users in protecting themselves from cyberattacks. The security awareness program enables users to act in a security-conscious manner. The bank also receives feedback from the consumers to improve service provisioning (Creese et al., 2021). P4 reported that users are constantly updated about the bank's security changes and the impact of these changes. P4 explained that their bank reimburses victims of identity theft crimes. The bank also provides legal advice to customers affected by cyberattacks and looks for ways to resolve such events. P5 reported that the end-users are made aware of the organization's data privacy guidelines. Furthermore, P5 ensures that the bank's service provisioning observes confidentiality, availability, and integrity guidelines designed to protect consumers' digital privacy.

Stability in a bank's system is a point of interest for regulators, consumers, and the business itself. However, having weak governance structures may cause the user to wreak havoc in a bank's system (Uddin et al., 2020). Users are the leading sources of hazards when it comes to the effective management of financial systems. Financial institutions must listen to the users so as to optimize service provisioning and address security concerns. For instance, a user-initiated denial of service (DOS) attack could shut down the bank's entire services (Haapamäki & Sihvonen, 2019). PMT's threat appraisal process may create user-centric intervention processes that minimize the impact of user errors on the system. Ameen et al. (2021) explained that a user-oriented approach may be integrated into cybersecurity to improve stability. IT professionals may integrate a user centric approach to optimize the efficacy of the security practices to protect their computer systems against identity-authentication attacks.

Rogers (1975) PMT noted that a persuasive messaging approach may be used by IT security professionals to enhance user compliance in observing security policies. Wu (2019) noted that knowledge sharing security procedures present in the PMT conceptual model maybe used to promote the response efficacy of cybersecurity experts against identity-based authentication attacks. IT security professionals are required to comprehend and practice intricate technical knowledge required to secure online banking platforms. In Johnston and Warkentin (2010) modified PMT, formulating adequate strategies against threats is a vital step in safeguarding resources. IT managers planning to secure their networks may use PMT strategies identified in this study to enhance system security. Johnston and Warkentin (2010) pointed out that IT security managers may integrate threat appraisal and coping appraisal processes into their data security procedures to improve user compliance with security guidelines.

The results of this study showcase that effective cybersecurity strategies utilizing a persuasive messaging design may assist IT managers to reduce instances of identity-theft attacks on online banking platforms. Moreover, persuasive messaging may cause users to be more cautious in observing data security principles, resulting in reduced data breaches. Wieder (2019) noted that in high stress situations, it is crucial that messages are received as intended by the audience. Therefore, it is essential that IT security managers identify communication barriers that may hinder a message's overall effectiveness. The findings of this study may help other financial tech organizations secure their platforms against cyberthreats and will improve user confidence in digital platforms. The literature review and participant responses on evaluating consumer needs align with PMT's threat appraisal attributes.

As more consumers embrace the use of digital payment platforms, questions over cybersecurity have become even more pressing for financial institutions. Ameen et al. (2021) explained that digital networks could be compromised using different vectors such as the loss of a device, insecure networks, insufficient privacy, SMS-based attacks, and weak authentication systems. These attacks are a significant source of concern for most organizations, especially when the institution loses customer data. As a result, banks and other financial organizations are taking a number of measures to improve consumer confidence in the use of digital platforms and reassure them of their data privacy. De Kimpe et al. (2021) pointed out that the PMT theory has been integrated into information security studies to persuade users of the effectiveness of cyberattack countermeasures. PMT's emphasis on the integration of trust-related variables has made it an ideal model that IT security experts may use to win over consumer trust. The findings of this study may be used to stimulate users to learn about effective cybersecurity practices thus becoming more trusting of digital platforms. IT security experts may also use the PMT concept to stress that data security is a matter of personal security, promoting protective behavior in digital platforms.

Applications to Professional Practice

This study examined the strategies used by IT security professionals working on internet banking platforms use to mitigate identity-based authentication attacks affecting digital privacy in online banking. The selected IT security professional participants were from the northeastern region of the United States. The study's findings are suitable for IT security professionals or IT security managers working with FinTech technologies or other financial applications. The study's population specified the different strategies used to promote digital privacy and secure web-based financial transaction platforms. These strategies can also create awareness of the importance of digital privacy in the financial sector.

P1, P2, P3, P4, and P5 pointed out that comprehensive user authentication practices, data encryption, system audits, intrusion detection systems, and user policies were the core strategies used to secure digital banking platforms against data breaches. Bankuoru Egala et al. (2021) stated that the rise of digital banking services has contributed to a decline in digital privacy rates. Internet banking applications are highly interlinked with other digital systems, which put consumers' privacy at risk. Vasilomanolakis and Mühlhäuser (2018) pointed out that cyberattacks targeting financial institutions are becoming increasingly sophisticated. Digital privacy has become a fuzzy concept (Barth et al., 2022). The intangible and non-urgent nature of online data has contributed to the growing lack of digital privacy. IT security professionals have been tasked with the role of educating consumers about their right to online privacy. Barth et al. (2022) further explained that CIOs, CISOs and IT managers should inform consumers of the importance of digital privacy and way to protect themselves. Rahi et al. (2018) reported that the PMT conceptual model can be integrated into cybersecurity messages to enhance message efficacy and user data security compliance. CIOs, CISOs, IT managers, and IT security professionals may integrate PMT's messaging tools to boost the efficacy of user data security training programs. Moreover, user training should only be provided by IT security professionals with extensive knowledge in banking technology.

This study's findings may assist banks in the northeastern region to secure the IT infrastructure against data breaches and formulate procedures to protect user privacy. Financial technology companies can use the strategies identified in this study's findings to build trust in financial institutions' solutions and help banks secure the customer's data. Some of the distinct strategies that arose from the study include the use of end-to-end encryption, integration of IDS tools, implementation of multifactor authentication, and implementation of NIST guidelines. This study's results offer strategies that IT bank managers can use to upgrade their system policies and improve user compliance. Bank managers may use the guidelines in this document to perform system upgrades while observing international data security regulations. Ultimately, the findings of this study may assist CIOs, CISOs, IT managers, and IT security professionals minimize cases of data breaches in the organizations.

The result of this study may help the IT community address a serious and increasing issue in relation to data security as well as potentially assisting with decreasing the number of identity thefts that occur annually. This study may help IT professionals in early detection, reduction, and prevention of identity-based authentication attacks on online banking. Aboobucker and Bao (2018) observed that internet banking services are prone to identity-based authentication attacks due to the financial incentive behind a successful system exploit. Consequently, cybercriminals target e-banking platforms and banking databases due to their wealth of information (Kiljan et al., 2018). By putting in place cybersecurity strategies to address digital privacy based on the results of this study may compel IT security professionals to effectively design, establish, and improve the existing digital privacy strategies and deter identity-based authentication attacks. In addition, the results may be used to properly ensure IT security professionals catalog each security incident experienced by the banks and enhance digital privacy on online banking platforms.

Implications for Social Change

The findings from this study may contribute to a positive social change that include increasing the number of users to effectively use cybersecurity policies, tools, techniques, and trainings designed to protect their online-banking accounts from identity-based authentication attacks. The results of this study offered effective training to individuals looking to protect themselves from identity-based authentication attacks. The findings of this study may effectively prevent and mitigate online banking fraud exploits targeting customers, employees, and organizations from identity-theft, thus protecting their privacy. The findings of this study may contribute to a positive social change in the proper use of security tools and technology by bank employees and users. Employee behavior plays a great role in the failure of a security chain of a system (Syniavska et al., 2019). For instance, a bank employee may share their system authentication credentials with third parties and inadvertently compromise the bank's information system. Bank employees and employees in other organizations may use the study's recommended techniques to effectively manage and update their passwords. With technology rapidly evolving, the bank's employees need to incorporate complex password management.

One of the significant challenges affecting financial institutions is the inability to ensure consumer trust on data privacy and security. Bank clients are always sceptical that their data will be shared with third-party organizations for one reason or another by their financial institution (Bankuoru Egala et al., 2021). As the business world continues to transition to data-driven services, financial institutions must demonstrate their willingness to protect their consumer's data. Implementing effective data strategies may improve consumer trust in digital banking platforms. Today, cybersecurity experts and IT leaders are encouraged to implement adequate secure procedures to ensure consumer safety in the digital banking sector.

The strategies identified in this study may assist financial institutions to identify more adequate secure techniques to protect their consumers from data breaches, thus promoting user trust levels on digital banking platforms. The positive social change of this study may help users effectively use online banking tools and features to protect their account and encourage more consumers transition to digital banking platforms. Lamontagne et al. (2021) stated that users exhibit negative emotions toward new IS systems. The methodologies included in this study will assist researchers to optimize the online banking platforms to ensure the customers are protected in technology adoption. Moreover, this study may result in financial institutions offering affordable services to their consumers. Bankuoru Egala et al. (2021) explained that data breaches affecting financial institutions lead to losses amounting to billions of dollars per year. The cost of bearing financial losses is then transferred to the end-user under the guise of transaction charges. This study proposes strategies that may minimize the financial losses experienced by online banking service providers using PMT’s threat appraisal process. Sealing these loopholes will reduce the economic losses banks incur and reduce the transaction costs transferred to the consumers. In addition, consumers may benefit from better quality financial services when banks implement PMT-based guidelines.

