CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL

Volume 5, No. 2
October 2026
ISSN: 2832-1006

In this issue:

4. **Bridging the Cybersecurity Skills Gap by Leveraging Cybersecurity Clinics: Developing the Arizona Cybersecurity Clinic**
Paul Wagner, University of Arizona
Robert Honomichl, University of Arizona
Shengjie Xu, University of Arizona

34. **What is Cybersecurity (or Cyber Security)? Answer [Still] Loading…**
Maguire Parsley, University of North Carolina Wilmington
Luke Warpula, University of North Carolina Wilmington
Ulku Clark, University of North Carolina Wilmington
Geoff Stoker, University of North Carolina Wilmington

59. **Enhancing Cyber Defense: A Federated Multi-Modal Deep Learning Framework for Privacy-Preserving Zero-Day Attack Detection**
Samuel Sambasivam, Woodbury University

78. **Evaluating Eleven Online CTF Platforms for Undergraduate Cybersecurity Competition Preparation**
Brandon P. Grech, Anderson University (SC)

104. **Federated Learning and Edge Computing for Privacy-Preserving Real-Time Predictive Maintenance in Industrial IoT Systems Semantic Technologies for**
Kiran Kumar Vejendla, City University of Seattle
Kyong (Jin) Chang, City University of Seattle
Brian Maeng, City University of Seattle
Sherin Aly, City University of Seattle

117. **Perceived Usefulness of Password Complexity: A Methodology Framework**
Kyle Herman, Georgia Southern University
Hayden Wimmer, Georgia Southern University

132. **Beyond Awareness: Building Digital Resilience Through Comprehensive Cybersecurity Foundations for K-5 Students**
Ellie Ebrahimi, University of North Carolina Wilmington
Yasin Emre Gokce, University of North Carolina Wilmington
Majorie Pare, University of North Carolina Wilmington
Berker Koyuncu, University of North Carolina Wilmington
Jude Vargas, University of North Carolina Wilmington
Jacob Blount, University of North Carolina Wilmington

iscap
Information Systems & Computing Academic Professionals

The **Cybersecurity Pedagogy and Practice Journal** (**CPPJ**) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (https://cppj.info). Our sister publication, the proceedings of the ISCAP Conference (https://proc.iscap.info) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point, papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal.

While the primary path to journal publication is through the ISCAP conference, CPPJ does accept direct submissions at https://iscap.us/papers. Direct submissions are subjected to a double-blind peer review process, where reviewers do not know the names and affiliations of paper authors, and paper authors do not know the names and affiliations of reviewers. All submissions (articles, teaching tips, and teaching cases & notes) to the journal will be refereed by a rigorous evaluation process involving at least three blind reviews by qualified academic, industrial, or governmental computing professionals. Submissions will be judged not only on the suitability of the content but also on the readability and clarity of the prose.

Currently, the acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

2026 ISCAP Board of Directors

Amy Connolly James Madison University President	Michael Smith Georgia Institute of Technology Vice President	Jeff Cummings Univ of NC Wilmington Past President
David Firth University of Montana Director	Mark Frydenberg Bentley University Director/Secretary	Leigh Mutchler James Madison University Director
RJ Podeschi Millikin University Director/Treasurer	Bryan Reinicke Rochester Institute of Technology / Director	Jeffry Babb West Texas A&M University Director/Curricular Matters
Eric Breimer Siena University Director/2026 Conf Chair	Tom Janicki Univ of NC Wilmington Director/Meeting Planner	Xihui "Paul" Zhang University of North Alabama Director/JISE Editor

Copyright ©2026 by Information Systems and Computing Academic Professionals (ISCAP). Permission to make digital or hard copies of all or part of this journal for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial use. All copies must bear this notice and full citation. Permission from the Editor is required to post to servers, redistribute to lists, or utilize in a for-profit or commercial use. Permission requests should be sent to editorcppj@iscap.us.

CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

Editors

Jeffrey Cummings
Co-Editor
University of North Carolina Wilmington

Anthony Serapiglia
Co-Editor
Saint Vincent College

Thomas Janicki
Publisher
University of North Carolina Wilmington

2026 Review Board

Brandon Brown
Coastline College

Shawn Clouse
University of Montana

Jeff Landry
Univ of South Alabama

Li-Jen Lester
Sam Houston State Univ

Jamie Pinchot
Robert Morris University

Samuel Sambasivam
Woodbury University

Shwadhin Sharma
California State University Monterey Bay

Sushma Mishra
Robert Morris University

Kevin Slonka
Saint Francis University

Geoff Stoker
Univ of NC Wilmington

Paul Wagner
University of Arizona

Paul Witman
California Lutheran University

Perceived Usefulness of Password Complexity: A Methodology Framework

Kyle Herman
kherman@georgiasouthern.edu

Hayden Wimmer*
hwimmer@georgiasouthern.edu

School of Computing
Georgia Southern University
Statesboro, GA, USA

Abstract

This exploratory study investigates the factors influencing the adoption of complex passwords through the lens of the Technology Acceptance Model (TAM) by Davis (Davis, 1989). Data was collected via Qualtrics, and survey constructs were adapted from the pertinent Information Systems literature. Using Iterative Independent Variable Selection, Linear Regression and Partial Least Squares Structural Equation Modeling was then utilized to find significant constructs. The analysis found that Attitude towards Use, General Security Orientation, and Perceived Utility were significant predictors of behavioral intention to use complex passwords, explaining over 50% of the variance. The findings are supported by literature emphasizing the growing complexity of cyber security and the critical role of strong, unique passwords amid advancing threats. The study highlights the importance of user perceptions in secure behavior and contributes to understanding how theoretical frameworks like TAM can guide effective cyber security practices.