This study uncovered the actions, ideas, and strategies used to protect bank customers and employees of digital payment systems from identity-based authentication attacks and threats. The social change of this research study results is to positively affect the life of bank customers and society as a whole. Identity-based authentication attacks have been identified as a menace to digital banking services in the past decade. Organizations spearheading cyber-security services and threat assessments have identified different ways identity-based authentication attacks compromise financial systems. Some of these attack vectors include credential theft, identity theft, disinformation, malware, data manipulation, and data theft. Essentially, identity-based authentication attacks take advantage of user authentication loopholes present in e-banking platforms. Moreover, identity-based authentication attacks exploit the victim’s trust in digital technology. This study may assist digital banking consumers in recognizing the different forms of identity-based authentication attacks and exercising caution while using digital banking services. The perpetrators of identity-based authentication attacks often target persons with little knowledge of cybersecurity policies such as the elderly. This study created awareness strategies that may educate non-technical consumers on detecting identity-based authentication attacks. The study's recommendations may help spread information on technological safeguards among the vulnerable. The most robust line of defense against identity-based authentication attacks is consumers' knowledge of information security.

Over the past few years, cyber breaches have targeted information-rich platforms and the financial sector. Internet users tend to reuse similar authentication credentials between different platforms, which put them at risk in the event of a data breach. For instance, consumers will use similar passwords for their social media accounts and banking applications. A data breach in one of the social media platforms will expose the user's authentication credentials to adversaries. This study seeks to dissuade the public from reusing their passwords across websites and digital platforms. Users are encouraged to be highly cautious when creating their authentication passwords. For example, practices such as using one's date of birth and nickname as part of their password combination may change. The study suggested ideal password selection strategies such as the use of strong and long alphanumeric login credentials.

Detecting which websites to trust with one's banking details is another social implication in this study. Today, phishing has become an effective tactic used in gaining access to a victim's accounts. Typically, an attacker sends a seemingly legit email or link to a potential victim to steal their passwords. Most victims of identity-based authentication attacks are victims of phishing attacks. Secondly, scam websites prey on their victim's trust levels to steal from them. The study results seek to inform users on ways to identify legit websites and avoid phishing attacks. Consumers may use various internet tools to assess a website's trust levels. For instance, Microsoft edge has rolled out a reputation checker for e-commerce platforms. The tool may be used to detect phishing links.

Responding to identity-based authentication attacks is also a crucial defense mechanism. The study aims to improve consumer response to cyberattacks and initiate protective measures. For example, if there has been a report of a significant cyberattack incident, users should respond by changing passwords to e-banking platforms. A culture of digital vigilance may reduce cases of identity-based authentication attacks. Digital vigilance is a passive strategy that enhances the user's preparedness against attacks. Users are encouraged to update themselves with cybersecurity policy and data trends. Appropriate research is essential in developing passive and active defense strategies against cyberattacks. This study seeks to proactively develop countermeasures against identity-based authentication attacks that consumers may use. Researchers have a social responsibility to inform the consumers on appropriate protective strategies against cyberthreats.

Recommendations for Action

This study is centered on the strategies used by IT security professionals working in banks in the northeastern region of the U.S to protect online banking applications against identity-based authentication attacks and enhance digital privacy. My first recommendation to banking organizations and chief information security officers

(CISOs) is to review their current user authentication procedures to ensure their digital platforms have a stronger verification system that may minimize identity-based authentication attacks. Today, hackers are utilizing identity-theft vulnerabilities to gain access to a bank's network and causing data breaches. Hackers use social engineering attacks to manipulate people into divulging confidential information that is used to gain access to the victim's online bank account. Examples of social engineering attacks include phishing, scareware, pretexting, and spear phishing. Ricci et al. (2018) stated that older individuals are highly susceptible to phishing attacks as they are more trusting. Younger people are also highly prone to identity-based authentication attacks. Having a solid user authentication mechanism may prevent bank customers from falling victim to social engineering attacks. IT managers working in banks and FinTech organizations should review their institution's current user authentication protocols and enforce more stringent verification procedures to protect their platforms.

The second recommendation is on the importance of conducting periodical system audits to detect data breaches and cases of identity theft. IT security professionals should carry out proper extensive system audits in order to secure their data and identify security loopholes existing in their platforms. Data security frameworks such as NIST and ISO should also be used to determine the system infrastructure compliance levels to data security guidelines by IT managers. Performing proper extensive security audits offers financial organizations with proactive means of handling security threats present in the organization's system. Moreover, proper extensive system audits may be used to identify digital privacy guidelines gaps that an attacker may use to compromise the bank's data security integrity. It is also advisable for the IT security team to share the results of the system audits with the customers to win over their trust.

The third recommendation is that banks should integrate adequate comprehensive data encryption protocols into their IT platforms. Providing adequate comprehensive data encryption is critical in actively protecting the bank’s data from breaches. An unsecured network exposes user data to attacks such as man-in-the-middle, packet sniffing, and data capturing tools that may expose their consumer’s personally identifiable information (PII) to attackers. A customer’s PII data may be used to gain unauthorized access to their bank accounts or swindle other unsuspecting users. Financial institutions should ensure that data-in-transit and data-at-rest communication channels are adequately encrypted to protect customer records.

The fourth recommendation is to integrate appropriate upgraded intrusion detection systems into the bank’s IT infrastructure. Online banking platforms need to set up appropriate upgraded defensive tools that detect and avert attacks automatically. Having an active appropriate upgraded defense system prevents excessive damage to the bank’s network by examining its contents. IDS systems applications monitor computer networks for malicious activity or users flouting system policies. These systems prevent cyber-attacks by examining hosts connected to the system using a rule-based detection system without affecting network performance. The integration of appropriate upgraded IDS tools is essential in securing the bank’s servers from experiencing sophisticated computer attacks. By incorporating IDS systems into the bank’s security system, IT manager can improve the security of the bank's network by detecting abnormal user behavior thus preventing data breaches.

The final recommendation is to train all users on secure usage of the bank's digital transaction platform. Banking organizations should provide mandatory privacy protection training and security awareness to customers before they successfully create or access their financial accounts; also providing updated mandatory active users privacy protection training regularly may minimize the chances of a cyberattack happening by enabling users to understand acceptable system usage practices. Moreover, training all users enables IT managers to understand their consumer's concerns on data privacy and identity theft. Training also assists CISOs to understand the bank's system usability and security loopholes. The IT security team plays a crucial role in training their users, thus minimizing data breaches. IT security managers should periodically update their organization's data security policies to reduce the bank's legal liabilities in cyberattacks. Stronger user policies are essential in averting data breaches and protecting the bank's critical IT infrastructure.

The study's findings will be published or disseminated to IT security managers and other IT personnel working in the banking sector in the United States. The study's findings are also applicable to digital banking platforms in use worldwide. Further research on the topic is recommended for online banking platforms implemented in other regions of the United States. The study's findings will be disseminated to other parts of the country to contribute to the advancement of digital privacy guidelines in the banking sector. Sharing these findings may assist IT managers based in the United States in combating identity-based authentication attacks targeting banking platforms.

Recommendations for Further Study

I interviewed experienced IT security professionals based in the northeastern part of the United States, as the study findings show. My first recommendation is to encourage other regions of the US to participate in my study or carry out similar studies to expand the geographic pool of my study's findings. My second recommendation is to expand my research to other FinTech fields such as e-commerce platforms and digital exchange platforms to determine effective countermeasures against identity-based authentication attacks. Financial motives usually drive perpetrators to use identity-based authentication attacks as an attack vector. Therefore, IT leaders managing digital exchange platforms should be wary of such vices. The purpose of this qualitative pragmatic study was to examine effective strategies that may be used to avert identity-based authentication attacks targeting online banking platforms. My last recommendation is that future studies may incorporate a mixed-method design to investigate the research question. Integrating qualitative and quantitative research methodologies may shed more light on the subject matter. Future studies should also use more diverse data collection methods to examine a larger population and make the study's findings better.

Reflections

The pragmatic design of this research study analyzed the strategies IT security professionals use to defend their platforms from identity-based authentication attacks and protect the consumer's right to privacy. I got an excellent glimpse of the problems plaguing digital financial platforms through this research. I reviewed industry set guidelines such as NIST data security guidelines and ISO standards designed to protect consumers. I learned that these strategies may be used by other organizations interested in integrating FinTech technologies into their platforms.

The DIT Doctoral Study process expanded my view on cybersecurity as I reviewed academic literature done by various accomplished authors. The doctoral process has been worthwhile and rewarding because I encountered numerous exciting publications. Overall, I have gained more exposure to the application of digital privacy principles in the banking IT field. I have developed an in-depth understanding of cybersecurity strategies that can be used to resolve identity-based authentication attacks. I will still continue to pursue the online banking niche in cybersecurity. My motivation is to ensure digital banking becomes a highly secure transaction medium, especially for future generations.

After compiling my research, a personal bias formed on the lack of adequate data security policies. My experience in the data security field also fueled my bias on the lack of data policies. Banking institutions rarely get reprimanded by digital privacy bodies for flouting data security regulations. However, I did not let my bias affect my study's findings. I took a neutral perspective and focused on enriching my study with honest feedback. I also ensured my actions did not influence the study's participants' feedback by observing IRB's data collection guidelines. Although, this study sampled a small population, the study's findings are most likely reproducible in another study.

Summary and Study Conclusions

This qualitative pragmatic study was intended to explore the strategies used by IT security professionals to mitigate the impact of identity-based authentication attacks on digital banking platforms. The research study's findings pointed to the following themes: (a) comprehensive user authentication, (b) importance of data encryption, (c) system audits, (d) intrusion detection systems, and (e) user policies and trainings, as essential techniques in countering identity-based authentication attacks. IT security professionals can implement NIST cybersecurity framework and CIA guidelines to optimize the security of online banking platforms.

Today, banking organizations are integrating different forms of financial technology to meet their customer demands for digital services. Digital banking allows banks to provide information and services to their customers with more convenience via self-service delivery channels such as the internet and mobile phone. Nevertheless, the provisioning of online-banking services presents severe risks to consumers and financial organizations. Stability in the banking sector is a matter of interest for consumers, businesses, and regulators involved with the industry. However, the fast development of disruptive technologies witnessed in the past 5 years have changed the global banking system. Attacks targeting these technologies have been transforming in sophistication and magnitude. It is therefore important that the key stakeholders involved in digital banking invest in cutting-edge technologies and strategies that will reduce instance data breaches in online banking platforms.

References

Aboobucker, I., & Bao, Y. (2018). What obstruct customer acceptance of internet banking? Security and privacy, risk, trust and website usability and the role of moderators. *The Journal of High Technology Management Research*, *29*(1), 109–123. https://doi.org/10.1016/j.hitech.2018.04.010

Adams, P. C. (2020). Agreeing to surveillance: Digital news privacy policies. *Journalism & Mass Communication Quarterly*, *97*(4), 868–889. https://doi.org/10.1177/1077699020934197

Agarwal, N., & Hussain, S. Z. (2018). A closer look at intrusion detection system for web applications. *Security and Communication Networks*, *2018*, 1–27. https://doi.org/10.1155/2018/9601357

Aguinis, H., & Solarino, A. M. (2019). Transparency and replicability in qualitative research: The case of interviews with elite informants. *Strategic Management Journal*, *40*(8). https://doi.org/10.1002/smj.3015

Akanfe, O., Valecha, R., & Rao, H. R. (2020). Assessing country-level privacy risk for digital payment systems. *Computers & Security*, *99*(1), 1–13. https://doi.org/10.1016/j.cose.2020.102065

Alam, M. K. (2020). A systematic qualitative case study: Questions, data collection, NVivo analysis and saturation. *Qualitative Research in Organizations and Management: An International Journal*, *16*(1). https://doi.org/10.1108/qrom-09-2019-1825

Aldiabat, K., & Le Navenec, C. L. (2018). Data saturation: The mysterious step in grounded theory method. *The Qualitative Report*. https://doi.org/10.46743/2160-3715/2018.2994

Alexander, B. N., & Smith, A. D. (2018). Organizational access in qualitative research. *Qualitative Research in Organizations and Management: An International Journal*, *14*(2). https://doi.org/10.1108/qrom-10-2017-1574

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Computers in Human Behavior*, *114*, 106531. https://doi.org/10.1016/j.chb.2020.106531

Ananda, S., Devesh, S., & Al Lawati, A. M. (2020). What factors drive the adoption of digital banking? An empirical study from the perspective of Omani retail banking. *Journal of Financial Services Marketing*, *25*(1-2), 14–24. https://doi.org/10.1057/s41264-020-00072-y

Antunes, M., Maximiano, M., & Gomes, R. (2022). A customizable web platform to manage standards compliance of information security and cybersecurity auditing. *Procedia Computer Science*, *196*, 36–43. https://doi.org/10.1016/j.procs.2021.11.070

Auernhammer, J. (2020). Design Research in Innovation Management: A pragmatic and human centered approach. *R&D Management*, *50*(3), 412–428. https://doi.org/10.1111/radm.12409

Aurigemma, S., & Mattson, T. (2018). Exploring the effect of uncertainty avoidance on taking voluntary protective security actions. *Computers & Security*, *73*, 219–234. https://doi.org/10.1016/j.cose.2017.11.001

Ayaz, A., & Yanartaş, M. (2020). An analysis on the unified theory of acceptance and use of technology theory (UTAUT): Acceptance of electronic document management system (EDMS). *Computers in Human Behavior Reports*, *2*, 100032. https://doi.org/10.1016/j.chbr.2020.100032

Bankuoru Egala, S., Boateng, D., & Aboagye M, S. (2021). To leave or retain? An interplay between quality digital banking services and customer satisfaction. *International Journal of Bank Marketing*, *39*(7), 1420–1445. https://doi.org/10.1108/ijbm-02-2021-0072

Barth, S., de Jong, M. D. T., & Junger, M. (2022). Lost in privacy? Online privacy from a cybersecurity expert perspective. *Telematics and Informatics*, *68*, 101782. https://doi.org/10.1016/j.tele.2022.101782

Bax, S., McGill, T., & Hobbs, V. (2021). Maladaptive behaviour in response to email phishing threats: The roles of rewards and response costs. *COMPUT SECUR*, *106*, 102278. https://doi.org/10.1016/j.cose.2021.102278

Becker, K. M. (2019). Beyond researcher as instrument. *Qualitative Research Journal*, *19*(4), 426–437. https://doi.org/10.1108/qrj-02-2019-0021

Benitez, J., Llorens, J., & Braojos, J. (2018). How information technology influences opportunity exploration and exploitation firm's capabilities. *Information & Management*, *55*(4), 508–523. https://doi.org/10.1016/j.im.2018.03.001

Bergström, E., Lundgren, M., & Ericson, Å. (2019). Revisiting information security risk management challenges: A practice perspective. *Information & Computer Security*, *27*(3), 358–372. https://doi.org/10.1108/ics-09-2018-0106

Bernerth, J. B., Aguinis, H., & Taylor, E. C. (2021). Detecting false identities: A solution to improve web-based surveys and research on leadership and health/well-being. *Journal of Occupational Health Psychology*, *26*(6), 564–581. https://doi.org/10.1037/ocp0000281

Blackwood-Brown, C., Levy, Y., & D'Arcy, J. (2019). Cybersecurity awareness and skills of senior citizens: A motivation perspective. *Journal of Computer Information Systems*, *61*(3), 1–12. https://doi.org/10.1080/08874417.2019.1579076

Bland, J. A., Petty, M. D., Whitaker, T. S., Maxwell, K. P., & Cantrell, W. A. (2020). Machine learning cyberattack and defense strategies. *Computers & Security*, *92*, 101738. https://doi.org/10.1016/j.cose.2020.101738

Boddez, Y., Moors, A., Mertens, G., & De Houwer, J. (2020). Tackling fear: Beyond associative memory activation as the only determinant of fear responding. *Neuroscience & Biobehavioral Reviews*, *112*, 410–419. https://doi.org/10.1016/j.neubiorev.2020.02.009

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2018). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research*, 1–25. https://doi.org/10.1177/0093650218800915

Bornschein, R., Schmidt, L., & Maier, E. (2020). The effect of consumers' perceived power and risk in digital information privacy: The example of cookie notices. *Journal of Public Policy & Marketing*, *39*(2), 135–154. https://doi.org/10.1177/0743915620902143

Branley, D. B., & Covey, J. (2018). Risky behavior via social media: The role of reasoned and social reactive pathways. *Computers in Human Behavior*, *78*, 183–191. https://doi.org/10.1016/j.chb.2017.09.036

Butler, A. E., Copnell, B., & Hall, H. (2018). The development of theoretical sampling in practice. *Collegian*, *25*(5), 561–566. https://doi.org/10.1016/j.colegn.2018.01.002

Byrne, J., Kirwan, G., & Mc Guckin, C. (2019). Social media surveillance in social work: Practice realities and ethical implications. *Journal of Technology in Human Services*, *37*(2-3), 142–158. https://doi.org/10.1080/15228835.2019.1584598

Call-Cummings, M., Dennis, B., & Martinez, S. (2018). The role of researcher in participatory inquiry: Modeling intra-active reflexivity in conversational reflections. *Cultural Studies, Critical Methodologies*, *19*(1), 68–76. https://doi.org/10.1177/1532708617750677

Cao, C., & Zhu, X. (2019). Strong anonymous mobile payment against curious third-party provider. *Electronic Commerce Research*, *19*(3), 501–520. https://doi.org/10.1007/s10660-018-9302-2

Caretta, M. A., & Pérez, M. A. (2019). When participants do not agree: Member checking and challenges to epistemic authority in participatory research. *Field Methods*, *31*(4), 359–374. https://doi.org/10.1177/1525822x19866578

Carhart-Harris, R. L., Wagner, A. C., Agrawal, M., Kettner, H., Rosenbaum, J. F., Gazzaley, A., Nutt, D. J., & Erritzoe, D. (2021). Can pragmatic research, real-world data and digital technologies aid the development of psychedelic medicine? *Journal of Psychopharmacology*, *36*(1), 026988112110085. https://doi.org/10.1177/02698811211008567

Carminati, M., Polino, M., Continella, A., Lanzi, A., Maggi, F., & Zanero, S. (2018). Security evaluation of a banking fraud analysis system. *ACM Transactions on Privacy and Security*, *21*(3), 1–31. https://doi.org/10.1145/3178370

Cepeda, C., Tonet, R., Osorio, D. N., Silva, H. P., Battegay, E., Cheetham, M., & Gamboa, H. (2019). Latent: A flexible data collection tool to research human behavior in the context of web navigation. *IEEE Access*, *7*, 77659–77673. https://doi.org/10.1109/access.2019.2916996

Chang, S. I., Chang, L. M., & Liao, J. C. (2020). Risk factors of enterprise internal control under the internet of things governance: A qualitative research approach. *Information & Management*, *57*(6), 103335. https://doi.org/10.1016/j.im.2020.103335