Keywords: Attitude Towards Use of Complex Passwords, Perceived Usefulness of Complex Passwords, Security Self-Efficacy, Cyber security, Linear Regression Analysis of Password Complexity.

Recommended Citation: Herman, K., Wimmer, H., (2026). Perceived Usefulness of Password Complexity: A Methodology Framework. *Cybersecurity Pedagogy and Practice Journal;* v2(n5) pp 117-131. DOI# https://doi.org/10.62273/OKIB1006

©2026 ISCAP (Information Systems and Computing Academic Professionals)

Perceived Usefulness of Password Complexity: A Methodology Approach

Kyle Herman and Hayden Wimmer

1. INTRODUCTION

Strong, complex passwords help safeguard individual users and their families, friends, and employers (Use Strong Passwords, n.d.). A compromised account can serve as a launch-pad for further attacks, exploiting trust within families or among colleagues in an organization. Gaining access to an email account or social media account enables bad actors to orchestrate scams and masquerade as the victim. In a corporate setting, a breached email account can be leveraged to spread misinformation, deceive high-value targets into revealing sensitive information, or trick them into clicking malicious links that steal credentials or install malware.

While Multi-Factor Authentication (MFA) has been widely adopted as a critical secondary layer of defense, passwords remain the primary authentication mechanism across most digital platforms. Furthermore, MFA systems often rely on primary passwords for account recovery, meaning a weak password can still compromise the entire security chain. Therefore, understanding what drives end-user adoption of complex passwords remains essential.

This study proposes an Iterative Independent Variable Selection (IIVS) method whereby we perform an exhaustive regression technique to determine the most important independent variables by reducing the regression equation to its significant independent variables. We confirm our method using Partial Least Squares (PLS) for latent variable calculation for each construct and model regression from the latent variable scores in SmartPLS 4. This work has the potential to advance information systems research by providing a new method for variable reduction and determining which factors are significant in adoption of technology.

Using Iterative Independent Variable Selection this exploratory study examines user's perceived usefulness of complex passwords. This work seeks to present a two-fold approach. We aim to determine the most salient factors for complex password adoption while also providing a methodological alternative to standard regression techniques.

2. LITERATURE REVIEW

Cybersecurity encompasses the resources, processes, and structures used to protect digital assets and cyberspace-enabled systems from unauthorized access, disruption, or exploitation (Craigen, Diakun-Thibault, et al., 2014). Similarly, the Cybersecurity and Infrastructure Security Agency (CISA) defines cybersecurity as the protection of networks, devices, and data from unauthorized access or criminal use while maintaining the confidentiality, integrity, and availability of information (What is Cybersecurity?, 2021). Within this broader security framework, passwords remain one of the most widely used mechanisms for user authentication. NIST Special Publication 800-132 defines a password or passphrase as a string of characters used to gain access to a restricted resource and establish user identity. Password strength is primarily influenced by length and randomness, particularly when passwords are used to derive cryptographic keys and must withstand offline guessing attacks (Turan, Barker, Burr, & Chen, 2010).

Although technical password requirements are important, their effectiveness is ultimately dependent on user behavior. Modern computing capabilities and automated password-cracking techniques increase the risk associated with weak, predictable, or reused credentials. NIST guidance emphasizes the importance of sufficiently long and unpredictable credentials, while CISA recommends unique passwords for individual accounts. However, enforcing increasingly complex password requirements does not necessarily produce more secure behavior. Instead, security requirements can create a tension between organizational security objectives and users' cognitive limitations.

Adams and Sasse (1999) demonstrated that when security mechanisms interfere with users' primary tasks, individuals frequently develop insecure coping strategies. These behaviors include writing passwords down, selecting predictable patterns, and reusing credentials across multiple accounts (Adams and Sasse, 1999). Herley (2009) further argued that users

often make security decisions based on the perceived costs and benefits of security practices, meaning that policies imposing substantial inconvenience may encourage users to circumvent them rather than comply (Herley, 2009).