Chen, F., Dai, S., Zhu, Y., & Xu, H. (2019). Will concerns for ski tourism promote pro□ environmental behaviour? An implication of protection motivation theory. *International Journal of Tourism Research*, *22*(3), 303–313. https://doi.org/10.1002/jtr.2336

Christensen, G., & Miguel, E. (2018). Transparency, reproducibility, and the credibility of economics research. *Journal of Economic Literature*, *56*(3), 920–980. https://doi.org/10.1257/jel.20171350

Clarke, E., & Visser, J. (2018). Pragmatic research methodology in education: Possibilities and pitfalls. *International Journal of Research & Method in Education*, *42*(5), 455–469. https://doi.org/10.1080/1743727x.2018.1524866

Crano, W. D. (2019). Reflections on a proposal designed to enhance the internal and internal validity of research in psychology. *Psychological Inquiry*, *30*(4), 211–215. https://doi.org/10.1080/1047840x.2019.1693868

Creese, S., Dutton, W. H., & Esteve-González, P. (2021). The social and cultural shaping of cybersecurity capacity building: A comparative study of nations and regions. *Personal and Ubiquitous Computing*, *25*(5), 941–955. https://doi.org/10.1007/s00779-021-01569-6

Crick, J. M. (2020). Qualitative research in marketing: What can academics do better? *Journal of Strategic Marketing*, *29*(5), 1–40. https://doi.org/10.1080/0965254x.2020.1743738

Cronje, J. C. (2020). Designing questions for research design and design research in eLearning. *The Electronic Journal of E-Learning*, *18*(1 Jan 2020). https://doi.org/10.34190/ejel.20.18.1.002

Cui, J., Zhang, X., Cao, N., Zhang, D., Ding, J., & Li, G. (2018). An improved authentication protocol–based dynamic identity for multi-server environments.

International Journal of Distributed Sensor Networks, *14*(5), 155014771877765. https://doi.org/10.1177/1550147718777654

Cumyn, A., Ouellet, K., Côté, A. M., Francoeur, C., & St-Onge, C. (2018). Role of researchers in the ethical conduct of research: A discourse analysis from different stakeholder perspectives. *Ethics & Behavior*, *29*(8), 621–636. https://doi.org/10.1080/10508422.2018.1539671

Cypress, B. S. (2019). Qualitative research. *Dimensions of Critical Care Nursing*, *38*(5), 264–270. https://doi.org/10.1097/dcc.0000000000000374

Daniel, K. E., Daros, A. R., Beltzer, M. L., Boukhechba, M., Barnes, L. E., & Teachman, B. A. (2020). How anxious are you right now? Using ecological momentary assessment to evaluate the effects of cognitive bias modification for social threat interpretations. *Cognitive Therapy and Research*, *44*(3), 538–556. https://doi.org/10.1007/s10608-020-10088-2

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2021). What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour & Information Technology*, *2021-03-24*, 1–13. https://doi.org/10.1080/0144929x.2021.1905066

De Matos, E., Tiburski, R. T., Moratelli, C. R., Johann Filho, S., Amaral, L. A., Ramachandran, G., Krishnamachari, B., & Hessel, F. (2020). Context information sharing for the Internet of Things: A survey. *Computer Networks*, *166*, 106988. https://doi.org/10.1016/j.comnet.2019.106988

DeVaney, S. A., Spangler, A., Lee, Y. A., & Delgadillo, L. (2018). Tips from the experts on conducting and reviewing qualitative research. *Family and Consumer Sciences Research Journal*, *46*(4), 396–405. https://doi.org/10.1111/fcsr.12264

Dia, D., Kahn, G., Labernia, F., Loiseau, Y., & Raynaud, O. (2020). A closed sets-based learning classifier for implicit authentication in web browsing. *Discrete Applied Mathematics*, *273*, 65–80. https://doi.org/10.1016/j.dam.2018.11.016

Donalds, C., & Osei-Bryson, K. M. (2019). Toward a cybercrime classification ontology: A knowledge-based approach. *Computers in Human Behavior*, *92*, 403–418. https://doi.org/10.1016/j.chb.2018.11.039

Donmez-Turan, A. (2019). Does unified theory of acceptance and use of technology (UTAUT) reduce resistance and anxiety of individuals towards a new system? *Kybernetes*, *49*(5), 1381–1405. https://doi.org/10.1108/k-08-2018-0450

DuBois, J. M., Strait, M., & Walsh, H. (2018). Is it time to share qualitative research data? *Qualitative Psychology*, *5*(3), 380–393. https://doi.org/10.1037/qup0000076

Dupuis, M., & Renaud, K. (2020). Scoping the ethical principles of cybersecurity fear appeals. *Ethics and Information Technology*, *2020*(1), 1–20. https://doi.org/10.1007/s10676-020-09560-0

Edwards, R., & Holland, J. (2020). Reviewing challenges and the future for qualitative interviewing. *International Journal of Social Research Methodology*, *23*(5), 581–592. https://doi.org/10.1080/13645579.2020.1766767

Elueze, I., & Quan-Haase, A. (2018). Privacy attitudes and concerns in the digital lives of older adults: Westin's privacy attitude typology revisited. *American Behavioral Scientist*, *62*(10), 1372–1391. https://doi.org/10.1177/0002764218787026

Ertefaie, A., Small, D. S., Leonard, C. E., Ji, X., & Hennessy, S. (2018). Assumptions underlying the trend-in-trend research design. *Epidemiology*, *29*(6), e52–e53. https://doi.org/10.1097/ede.0000000000000890

Esmaeilzadeh, P. (2020). The impacts of the privacy policy on individual trust in health information exchanges (HIEs). *Internet Research*, *30*(3), 811–843. https://doi.org/10.1108/intr-01-2019-0003

Fernando, M., & Bandara, R. (2020). Towards virtuous and ethical organizational performance in the context of corruption: A case study in the public sector. *Public Administration and Development*. https://doi.org/10.1002/pad.1882

Flemming, K., Booth, A., Hannes, K., Cargo, M., & Noyes, J. (2018). Cochrane Qualitative and Implementation Methods Group guidance series paper 6: Reporting guidelines for qualitative, implementation, and process evaluation evidence syntheses. *Journal of Clinical Epidemiology*, *97*, 79–85. https://doi.org/10.1016/j.jclinepi.2017.10.022

Fuller, C. S. (2019). Is the market for digital privacy a failure? *Public Choice*, *180*(3-4), 353–381. https://doi.org/10.1007/s11127-019-00642-2

Gallagher, J. R. (2019). A framework for Internet case study methodology in writing studies. *Computers and Composition*, *54*, 102509. https://doi.org/10.1016/j.compcom.2019.102509

Gazendam, F. J., Krypotos, A.-M., Kamphuis, J. H., van der Leij, A. R., Huizenga, H. M. H., Eigenhuis, A., & Kindt, M. (2020). From adaptive to maladaptive fear: Heterogeneity in threat and safety learning across response systems in a representative sample. *International Journal of Psychophysiology*, *158*, 271–287. https://doi.org/10.1016/j.ijpsycho.2020.09.017

Gies, S. V., Piquero, N. L., Piquero, A. R., Green, B., & Bobnis, A. (2020). Wild, wild theft: Identity crimes in the digital frontier. *Criminal Justice Policy Review*, *32*(6), 088740342094965. https://doi.org/10.1177/0887403420949650

Gill, S. L. (2020). Qualitative sampling methods. *Journal of Human Lactation*, *36*(4), 089033442094921. https://doi.org/10.1177/0890334420949218

Giwah, A. D., Wang, L., Levy, Y., & Hur, I. (2019). Empirical assessment of mobile device users' information security behavior towards data breach: Leveraging protection motivation theory, *Journal of Intellectual Capital*, Vol. 21 No. 2, pp. 215 233. https://doi.org/10.1108/JIC-03-2019-0063

Glegg, S. M. N. (2018). Facilitating interviews in qualitative research with visual tools: a typology. *Qualitative Health Research*, *29*(2), 301–310. https://doi.org/10.1177/1049732318786485

Good, M. C., & Hyman, M. R. (2020). Protection motivation theory and brick-and-mortar salespeople. *International Journal of Retail & Distribution Management*, *48*(8), 865–879. https://doi.org/10.1108/ijrdm-05-2019-0155

Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, J. P., Lefkovitz, N. B., Danker, J. M., Choong, Y. Y., Greene, K. K., &

Theofanos, M. F. (2018). Digital identity guidelines: Authentication and lifecycle management. *National Institute of Standards and Technology Special Publication*, *800*(63). https://doi.org/10.6028/nist.sp.800-63b

Green, B., Gies, S., Bobnis, A., Piquero, N. L., Piquero, A. R., & Velasquez, E. (2020). The role of victim services for individuals who have experienced serious identity-based crime. *Victims & Offenders*, *15*(6), 720–743. https://doi.org/10.1080/15564886.2020.1743804

Greener, S. (2018). Research limitations: The need for honesty and common sense. *Interactive Learning Environments*, *26*(5), 567–568. https://doi.org/10.1080/10494820.2018.1486785

Grobler, M., Gaire, R., & Nepal, S. (2021). User, usage and usability: Redefining human centric cyber security. *Frontiers in Big Data*, *4*(2021), 1–24. https://doi.org/10.3389/fdata.2021.583723

Gruschka, N., Mavroeidis, V., Vishi, K., & Jensen, M. (2018, December 1). Privacy issues and data protection in big data: A case study analysis under GDPR. *IEEE Xplore*. https://doi.org/10.1109/BigData.2018.8622621

Gunsalus, C. K., Marcus, A. R., & Oransky, I. (2018). Institutional research misconduct reports need more credibility. *JAMA*, *319*(13), 1315. https://doi.org/10.1001/jama.2018.0358

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, *34*(7), 808–834. https://doi.org/10.1108/maj-09-2018-2004

Hagues, R. (2019). Conducting critical ethnography: Personal reflections on the role of the researcher. *International Social Work*, *64*(3), 002087281881973. https://doi.org/10.1177/0020872818819731

Hamilton, A. B., & Finley, E. P. (2019). Qualitative methods in implementation research: an introduction. *Psychiatry Research*, *280*, 112516. https://doi.org/10.1016/j.psychres.2019.112516

Harvey, E. J., Rubin, L. F., Smiley, S. L., Zhou, Y., Elmasry, H., & Pearson, J. L. (2018). Mobile phone ownership is not a serious barrier to participation in studies: Descriptive Study. *JMIR MHealth and UHealth*, *6*(2), e21. https://doi.org/10.2196/mhealth.8123

Haven, T. L., & Van Grootel, D. L. (2019). Preregistering qualitative research. *Accountability in Research*, *26*(3), 229–244. https://doi.org/10.1080/08989621.2019.1580147

Hilger, A., Rose, M., & Wanner, M. (2018). Changing faces - Factors influencing the roles of researchers in real-world laboratories. *GAIA - Ecological Perspectives for Science and Society*, *27*(1), 138–145. https://doi.org/10.14512/gaia.27.1.9

Holtrop, J. S., & Glasgow, R. E. (2020). Pragmatic research: An introduction for clinical practitioners. *Family Practice*, *37*(3), 424–428. https://doi.org/10.1093/fampra/cmz092

Hooper, V., & Blunt, C. (2019). Factors influencing the information security behaviour of IT employees. *Behaviour & Information Technology*, *39*(8), 1–13. https://doi.org/10.1080/0144929x.2019.1623322

Hoorani, B. H., Nair, L. B., & Gibbert, M. (2019). Designing for impact: The effect of rigor and case study design on citations of qualitative case studies in management. *Scientometrics*, *121*(1), 285–306. https://doi.org/10.1007/s11192-019-03178-w

Hu, W., Liu, J., Huang, T., & Liu, Y. (2018). A completion time-based flow scheduling for Inter-data center traffic optimization. *IEEE Access*, *6*(1), 26181–26193. https://doi.org/10.1109/access.2018.2834482

Huarng, K. H., Rey-Martí, A., & Miquel-Romero, M. J. (2018). Quantitative and qualitative comparative analysis in business. *Journal of Business Research*, *89*, 171–174. https://doi.org/10.1016/j.jbusres.2018.02.032

Hurst, K., & Stern, M. J. (2020). Messaging for environmental action: The role of moral framing and message source. *Journal of Environmental Psychology*, *68*, 101394. https://doi.org/10.1016/j.jenvp.2020.101394

Ibrahim, A. S., Hartjes, T. M., Rivera, L., Adebayo, A., Pierre, L., & Scruth, E. (2019). Mentoring researchers in resource-poor countries. *Clinical Nurse Specialist*, *33*(1), 7–11. https://doi.org/10.1097/nur.0000000000000413

Iivari, N. (2018). Using member checking in interpretive research practice. *Information Technology & People*, *31*(1), 111–133. https://doi.org/10.1108/itp-07-2016-0168

Ivankova, N., & Wingo, N. (2018). Applying mixed methods in action research: methodological potentials and advantages. *American Behavioral Scientist*, *62*(7), 978–997. https://doi.org/10.1177/0002764218772673

Jain, N. (2021). Survey versus interviews: Comparing data collection tools for exploratory research. *The Qualitative Report*, *26*(2). https://doi.org/10.46743/2160-3715/2021.4492

Jansen, J., & van Schaik, P. (2019). The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human-Computer Studies*, *123*, 40–55. https://doi.org/10.1016/j.ijhcs.2018.10.004

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549. https://doi.org/10.2307/25750691

Jung, E. S., LIiu, S., Kettimuthu, R., & Chung, S. (2019). High-performance End-to-End integrity verification on big data transfer. *IEICE Transactions on Information and Systems*, *E102.D*(8), 1478–1488. https://doi.org/10.1587/transinf.2018edp7297

Kamoun-Abid, F., Rekik, M., Meddeb-Makhlouf, A., & Zarai, F. (2021). Secure architecture for Cloud/Fog computing based on firewalls and controllers. *Procedia Computer Science*, *192*(1), 822–833. https://doi.org/10.1016/j.procs.2021.08.085

Kaur, S. J., Ali, L., Hassan, M. K., & Al-Emran, M. (2021). Adoption of digital banking channels in an emerging economy: exploring the role of in-branch efforts. *Journal of Financial Services Marketing*, *26*(2). https://doi.org/10.1057/s41264-020-00082-w

Kellam, N., & Cirell, A. M. (2018). Quality considerations in qualitative inquiry: expanding our understandings for the broader dissemination of qualitative research. *Journal of Engineering Education*, *107*(3), 355–361. https://doi.org/10.1002/jee.20227

Kelley-Quon, L. I. (2018). Surveys: Merging qualitative and quantitative research methods. *Seminars in Pediatric Surgery*, *27*(6), 361–366. https://doi.org/10.1053/j.sempedsurg.2018.10.007

Khuntia, J., Saldanha, T. J. V., Mithas, S., & Sambamurthy, V. (2018). Information technology and sustainability: Evidence from an emerging economy. *Production and Operations Management*, *27*(4), 756–773. https://doi.org/10.1111/poms.12822

Kiljan, S., Vranken, H., & van Eekelen, M. (2018). Evaluation of transaction authentication methods for online banking. *Future Generation Computer Systems*, *80*, 430–447. https://doi.org/10.1016/j.future.2016.05.024

Kim, J., Yang, K., Min, J., & White, B. (2021). Hope, fear, and consumer behavioral change amid COVID□19: Application of protection motivation theory. *International Journal of Consumer Studies*, *2021*(00), 1–17. https://doi.org/10.1111/ijcs.12700

Kolman, J. M., & Miller, S. M. (2018). Six values never to silence: Jewish perspectives on nazi medical professionalism. *Rambam Maimonides Medical Journal*, *9*(1), e0007. https://doi.org/10.5041/rmmj.10327

Korać, D., Damjanović, B., & Simić, D. (2021). A model of digital identity for better information security in E-learning systems. *The Journal of Supercomputing*, *78*(3), 3325–3354. https://doi.org/10.1007/s11227-021-03981-4

Kumar, S., Akbar Abbas Jafri, S., Nigam, N., Gupta, N., Gupta, G., & Singh, S. K. (2020). A new user identity based authentication, using security and distributed for cloud computing. *IOP Conference Series: Materials Science and Engineering*, *748*(1), 12026. https://doi.org/10.1088/1757-899x/748/1/012026

LaDonna, K. A., Taylor, T., & Lingard, L. (2018). Why open-ended survey questions are unlikely to support rigorous qualitative insights. *Academic Medicine*, *93*(3), 347–349. https://doi.org/10.1097/acm.0000000000002088

Lamontagne, C., Sénécal, S., Fredette, M., Labonté-LeMoyne, É., & Léger, P. M. (2021). The effect of the segmentation of video tutorials on User's training experience and performance. *Computers in Human Behavior Reports*, *3*, 100071. https://doi.org/10.1016/j.chbr.2021.100071

Lester, J. N., Cho, Y., & Lochmiller, C. R. (2020). Learning to do qualitative data analysis: A starting point. *Human Resource Development Review*, *19*(1), 94–106. https://doi.org/10.1177/1534484320903890

Levitan, J., Mahfouz, J., & Schussler, D. L. (2018). Pragmatic identity analysis as a qualitative interview technique. *Forum, Qualitative Social Research*, *19*(3), 1–22. https://doi.org/10.17169/fqs19.3.3032

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior.

International Journal of Information Management, *45*, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Liu, Y., Liu, A., Liu, X., & Huang, X. (2019). A statistical approach to participant selection in location-based social networks for offline event marketing. *Information Sciences*, *480*, 90–108. https://doi.org/10.1016/j.ins.2018.12.028

Lo, F. Y., Rey-Martí, A., & Botella-Carrubi, D. (2020). Research methods in business: Quantitative and qualitative comparative analysis. *Journal of Business Research*, *115*, 221–224. https://doi.org/10.1016/j.jbusres.2020.05.003

Losavio, M. (2020). Fog computing, edge computing and a return to privacy and personal autonomy. *Procedia Computer Science*, *171*, 1750–1759. https://doi.org/10.1016/j.procs.2020.04.188

Luchkina, N. V., & Bolshakov, V. Y. (2018). Mechanisms of fear learning and extinction: synaptic plasticity–fear memory connection. *Psychopharmacology*, *236*(1), 163–182. https://doi.org/10.1007/s00213-018-5104-4

Maher, C., Hadfield, M., Hutchings, M., & de Eyto, A. (2018). Ensuring rigor in qualitative data analysis. *International Journal of Qualitative Methods*, *17*(1), 160940691878636. https://doi.org/10.1177/1609406918786362

Maitlo, A., Ameen, N., Peikari, H. R., & Shah, M. (2019). Preventing identity theft. *Information Technology & People*, *32*(5), 1184-1214. https://doi.org/10.1108/itp-05-2018-0255

Mani, Z., & Chouk, I. (2019). Impact of privacy concerns on resistance to smart services: Does the “Big Brother effect” matter? *Journal of Marketing Management*, *35*(15-16), 1–20. https://doi.org/10.1080/0267257x.2019.1667856