Password reuse represents a particularly significant consequence of this usability/security conflict. Florencio and Herley (2007) and Das et al. (2014) found that password reuse is widespread among web users, with reported reuse affecting approximately 43% to 51% of users (Florencio and Herley, 2007) and (Das et al., 2014). Das et al. (2014) further demonstrated that users frequently modify existing passwords in predictable ways to satisfy different website requirements. Although these modifications may technically produce different passwords, predictable transformation patterns can still be exploited by password-cracking algorithms. Consequently, increasing password complexity requirements may not eliminate insecure behavior and can instead encourage users to adopt predictable strategies for managing multiple credentials (Das et al., 2014).

This relationship between security knowledge and actual behavior is commonly described as the attitude–behavior gap. Herath and Rao (2009) found that employees may hold positive attitudes toward security policies while failing to consistently comply with them because immediate concerns such as convenience, productivity, and time savings can outweigh security considerations (Rao, 2009). Vance, Siponen, and Pahnila (2012) similarly identified the importance of habits and protection motivation in sustaining secure behavior. These findings demonstrate that security awareness alone does not guarantee secure password practices. Users may understand the importance of strong passwords while continuing to reuse credentials or select simpler alternatives when security requirements create excessive inconvenience (Vance, Siponen, and Pahnila, 2012).

Because password security depends on both technical requirements and user acceptance, Information Systems researchers have increasingly applied technology acceptance and behavioral models to understand secure password adoption. Davis's (1989) Technology Acceptance Model (TAM) proposes that perceived usefulness and perceived ease of use influence an individual's intention to adopt and use a technology (Davis, 1989). Building on this theoretical foundation, Novakovic et al. (2009) applied the Unified Theory of Acceptance and Use of Technology (UTAUT) to password security. Their findings indicated that perceptions of effort and performance expectancy influence both users' intentions to employ secure passwords and their actual secure behavior. These findings suggest that password policies imposing excessive cognitive or usability burdens can generate negative attitudes and encourage policy avoidance (Novakovic et al, 2009).

Other research reinforces the importance of user perceptions, self-efficacy, habit, and organizational support. Rhee et al. (2009) identified security self-efficacy as an important factor in security behavior (Rhee et al., 2009), while Bulgurcu et al. (2010) demonstrated the role of security awareness in shaping secure practices (Bulgurcu et al., 2010). Together, these findings indicate that effective password security cannot be evaluated solely by measuring the technical strength of a credential. User perceptions of difficulty, usefulness, confidence, and inconvenience also influence whether secure practices are adopted and maintained.

Human-centered interventions have therefore been proposed to reduce the cognitive burden associated with password security. Passphrases provide one potential solution by allowing users to create memorable credentials while maintaining substantial resistance to guessing attacks (Bonneau et al., 2012). Password managers provide another approach by generating and securely storing credentials, reducing the number of passwords users must remember and potentially reducing password reuse (Das et al., 2014) and (Pearman et al., 2019). However, adoption of these tools is not universal, indicating that technical availability alone does not guarantee behavioral change. Organizational support, appropriate security education, and policies that account for human factors remain important components of effective password security (Herley, 2009).

Overall, the literature demonstrates that password security is not solely a technical problem. While strong passwords and authentication controls provide an important defense against unauthorized access, their effectiveness is constrained by human cognitive limitations and user acceptance. Excessive complexity can encourage insecure coping strategies, while insufficient security requirements can leave organizations vulnerable to credential attacks. The attitude behavior gap further demonstrates that awareness of security risks does not necessarily translate into secure

behavior. Technology acceptance models such as TAM and UTAUT provide a framework for examining how perceived usefulness, ease of use, effort, self-efficacy, and other behavioral factors influence password security practices. Consequently, evaluating password security through both technical and behavioral perspectives provides a more comprehensive understanding of why users comply with, resist, or circumvent organizational password requirements.

3. RESEARCH QUESTION

Prior literature demonstrates that strong, complex passwords significantly enhance information security. However, technical controls are only as effective as end-user compliance. Understanding what drives user adoption of complex password habits is critical for improving overall security posture.

To address this gap, this study uses the Technology Acceptance Model (TAM) as an initial theoretical baseline. Our primary research objectives are to:

- Identify salient adoption factors: Determine the primary perceptual and contextual drivers that lead users to adopt complex password behaviors.
- Evaluate theoretical fit: Assess how effectively core TAM constructs explain password security compliance and habit formation.

4. METHODS

Data were collected using Qualtrics, a cloud-based platform for creating and distributing surveys that also provides built-in data analysis tools (What is Qualtrics?, 2025). The web-based survey was administered from October 24, 2024, through November 7, 2024, and yielded 101 responses. Participants were recruited through Amazon Mechanical Turk (MTurk), an online marketplace that enables individuals and businesses to outsource tasks such as data validation, survey participation, and content moderation (Amazon Mechanical Turk, 2025), as well as through a survey link distributed to students.