Matta, P., Arora, M., & Sharma, D. (2021). A comparative survey on data encryption Techniques: Big data perspective. *Materials Today: Proceedings*, *46*(2021), 11035–11039. https://doi.org/10.1016/j.matpr.2021.02.153

Mawhinney, L., & Rinke, C. R. (2018). The balance and imbalance of sampling former teachers hidden-by-choice: A snowball in summer. *International Journal of Research & Method in Education*, *42*(5), 502–512. https://doi.org/10.1080/1743727x.2018.1513480

Maxwell, J. A. (2019). Distinguishing between quantitative and qualitative research: A response to Morgan. *Journal of Mixed Methods Research*, *13*(2), 155868981982825. https://doi.org/10.1177/1558689819828255

Mbama, C. I., Ezepue, P., Alboul, L., & Beer, M. (2018). Digital banking, customer experience and financial performance. *Journal of Research in Interactive Marketing*, *12*(4), 432–451. https://doi.org/10.1108/jrim-01-2018-0026

McEvoy, R., Tierney, E., & MacFarlane, A. (2019). Participation is integral: understanding the levers and barriers to the implementation of community participation in primary healthcare: a qualitative study using normalization process theory. *BMC Health Services Research*, *19*(1). https://doi.org/10.1186/s12913-019-4331-7

McGrath, C., Palmgren, P. J., & Liljedahl, M. (2018). Twelve tips for conducting qualitative research interviews. *Medical Teacher*, *41*(9), 1–5. https://doi.org/10.1080/0142159x.2018.1497149

McKenna, L., & Gray, R. (2018). The importance of ethics in research publications. *Collegian*, *25*(2), 147–148. https://doi.org/10.1016/j.colegn.2018.02.006

Megargel, A., & Shankarararman, V. (2020). Digital banking accelerator: A service-oriented architecture starter kit for banks. *IEEE Software*, *38*(3), 106–112. https://doi.org/10.1109/ms.2020.3029876

Mehraj, H., Jayadevappa, D., Haleem, S. L. A., Parveen, R., Madduri, A., Ayyagari, M. R., & Dhabliya, D. (2021). Protection Motivation Theory using multi-factor authentication for providing security over social networking sites. *Pattern Recognition Letters*, *152*(1), 218–224. https://doi.org/10.1016/j.patrec.2021.10.002

Melnychenko, S., Volosovych, S., & Baraniuk, Y. (2020). Dominant ideas of financial technologies in digital banking. *Baltic Journal of Economic Studies*, *6*(1), 92. https://doi.org/10.30525/2256-0742/2020-6-1-92-99

Meske, C., Wilms, K., & Stieglitz, S. (2019). Enterprise social networks as digital infrastructures - Understanding the utilitarian value of social media at the workplace. *Information Systems Management*, *36*(4), 350–367. https://doi.org/10.1080/10580530.2019.1652448

Monaro, M., Gamberini, L., Zecchinato, F., & Sartori, G. (2018). False identity detection using complex sentences. *Frontiers in Psychology*, *9*(6), 564–581. https://doi.org/10.3389/fpsyg.2018.00283

Moreira, F. R., Da Silva Filho, D. A., Nze, G. D. A., de Sousa Júnior, R. T., & Nunes, R. R. (2021). Evaluating the performance of NIST's framework cybersecurity controls through a constructivist multicriteria methodology. *IEEE Access*, *9*, 129605–129618. https://doi.org/10.1109/ACCESS.2021.3113178

Mousavi, R., Chen, R., Kim, D. J., & Chen, K. (2020). Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. *Decision Support Systems*, *135*(2020), 113323. https://doi.org/10.1016/j.dss.2020.113323

Nakamura, S., Enokido, T., & Takizawa, M. (2020). Time based legality of information flow in the capability based access control model for the Internet of Things. *Concurrency and Computation: Practice and Experience*, *33*(23). https://doi.org/10.1002/cpe.5944

Natow, R. S. (2019). The use of triangulation in qualitative studies employing elite interviews. *Qualitative Research*, *20*(2), 146879411983007. https://doi.org/10.1177/1468794119830077

Ng, K. C., Zhang, X., Thong, J. Y. L., & Tam, K. Y. (2021). Protecting against threats to information security: An attitudinal ambivalence perspective. *Journal of Management Information Systems*, *38*(3), 732–764. https://doi.org/10.1080/07421222.2021.1962601

O'Connor, C., & Joffe, H. (2020). Intercoder reliability in qualitative research: Debates and practical guidelines. *International Journal of Qualitative Methods*, *19*, 160940691989922. https://doi.org/10.1177/1609406919899220

Oertzen, A. S., & Odekerken-Schröder, G. (2019). Achieving continued usage in online banking: A post-adoption study. *International Journal of Bank Marketing*, *37*(6), 1394–1418. https://doi.org/10.1108/ijbm-09-2018-0239

Ogbanufe, O., & Pavur, R. (2022). Going through the emotions of regret and fear: Revisiting protection motivation for identity theft protection. *International Journal of Information Management*, *62*, 102432. https://doi.org/10.1016/j.ijinfomgt.2021.102432

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. *Cryptography*, *2*(1), 1. https://doi.org/10.3390/cryptography2010001

Özmen, M. U., & Yucel, E. (2019). Handling of online information by users: Evidence from TED talks. *Behaviour & Information Technology*, *38*(12), 1309–1323. https://doi.org/10.1080/0144929x.2019.1584244

Pallisera, M. (2019). The control of access to participants as a form of protection and self-protection: a challenge for researchers - a response to Williams. *European Journal of Special Needs Education*, *35*(1), 19–20. https://doi.org/10.1080/08856257.2019.1687558

Pang, S. M., Tan, B. C., & Lau, T. C. (2021). Antecedents of consumers' purchase intention towards organic food: Integration of theory of planned behavior and protection motivation theory. *Sustainability*, *13*(9), 5218. https://doi.org/10.3390/su13095218

Paradis, E., & Varpio, L. (2018). Difficult but important questions about the ethics of qualitative research. *Perspectives on Medical Education*, *7*(2), 65–66. https://doi.org/10.1007/s40037-018-0414-0

Pedrosa, I., Costa, C. J., & Aparicio, M. (2019). Determinants adoption of computer-assisted auditing tools (CAATs). *Cognition, Technology & Work*, *22*(3), 565–583. https://doi.org/10.1007/s10111-019-00581-4

Perchoux, C., Chaix, B., & Kestens, Y. (2019). Activity spaces in place and health research: Novel exposure measures, data collection tools, and designs. *Health & Place*, *58*, 102130. https://doi.org/10.1016/j.healthplace.2019.05.008

Piquero, N. L., Piquero, A. R., Gies, S., Green, B., Bobnis, A., & Velasquez, E. (2021). Preventing identity theft: Perspectives on technological solutions from industry insiders. *Victims & Offenders*, *16*(3), 444–463. https://doi.org/10.1080/15564886.2020.1826023

Poe, S. S., Dawson, P. B., Cvach, M., Burnett, M., Kumble, S., Lewis, M., Thompson, C. B., & Hill, E. E. (2018). The Johns Hopkins fall risk assessment tool: A study of reliability and validity. *Journal of Nursing Care Quality*, *33*(1), 10–19. https://doi.org/10.1097/NCQ.0000000000000301

Rahi, S., Abd. Ghani, M., Alnaser, F. M., & Ngah, A. H. (2018). Investigating the role of unified theory of acceptance and use of technology (UTAUT) in internet banking adoption context. *Management Science Letters*, *8*(3), 173–186. https://doi.org/10.5267/j.msl.2018.1.001

Rajab, M., & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security*, *80*, 211–223. https://doi.org/10.1016/j.cose.2018.09.016

Ramanadhan, S., Revette, A. C., Lee, R. M., & Aveling, E. L. (2021). Pragmatic approaches to analyzing qualitative data for implementation science: An introduction. *Implementation Science Communications*, *2*(1) 1-10. https://doi.org/10.1186/s43058-021-00174-1

Rawson, N. S. B., & D'Arcy, C. (2018). Healthcare databases for drug safety research: Data validity assessment remains crucial. *Drug Safety*, *41*(9), 829–833. https://doi.org/10.1007/s40264-018-0673-z

Raza, M. S., Zhan, Q., & Rubab, S. (2020). Role of money mules in money laundering and financial crimes a discussion through case studies. *Journal of Financial Crime*, *27*(3), 911–931. https://doi.org/10.1108/jfc-02-2020-0028

Reis, J., Amorim, M., & Melão, N. (2019). Multichannel service failure and recovery in a O2O era: A qualitative multi-method research in the banking services industry. *International Journal of Production Economics*, *215*, 24–33. https://doi.org/10.1016/j.ijpe.2018.07.001

Ricci, J., Breitinger, F., & Baggili, I. (2018). Survey results on adults and cybersecurity education. *Education and Information Technologies*, *24*(1), 231–249. https://doi.org/10.1007/s10639-018-9765-8

Richard, B., Sivo, S. A., Orlowski, M., Ford, R. C., Murphy, J., Boote, D. N., & Witta, E. L. (2020). Qualitative research via focus groups: Will going online affect the diversity of your findings? *Cornell Hospitality Quarterly*, *62*(1), 32–45. https://doi.org/10.1177/1938965520967769

Rikhardsson, P., Singh, K., & Best, P. (2019). Exploring continuous auditing solutions and internal auditing: A research note. *Journal of Accounting and Management Information Systems*, *18*(4). https://doi.org/10.24818/jamis.2019.04006

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rose, J., & Johnson, C. W. (2020). Contextualizing reliability and validity in qualitative research: toward more rigorous and trustworthy qualitative social science in leisure research. *Journal of Leisure Research*, *51*(4), 1–20. https://doi.org/10.1080/00222216.2020.1722042

Rose, R. V. (2019). New NIST revisions – What do they mean for regulatory compliance? *EDPACS*, *59*(6), 5–13. https://doi.org/10.1080/07366981.2019.1642559

Saks, M. J. (2018). Methodological triangulation. *Nature Human Behaviour*, *2*(11), 806–807. https://doi.org/10.1038/s41562-018-0458-5

Salarvand, S., Mousavi, M. S., Esmaeilbeigy, D., Changaee, F., & Almasian, M. (2020). The perceived health needs of primiparous mothers referring to primary health care centers: A qualitative study. *International Journal of Women's Health*, *Volume 12*, 745–753. https://doi.org/10.2147/ijwh.s258446

Schuetz, S. W., Benjamin Lowry, P., Pienta, D. A., & Bennett Thatcher, J. (2020). The effectiveness of abstract versus concrete fear appeals in information security. *Journal of Management Information Systems*, *37*(3), 723–757. https://doi.org/10.1080/07421222.2020.1790187

Schupmann, W., & Moreno, J. D. (2020). Belmont in context. *Perspectives in Biology and Medicine*, *63*(2), 220–239. https://doi.org/10.1353/pbm.2020.0028

Sebele-Mpofu, F. Y. (2020). Saturation controversy in qualitative research: Complexities and underlying assumptions. A literature review. *Cogent Social Sciences*, *6*(1), 1838706. https://doi.org/10.1080/23311886.2020.1838706

Shah, S. W., & Kanhere, S. S. (2019). Recent trends in user authentication – A survey. *IEEE Access*, *7*(2019), 112505–112519. https://doi.org/10.1109/access.2019.2932400

Shahbaznezhad, H., Kolini, F., & Rashidirad, M. (2020). Employees' behavior in phishing attacks: What individual, organizational, and technological factors matter? *Journal of Computer Information Systems*, *61*(6), 539–550. https://doi.org/10.1080/08874417.2020.1812134

Sharma, M. K., & Nene, M. J. (2020). Dual factor third party biometric based authentication scheme using quantum one-time passwords. *Security and Privacy*, *3*(6), 1–18. https://doi.org/10.1002/spy2.129

Sinigaglia, F., Carbone, R., Costa, G., & Zannone, N. (2020). A survey on multi-factor authentication for online banking in the wild. *Computers & Security*, *95*, 101745. https://doi.org/10.1016/j.cose.2020.101745

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems*, *44*(1), 100548. https://doi.org/10.1016/j.accinf.2021.100548

Snider, S. E., DeHart, W. B., Epstein, L. H., & Bickel, W. K. (2019). Does delay discounting predict maladaptive health and financial behaviors in smokers? *Health Psychology*, *38*(1), 21–28. https://doi.org/10.1037/hea0000695

Snyder, J., & Cistulli, M. D. (2020). Social media efficacy and workplace relationships. *Corporate Communications: An International Journal*, *25*(3), 463–476. https://doi.org/10.1108/ccij-01-2020-0006

Soilemezi, D., & Linceviciute, S. (2018). Synthesizing qualitative research. *International Journal of Qualitative Methods*, *17*(1), 160940691876801. https://doi.org/10.1177/1609406918768014

Solovyev, A. V. (2020). Authentication control algorithm for long-term keeping of digital data. *IOP Conference Series: Materials Science and Engineering*, *862*(5), 052080. https://doi.org/10.1088/1757-899x/862/5/052080

Sommestad, T., Karlzén, H., & Hallberg, J. (2018). The theory of planned behavior and information security policy compliance. *Journal of Computer Information Systems*, *59*(4), 344–353. https://doi.org/10.1080/08874417.2017.1368421

Son, Y., Kwon, H. E., Tayi, G. K., & Oh, W. (2019). Impact of customers' digital banking adoption on hidden defection: A combined analytical–empirical approach. *Journal of Operations Management*, *66*(4), 418–440. https://doi.org/10.1002/joom.1066

Srivastava, C., Goli, M., & Vandana, V. (2021). Adoption of contactless payments during Covid 19 pandemic an integration of protection motivation theory (PMT) and unified theory of acceptance and use of technology (UTAUT). *Academy of Marketing Studies Journal*, *25*(1), 1–20. https://www.abacademies.org/abstract/adoption-of-contactless-payments-during-covid-19-pandemic-an-integration-of-protection-motivation-theory-pmt-and-unified-9970.html

Srivastava, P., & Hopwood, N. (2018). Reflection/commentary on a past article: "A Practical Iterative Framework for Qualitative Data Analysis." *International Journal of Qualitative Methods*, *17*(1), 160940691878820. https://doi.org/10.1177/1609406918788204

Stafford, T., Deitz, G., & Li, Y. (2018). The role of internal audit and user training in information security policy compliance. *Managerial Auditing Journal*, *33*(4), 410–424. https://doi.org/10.1108/maj-07-2017-1596

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society*, *71*, 15–29. https://doi.org/10.1016/j.aos.2018.04.005

Stenfors, T., Kajamaa, A., & Bennett, D. (2020). How to assess the quality of qualitative research. *The Clinical Teacher*, *17*(6). https://doi.org/10.1111/tct.13242

Stewart, H., & Jürjens, J. (2018). Data security and consumer trust in FinTech innovation in Germany. *Information and Computer Security*, *26*(1), 109–128. https://doi.org/10.1108/ics-06-2017-0039

Strickland, J. C., & Stoops, W. W. (2019). Utilizing content-knowledge questionnaires to assess study eligibility and detect deceptive responding. *The American Journal of Drug and Alcohol Abuse*, *46*(2), 149–157. https://doi.org/10.1080/00952990.2019.1689990

Syniavska, O., Dekhtyar, N., Deyneka, O., Zhukova, T., & Syniavska, O. (2019). Security of e-banking systems: Modelling the process of counteracting e-banking fraud. *SHS Web of Conferences*, *65*, 1–5. https://doi.org/10.1051/shsconf/20196503004

Taylor, A. K., Armitage, S., & Kausar, A. (2021). A challenge in qualitative research: Family members sitting in on interviews about sensitive subjects. *Health Expectations*, *24*(4), 1545–1546. https://doi.org/10.1111/hex.13263

Team, V., Bugeja, L., & Weller, C. D. (2018). Barriers and facilitators to participant recruitment to randomised controlled trials: A qualitative perspective. *International Wound Journal*, *15*(6), 929–942. https://doi.org/10.1111/iwj.12950

Teece, A., Baker, J., & Smith, H. (2021). Understanding the decision making of critical care nurses when restraining a patient with psychomotor agitation secondary to hyperactive delirium: A "Think Aloud" study. *Journal of Clinical Nursing*, *31*(1-2), 121–133. https://doi.org/10.1111/jocn.15889

Teh, P. S., Zhang, N., Tan, S. Y., Shi, Q., Khoh, W. H., & Nawaz, R. (2019). Strengthen user authentication on mobile devices by using user's touch dynamics pattern. *Journal of Ambient Intelligence and Humanized Computing*, *11*(10), 4019–4039. https://doi.org/10.1007/s12652-019-01654-y

Trevisan, F., Bello, B., Vaughan, M., & Vromen, A. (2019). Mobilizing personal narratives: The rise of digital story banking in U.S. grassroots advocacy. *Journal of Information Technology & Politics*, *17*(2), 146–160. https://doi.org/10.1080/19331681.2019.1705221

Uddin, M. H., Mollah, S., & Ali, M. H. (2020). Does cyber tech spending matter for bank stability? *International Review of Financial Analysis*, *72*, 101587. https://doi.org/10.1016/j.irfa.2020.101587

van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*, *123*, 29–39. https://doi.org/10.1016/j.ijhcs.2018.11.003

Vasilev, Y. S., Zegzhda, D. P., & Poltavtseva, M. A. (2018). Problems of security in digital production and its resistance to cyber threats. *Automatic Control and Computer Sciences*, *52*(8), 1090–1100. https://doi.org/10.3103/s0146411618080254

Vasilomanolakis, E., & Mühlhäuser, M. (2018). Detection and mitigation of monitor identification attacks in collaborative intrusion detection systems. *International Journal of Network Management*, *29*(2), e2059. https://doi.org/10.1002/nem.2059

Veale, M., & Brown, I. (2020). Cybersecurity. *Internet Policy Review*, *9*(4), 1–21. https://doi.org/10.14763/2020.4.1533

Vedadi, A., & Warkentin, M. (2018). Secure behavior over time: Perspectives from the theory of process memory. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *49*(1), 39–48. https://doi.org/10.1145/3210530.3210534

Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers & Security*, *77*, 860–870. https://doi.org/10.1016/j.cose.2018.03.008

Vučković, Z., Vukmirović, D., Milenković, M. J., Ristić, S., & Prljić, K. (2018). Analyzing of e-commerce user behavior to detect identity theft. *Physica A: Statistical Mechanics and Its Applications*, *511*, 331–335. https://doi.org/10.1016/j.physa.2018.07.059

Wall, J. D., & Warkentin, M. (2019). Perceived argument quality's effect on threat and coping appraisals in fear appeals: An experiment and exploration of realism check heuristics. *Information & Management*, *56*(8), 103157. https://doi.org/10.1016/j.im.2019.03.002