Survey questions were derived from questions administered by Donalds and Osei-Bryson (2017) and from the Technology Acceptance Model (TAM) developed by Davis (1989); the complete survey is provided in Appendix A. Because the original TAM construct of Perceived Usefulness (PU) is intended to measure the degree to which an individual believes that a system enhances job or task performance, the corresponding items in this study were adapted to address password security. The modified items focused on participants' perceptions of the effectiveness and value of complex passwords, their confidence in using them, and their behavioral tendencies regarding password security rather than their contribution to productivity or task performance. This study relabeled Perceived Usefulness as Perceived Utility (PU). The revised terminology reflects the broader personal and practical value participants associated with complex passwords. This modification allows the construct to represent participants' perceptions of the security benefits and usefulness of password complexity without implying that complex passwords necessarily improve occupational or task performance. The modified construct therefore maintains the theoretical foundation of TAM while adapting its measurement to the password-security context examined in this study.

This study employs a custom Iterative Independent Variable Selection (IIVS) procedure, illustrated in Figure 1. Variable selection methods are used to systematically identify variables that are most relevant to a particular analytical objective, including regression modeling (Chaurasia & Harel, 2012). Regression-based approaches have also been used to identify dependent and explanatory variables in Information Systems research, including through regression and path-analysis approaches (Richmond et al., 2020) and (Wang et al., 2025).

IIVS is based on the principle of backward elimination, a stepwise variable-selection procedure in which a model initially includes all available independent variables and subsequently removes variables that do not meet a specified statistical significance criterion (Chowdhury & Turin, 2020). In this study, the procedure is applied iteratively across multiple representations of the survey variables rather than being limited to a single regression model. At each iteration, variables that fail to meet the predefined significance threshold are removed, and the resulting model is re-estimated. This process continues until the remaining variables satisfy the selection criterion.

The IIVS procedure is applied at three levels of representation. First, individual survey items are evaluated as independent variables. Second, items are aggregated into averaged construct scores, and the resulting construct-level variables

are evaluated. Third, latent variable scores generated through SmartPLS 4 are subjected to the same variable-selection procedure. Applying the procedure at these multiple levels allows the study to evaluate whether relationships identified at the individual-item level remain present when the variables are represented as construct composites and as latent-variable scores.

The proposed IIVS procedure is intended to complement, rather than replace, established data-reduction and structural-modeling techniques. Its purpose is to identify variables that demonstrate direct predictive relevance to the dependent variable while subsequently examining whether those relationships remain when measurement constructs are modeled using PLS-SEM.

Variable selection is important when adapting theoretical frameworks such as TAM to multi-item survey instruments because individual survey items may contain redundant or overlapping information. Exploratory Factor Analysis (EFA) evaluates the covariance structure among observed variables and groups items according to their underlying relationships. Factor extraction and item retention are therefore based primarily on relationships among the predictors themselves. IIVS instead evaluates candidate variables against the study's target dependent variable, Behavioral Intention to Use (BITU), allowing variables to be retained based on their demonstrated predictive relationship with the outcome rather than solely on inter-item covariance.

IIVS extends the concept of standard backward stepwise regression by applying the elimination procedure across multiple levels of representation. Conventional backward elimination is typically performed using either individual observed variables or composite variables. IIVS applies the procedure sequentially to raw survey indicators, average construct composites, and PLS-SEM latent variable scores. This provides an opportunity to examine whether variable relationships remain consistent as the representation of the underlying constructs changes.

IIVS differs from regularization approaches such as LASSO and Elastic Net in its emphasis on statistical significance and interpretability. Regularized regression introduces penalties that shrink coefficients and can set some coefficients to zero, making it useful for predictive variable selection in high-dimensional datasets. IIVS instead applies an explicit statistical significance threshold of $p < .005$ at each elimination step. This preserves a direct hypothesis-testing framework and allows the retained variables to be interpreted using conventional inferential statistics.

IIVS incorporates a PLS-SEM validation stage using SmartPLS 4. After the measurement model is evaluated, standardized latent variable scores are extracted and used as inputs to a subsequent IIVS procedure. This step examines whether the relationships identified during the observed-variable analysis remain when the constructs are represented as latent variables within a structural equation modeling framework. The approach therefore provides a means of connecting item-level exploratory variable selection with variance-based structural modeling.

Overall, IIVS links iterative backward elimination with multiple levels of variable representation and subsequent PLS-SEM validation. The procedure is designed to reduce redundant variables while maintaining explanatory power, with the study targeting an overall coefficient of determination of $R^2 > .60$. Figure 1 illustrates the sequence of the IIVS procedure, from initial independent-variable selection through construct-level analysis and final validation using SmartPLS 4.

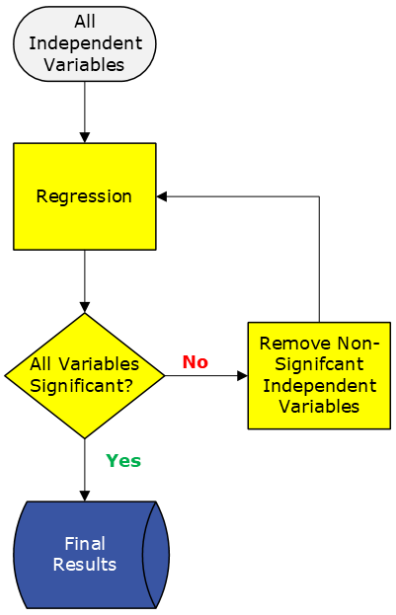


Figure 1: **Iterative Independent Variable Selection**

To further explore predictive relationships, Partial Least Squares Structural Equation Modeling (PLS-SEM) was conducted using SmartPLS 4. Latent

variable scores were generated, and an exploratory model was developed to identify significant predictors of Behavioral Intention to Use (BITU). Non-significant constructs were removed through iterative analyses. The final model retained three key predictors: Attitude Towards Use (AT), General Security Orientation (GSO), and Perceived Utility (PU). All three demonstrated statistically significant relationships with behavioral intention, and the model explained more than 50% of the variance in BITU across the dependent variable configurations examined.

Structural Equation Modeling (SEM) is a multivariate statistical technique that combines factor analysis and multiple regression to estimate interrelated relationships among observable indicator variables and unobservable latent constructs. In Information Systems research, SEM methodologies generally fall into two primary paradigms: Covariance-Based SEM (CB-SEM) and Partial Least Squares SEM (PLS-SEM). CB-SEM focuses primarily on confirming established theoretical models by minimizing the difference between estimated and sample covariance matrices, whereas PLS-SEM is a variance-based, predictive approach that emphasizes the explanation of variance in dependent latent constructs.

PLS-SEM, implemented using SmartPLS 4, was selected as the primary structural modeling method over traditional CB-SEM based on the theoretical and empirical characteristics of this study. First, the study has an exploratory focus, extending the Technology Acceptance Model into the domain of complex password security behaviors while combining structural modeling with the proposed IIVS procedure. PLS-SEM is appropriate for studies that extend theoretical frameworks and seek to identify salient predictors in exploratory research settings. Second, data filtering resulted in a final sample of N = 84 valid responses. PLS-SEM was selected because of its ability to accommodate smaller samples and non-normal data distributions. Third, PLS-SEM generates standardized latent variable scores for each construct, including Perceived Utility, General Security Orientation, and Attitude Towards Use. These scores allow the IIVS procedure to evaluate construct relationships using latent-variable representations rather than unweighted item averages. Finally, because the study focuses on identifying perceptual factors associated with Behavioral Intention to Use complex passwords, PLS-SEM's variance-based estimation approach supports the study's emphasis on explaining variance in BITU.

5. RESULTS

Qualtrics yielded 101 responses. After data cleaning, 12 incomplete responses and five that failed embedded attention-check questions were removed, resulting in 84 valid responses for analysis. To address the seven participants who listed two nationalities in the demographic question (DM3), the variable was split into two fields (DM3_1 and DM3_2). For participants who reported only one nationality, the same value was entered in both fields to maintain consistency.

To ensure consistency in response directionality, 14 survey items were reverse-coded. For instance, item A1_1 was positively worded, while A1_2 was negatively worded; to align their scales, responses to A1_1 were reversed (e.g., a response of 7 was re-coded as 1, 6 as 2, and so on). After reverse-coding, A1_1 and A1_2 responses were within two points of each other for 66 out of 84 participants, indicating consistent interpretation. Similar reverse-coding was applied to items related to Perceived Utility, General Security Orientation, Security Self-Efficacy, and Behavioral Intention to Use, which were either negatively worded or had scales ordered differently from other items. Finally, composite variables were created by averaging responses within each construct to prepare the dataset for regression analysis.

Of these 84 responses, 35 were students. Of these 35, 29 participants were male. Of these 35, the most common age group was 25-34 years old (n=14). White/Caucasian was the most common ethnicity (n=20). 26 described their highest degree of education as High School Diploma. 17 described their employment status as full-time. 33 reported North America as their home, and 22 reported their marital status as single. In summary, this group is mostly high school graduates, single, white, male, 25 – 34 years old, who are full employed and from North America.

Of the 84 responses, 49 responses were acquired using Amazon Mechanical Turk. 32 were male, 21 reported an age range of 35-44 and an additional 21 reported an age range of 45-54. 36 reported as white/Caucasian. 21 reported having completed a bachelor’s degree. 34 were full-time employees, 30 reported North America as the location of their home and 26 reported as being single. In summary, this group is mostly college graduates, single, white, male, 35 - 54 years old, who are full employed and from North America. In comparing the student group to the MTurk group, the student group was in a younger age

group and had less education.

A simple linear regression line follows the equation $Y = a + bX$, where X is the explanatory variable, Y is the dependent variable, a is the intercept (indicating where the line crosses the Y-axis), and b represents the slope, or the expected change in Y for each one-unit increase in X.

Using the 84 valid survey responses, four regression models were developed following the Iterative Independent Variable Selection (IIVS) process. This method involves running a linear regression, removing non-significant variables, and repeating the process until only statistically significant predictors remain. The first three models were conducted using IBM SPSS, while the fourth and final model was developed in SmartPLS 4.