Wang, B., Li, W., & Xiong, N. N. (2019). Time-based access control for multi-attribute data in Internet of Things. *Mobile Networks and Applications*, *26*(2), 797–807. https://doi.org/10.1007/s11036-019-01327-2

Weil, T. (2018). Taking compliance to the cloud—Using ISO standards (Tools and Techniques). *IT Professional*, *20*(6), 20–30. https://doi.org/10.1109/mitp.2018.2877312

Wiafe, I., Koranteng, F. N., Obeng, E. N., Assyne, N., Wiafe, A., & Gulliver, S. R. (2020). Artificial intelligence for cybersecurity: A systematic mapping of literature. *IEEE Access*, *8*, 146598–146612. https://doi.org/10.1109/access.2020.3013145

Wieder, J. S. (2019). Communicating radiation risk: The power of planned, persuasive messaging. *Health Physics*, *116*(2), 207–211. https://doi.org/10.1097/hp.0000000000000998

Wolnik, D., Cheek, J., & Weaver, M. (2018). Designing effective, scalable data collection tools to measure farmers market impacts. *Journal of Agriculture, Food Systems, and Community Development*, *18*(1), 1–17. https://doi.org/10.5304/jafscd.2018.08c.003

Wu, D. (2019). Empirical study of knowledge withholding in cyberspace: Integrating protection motivation theory and theory of reasoned behavior. *Computers in Human Behavior*, *105*, 106229. https://doi.org/10.1016/j.chb.2019.106229

Wu, X., Xu, J., Wang, J., Li, Y., Li, W., & Guo, Y. (2019). Identity authentication on mobile devices using face verification and ID image recognition. *Procedia Computer Science*, *162*, 932–939. https://doi.org/10.1016/j.procs.2019.12.070

Xu, A., Baysari, M. T., Stocker, S. L., Leow, L. J., Day, R. O., & Carland, J. E. (2020). Researchers' views on, and experiences with, the requirement to obtain informed consent in research involving human participants: a qualitative study. *BMC Medical Ethics*, *21*(1). https://doi.org/10.1186/s12910-020-00538-7

Yen, J. C., Lim, J. H., Wang, T., & Hsu, C. (2018). The impact of audit firms' characteristics on audit fees following information security breaches. *Journal of Accounting and Public Policy*, *37*(6), 489–507. https://doi.org/10.1016/j.jaccpubpol.2018.10.002

Ylang, N. (2020). Capable guardianship against identity theft. *Journal of Financial Crime*, *27*(1), 130–142. https://doi.org/10.1108/jfc-12-2018-0140

Zapata-Barrero, R., & Yalaz, E. (2020). Qualitative migration research ethics: a roadmap for migration scholars. *Qualitative Research Journal*, *20*(3), 269–279. https://doi.org/10.1108/qrj-02-2020-0013

Zhang, X., Liu, S., Wang, L., Zhang, Y., & Wang, J. (2019). Mobile health service adoption in China. *Online Information Review*, *44*(1), 1–23. https://doi.org/10.1108/oir-11-2016-0339

Zhao, X., Roditis, M. L., & Alexander, T. N. (2019). Fear and humor appeals in "the real cost" campaign: Evidence of potential effectiveness in message pretesting.

American Journal of Preventive Medicine, *56*(2), S31–S39.

https://doi.org/10.1016/j.amepre.2018.07.033

Appendix A: Interview Protocol

Project: Walden University Doctorate of Information Technology Study

Type of Interview:

Date:

Location:

Interviewer's Details:

Interviewee's Details:

Interviewee's Profession:

Pre-interview

I will initiate contact with the target participants in LinkedIn and other social media with the study invitation and determine the date and time they will be available via email. I will indicate 20 minutes time limit for the interviews. Due to COVID-19 restrictions, the interviews will be conducted via Zoom. Interviewees are required to select a quiet and isolated room. Interviewees should avoid having other responsibilities during the interview session to minimize distractions. An overview and purpose of the study will be given at the start of the session. I will inform the interviewees that interview audio will be recorded and note will be taken. I will confirm if the interviewees agree with audio recording and will provide recorded audio copy if it is required. I will test the digital audio recorder to ensure it works very well before interview. The consent form assures their confidentiality, but the interviewer will reiterate the processes that are in place to guarantee their confidentiality and that they are allowed to stop participating in the study at any time. Interviewees' consent forms will be obtained digitally before the start of the interview.

The research question is what strategies do IT security professionals use to mitigate identity-based authentication attacks that affect digital privacy in online banking?

Pre-interview questions

1. Briefly describe:

    a. Your professional background

    b. Your experience with banking platform

2. How many users have you supported?

3. How would you define identity-based authentication attacks?

Interview questions

1. What strategies have you implemented to support digital privacy?
2. What strategies have you implemented to ensure users comply with digital privacy rules when registering or using online payment platforms?
3. What strategies do you use against data breaches?
4. What procedures have you used to conduct internal compliance audit to protect user's privacy?
5. How do you deal with identity-based authentication attacks?
6. What is involved in following up identity-theft cases on your network?
7. What type of information is typically lost in identity-based authentication attacks?
8. What policies are in place to improve the information security awareness by end-users?

9. What procedures are involved in resolving identity-based authentication attacks cases?
10. How would you describe your proficiency in handling identity-based authentication attacks on your network?
11. How often do you update digital privacy policies?
12. What type of mitigation techniques have you integrated into your protection strategies against identity-based authentication attacks?

Appendix B: Interview Consent Form

You are invited to take part in a research study about challenges of digital privacy in banking organizations. This form is part of a process called "informed consent" to allow you to understand this study before deciding whether to take part.

This study seeks 3-7 volunteers who are: IT security professionals with at least 5 years of online banking experience and must be age of 18 years old or older.

This study is being conducted by a researcher named Okechukwu Ogudebe, who is a doctoral student at Walden University.

Interested participants have 10 business days to review the study information and ask questions before giving their consent. Participants are required to select a quiet venue/room to avoid distractions during the interview.

Study Purpose:

The purpose of this study is to examine the strategies IT security professionals working on internet banking platforms use to mitigate identity-based authentication attacks affecting digital privacy in online banking.

Procedures:

This study will involve you completing the following steps:

- I the interviewer will be recording your input (audio). Also, interviewer will be taking notes during the interview. The interviews will be conducted via Zoom. The duration of the interview will be between 20-30 minutes.
- After the interviews, I will transcribe the interview and write up the findings. I will present each participant with my analysis of the interview for their review.

This will allow the participants to ensure the accuracy of my interpretation. Within one week from the interview, I will provide participants with the opportunity to review my analysis of the data collected during the interview. Participants review should take between 20-30 minutes.

Here are some sample questions:

1. What strategies have you implemented to support digital privacy?

2. What strategies have you implemented to ensure users comply with digital privacy rules when registering or using online payment platforms?

3. What strategies do you use against data breaches?

Voluntary Nature of the Study:

Research should only be done with those who freely volunteer. So everyone involved will respect your decision to join or not. If you decide to join the study now, you can still change your mind later. You may stop at any time.

Risks and Benefits of Being in the Study:

Being in this study could involve some risk of the minor discomforts that can be encountered in daily life such as discomfort from sitting for the interview and discomfort from the lighting in the interview location. Being in this study would not pose risk to your safety or wellbeing.

This study offers no direct benefits to individual volunteers. The aim of this study is to benefit society. Potential benefits to participating in this study are to help the IT community address a serious and increasing issue in relation to data security as well as potentially assisting with decreasing the number of identity thefts that occur annually. Once the analysis is complete, the researcher will share the overall results by email.

Payment

Participation in this study is voluntary, there will be no monetary compensation.

Privacy:

The researcher is required to protect your privacy. Your identity will be kept safe and confidential, within the limits of the law. The researcher will not use your personal information for any purposes outside of this research project. Also, the researcher will not include your name or anything else that could identify you in the study reports. If the researcher were to share this dataset with another researcher in the future, the dataset would contain no identifiers so this would not involve another round of obtaining informed consent. Data will be kept secure by the researcher and it is stored in his house in an encrypted drive. Data will be kept for a period of at least 5 years, as required by the university.

Contacts and Questions:

You can ask questions of the researcher by email (okechukwu.ogudebe@waldenu.edu). If you want to talk privately about your rights as a participant or any negative parts of the study, you can call Walden University's Research Participant Advocate at 612-312-1210. Walden University's approval number for this study is 12-21-21-1000257. It expires on December 20, 2022.

You might wish to retain this consent form for your records. You may ask the researcher or Walden University for a copy at any time using the contact info above.

Obtaining Your Consent

If you feel you understand the study and wish to volunteer, please indicate your consent by replying to this email with the words, I consent.

Interview questions

1. What strategies have you implemented to support digital privacy?
2. What strategies have you implemented to ensure users comply with digital privacy rules when registering or using online payment platforms?
3. What strategies do you use against data breaches?
4. What procedures have you used to conduct internal compliance audit to protect user's privacy?
5. How do you deal with identity-based authentication attacks?
6. What is involved in following up identity-theft cases on your network?
7. What type of information is typically lost in identity-based authentication attacks?
8. What policies are in place to improve the information security awareness by end-users?
9. What procedures are involved in resolving identity-based authentication attacks cases?
10. How would you describe your proficiency in handling identity-based authentication attacks on your network?
11. How often do you update digital privacy policies?

12. What type of mitigation techniques have you integrated into your protection strategies against identity-based authentication attacks?