In the first model, mean scores were calculated for each construct, and Behavioral Intention to Use – Averaged (BITUA) was selected as the dependent variable, with all other constructs entered as independent variables (see Table 1). The coefficient of determination (R^2) was used to assess model fit, representing the proportion of variance in the dependent variable explained by the model. In this analysis, a significance threshold of $p < .005$ was applied to determine whether relationships between predictors and the outcome variable were statistically significant (i.e., unlikely to have occurred by chance under the null hypothesis).

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	$.727^a$	.529	.485	.911
a. Predictors: (Constant), SSE, At, PCBI, GCSB, GSA, GSO, PU				

	t	Sig.
(Constant)	.708	.481
AT	-1.310	.194
PU	4.570	<.001
PCBI	2.115	.038
GCSB	.555	.581
GSA	-.562	.576
SEE	-.856	.395

Table 1: **Linear Regression – Averaged Constructs**

The BITUA model yielded an R^2 value of .529. Perceived Utility (PU), General Security Orientation (GSO), and Password Compliance Behavior (PCBI) emerged as significant predictors. Additional regression models were evaluated using BITU2 and then BITU1 as dependent variables. The BITU2 model (excluding BITU1) resulted in an R^2 of .689, with no predictors being statistically significant. The BITU1 model (excluding BITU2) yielded the strongest fit (R^2 = .784), with three items — A2 (Attitude toward Use), PU2_3 (Perceived Utility), and SSE2_2 (Security Self-Efficacy).

In the second regression model, BITU2 was designated as the dependent variable, with all other constructs—excluding BITU1—entered as independent variables (see Table 2). The model produced an R^2 value of 0.689, indicating that approximately 69% of the variance in BITU2 was explained by the predictors. However, only PU1_1 demonstrated statistical significance ($p = .015$), while all other variables failed to reach the significance threshold. Given the limited number of significant predictors, linear regression was considered less suitable for modeling BITU2 as a dependent variable.

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	$.830^a$	.689	.560	.915
a. Predictors: (Constant), SSE2_2, PCB1_1, GSA2_3, PU1_2, GSCB1_2, PCB1_2, GSA1_1, GSCB1_1, PU2_2, A1_1, GSO1_1, SSE2_1, GSA2_1, PU2_3, A2, PU2_1, SSE1_1, SSE1_2, GSO1_2, A2_2, PU1_1, GSA1_2, PU1_3, SSE1_3				

	t	Sig.
(Constant)	.006	.995
A1_1	-1.361	.179
A1_2	.662	.511
A2	.201	.842
PU1_1	2.506	.015
PU1_2	-1.090	.280
PU1_3	1.707	.093
PU2_1	-.219	.827
PU2_2	-.633	.529
PU2_3	1.685	.097
PCB1_1	.163	.871
PCB1_2	1.410	.164
GSCB1_1	-.971	.335
GSCB1_2	-.336	.738
GSA1_1	.020	.984
GSA1_2	.817	.417
GSA2_1	-1.251	.216
GSA2_3	-.267	.791
GSO1_1	1.628	.109
GSO1_2	1.728	.089
SSE1_1	-.972	.335
SSE1_2	-1.101	.276
SSE1_3	.047	.963
SSE2_1	-.331	.742
SSE2_2	1.922	.060

Table 2: **Linear Regression – BITU2 as dependent variable**

A third regression model was run using BITU1 as the dependent variable, excluding BITU2 from the independent variables (see Table 3). This model produced the highest R^2 value (.784), indicating a strong model fit. Among the 24 independent variables, three variables: A2, PU2_3, and SSE2_2, had p-values below .005, identifying them as statistically significant predictors of BITU1. These variables reflect users' comfort with using complex passwords (A2), their frustration with password requirements (PU2_3), and their confidence in learning to protect their information (SSE2_2). To further explore their impact, a final regression model was conducted using only these three predictors (see Table 4), resulting in an R^2 of .626. While this was lower than the full model, it demonstrated that these three factors alone explain a substantial portion of the variance in users' behavioral intention to adopt or continue using complex passwords.

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	886[4]	.784	.695	.722
a. Predictors: (Constant), SSE2_2, PCB1_1, GSA2_3, PU1_2, GSCB1_2, PCB1_2, GSA1_1, GSCB1_1, PU2_2, A1_1, GSO1_1, SSE2_1, GSA2_1, PU2_3, A2, PU2_1, SSE1_1, SSE1_2, GSO1_2, A2_2, PU1_1, GSA1_2, PU1_1, SSE1_3				

	t	Sig.
(Constant)	.342	.734
A1_1	1.458	.150
A1_2	-1.427	.159
A2	5.143	<.001
PU1_1	.735	.465
PU1_2	-1.670	.100
PU1_3	1.121	.267
PU2_1	.540	.591
PU2_2	.024	.981
PU2_3	2.533	.014
PCB1_1	1.253	.215
PCB1_2	.286	.776
GSCB1_1	.191	.849
GSCB1_2	.490	.626
GSA1_1	.176	.861
GSA1_2	.552	.583
GSA2_1	.066	.948
GSA2_3	.029	.977
GSO1_1	-.292	.771
GSO1_2	.513	.610
SSE1_1	.034	.973
SSE1_2	-1.478	.145
SSE1_3	-1.476	.145
SSE2_1	-.676	.502
SSE2_2	2.072	.043

Table 3: **Linear Regression – BITU1 as dependent variable**

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.791[4]	.626	.611	.815
a. Predictors: (Constant), SSE2_2, A2, PU2_3				

	t	Sig.
(Constant)	.953	.343
A2	8.320	<.001
PU2_3	2.133	.036
SSE2_2	-2.34	.815

***Table 4:* Linear Regression – BITU1 as dependent variable and only significant independent variables**

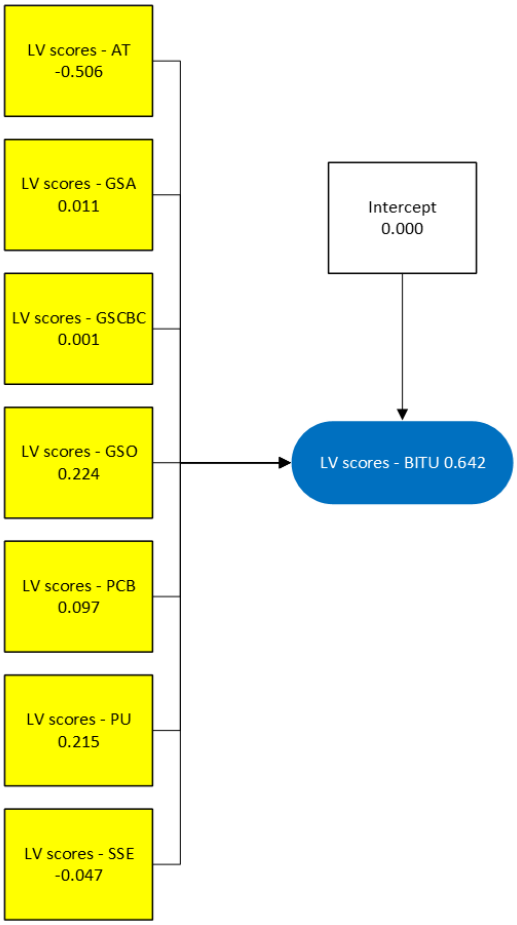


***Figure 2:* Exploratory Regression Model using SmartPLS 4**

To further explore predictive relationships, Partial Least Squares Structural Equation Modeling (PLS-SEM) was conducted using SmartPLS 4 (see Figures 2 and Table 5). Latent variable scores were generated from all survey questions to build an exploratory model predicting Behavioral Intention to Use (BITU). Non-significant constructs were removed through iterative analyses, and the final model retained three statistically significant predictors: Attitude towards Use (AT), General Security Orientation (GSO), and Perceived Utility (PU). These variables explained over 50% of the variance in BITU across multiple dependent variable configurations and were carried forward for subsequent regression modeling.

	T value	**P value**
LV scores - AT	4.555	**0.000**
LV scores - GSA	0.129	0.898
LV scores - GSCBC	0.011	0.991
LV scores - GSO	2.614	**0.011**
LV scores - PCB	1.258	0.212
LV scores - PU	2.03	0.046
LV scores - SSE	0.529	0.598
Intercept	0	1

***Table 5:* Calculated latent variable scores for all questions using SmartPLS4**

6. DISCUSSION

Following an Iterative Independent Variable Selection process, the model with BITU1 as the dependent variable had the highest R^2 value (.784). The significant constructs were A2, PU2_3, and SSE2_2.

A2 (Attitude toward Use) asked participants, "How comfortable are you using complex passwords for your accounts?" The significance of this variable indicates that comfort with complex password use is a critical driver of behavioral intention. Users who feel more at ease using complex passwords are more inclined to continue using them.

PU2_3 (Perceived Utility) measured the item, "Do you find it frustrating to comply with complex password requirements?" It suggests that frustration or lack of perceived value in password complexity negatively impacts users' intentions to adopt secure behaviors.

SSE2_2 (Security Self-Efficacy) was based on the statement, "I feel confident that I can learn methods to protect my information and information system." This item captures users' belief in their own ability to engage in security-

related tasks. Its significance indicates that users with higher self-efficacy. Those who believe they can learn and apply protective measures are more likely to adopt complex passwords. This suggests that confidence in one's ability to manage security plays an important role in motivating protective behaviors in cyber security.

Together, these three variables suggest that behavioral intention to use complex passwords is significantly influenced by users' comfort with the behavior, their perception of its usefulness or ease, and their confidence in managing their own security. For system designers concerned with password policy development, this highlights the need to reduce user frustration, increase perceived value, and build users' confidence through education and intuitive design.

In comparing the dependent variables and their respective significant independent variables, see Table 6, the exploratory regression model using SmartPLS 4 supports the findings of the previous regression models run through IBM SPSS.

Dependent Variable	Significant Independent Variables
BITUA (SPSS)	GSO, PCBI, PU
BITU2 (SPSS)	PU1_1
BITU1 (SPSS)	A2, PU2_3, SSE2_2
BITU (Smart PLS))	AT, GSO, PU

Table 6: **Comparison of dependent variables and their significant independent variables**

After removing the non-significant constructs and rerunning the model in SmartPLS, the results show that Attitude towards Use (AT), General Security Orientation (GSO), and Perceived Utility (PU) are all statistically significant predictors in the regression model. This indicates that each of these factors has a meaningful influence on individuals' intention to adopt strong passwords. As shown in Table 7 and 8 the R^2 values for all endogenous variables exceed 0.60, suggesting that the model explains a substantial proportion of the variance in behavioral intention. This level of explanatory power is comparable to earlier work in the field, such as the Technology Acceptance Model (TAM) by Davis (1989), which similarly identified perceived usefulness as a strong predictor of technology adoption.

	T value	P value
LV scores - AT	5.228	0
LV scores - GSO	2.911	0.005
LV scores - PU	2.177	0.032

Table 7: **Calculated latent variable score for only significant questions using SmartPLS 4**

	LV scores - BITU
R-square	0.633
R-square adjusted	0.619

Table 8: **BITU R^2**

As expected, both General Security Orientation and Perceived Utility had positive effects: individuals who are more security-conscious and who perceive strong passwords as useful are more likely to intend to adopt them. However, Attitude towards Use showed a negative effect, which is unexpected. People who said they felt positive about using strong passwords were less likely to say they planned to use them. This type of gap between what people think and what they do has been seen in other security research. For example, Herath and Rao found that even when employees agreed that security policies were important, they sometimes ignored them because they were inconvenient, time-consuming, or did not fit into their normal work habits (Herath and Rao, 2009). With passwords, people may like the idea of strong passwords in theory but avoid them if they feel they are too hard to remember or take too much effort to create (Vance, Siponen, & Pahnila, 2012). This finding highlights the need for further investigation to better understand how attitude interacts with perceived usefulness and security orientation in shaping password-related behavior.

7. CONCLUSION

This exploratory study gathered data through a Qualtrics survey administered to students and participants recruited via Amazon Mechanical Turk, yielding 84 valid responses after data cleaning. Survey items were adapted from the Technology Acceptance Model (TAM) and from Donalds and Osei-Bryson. Regression and PLS-SEM analyses demonstrated that Attitude towards Use, General Security Orientation, and Perceived Utility significantly predicted behavioral intention to use complex passwords, collectively explaining over 50% of the variance in the final model. Furthermore, we present a method for

independent variable selection designated Iterative Independent Variable Selection (IIVS) and confirmed results via regression with latent variable scores.

These findings align with the broader literature, which underscores the increasing importance and complexity of cyber security. As digital threats grow in scale and sophistication, strong, unique passwords continue to be a frontline defense for both personal and organizational systems. The theoretical foundation provided by TAM helps explain users' adoption of these practices, reinforcing the role of Perceived Utility in fostering stronger password behavior and heightened cyber security awareness.

9. REFERENCES

Adams, A., & Sasse, M. A. (1999). Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures. *Communications of the ACM, 42*(12), 40–46. https://doi.org/10.1145/322796.322806

Amazon. (2025). *Amazon Mechanical Turk*. Retrieved June 4, 2025, from https://www.mturk.com/

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437-443. https://doi.org/10.1016/j.chb.2016.12.040

Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of Web authentication schemes. *2012 IEEE Symposium on Security and Privacy*, 553–567. https://doi.org/10.1109/SP.2012.44

Brown, S. (2010). "Likert Scale Examples for Surveys." from https://www.extension.iastate.edu/documents/anr/likertscaleexamplesforsurveys.pdf.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548. DOI: 10.2307/25750690

Chaurasia, A., & Harel, O. (2012). Using AIC in multiple linear regression framework with multiply imputed data. *Health Services and Outcomes Research Methodology, 12*, 219-233. DOI: 10.1007/s10742-012-0088-8

Chowdhury, M. Z. I., & Turin, T. C. (2020). Variable selection strategies and its importance in clinical prediction modelling. *Family Medicine and Community Health, 8*(1), e000262. DOI: 10.1136/fmch-2019-000262

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, October. DOI: 10.22215/timreview/835

Das, S., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014). The tangled web of password reuse. *Network and Distributed System Security Symposium (NDSS)*. https://doi.org/10.14722/ndss.2014.23290

Davis, F. D. (1989). *Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology*. Management Information Systems Research Center, 13(Sept): 319-340. https://doi.org/10.2307/249008

Donalds, C., & Osei-Bryson, K.-M. (2017). Exploring the impacts of individual styles on security compliance behavior: A preliminary analysis. *SIG GlobDev 2017 Proceedings, 1*. https://aisel.aisnet.org/globdev2017/1

Florencio, D., & Herley, C. (2007). A large-scale study of web password habits. Proceedings of the 16th International Conference on World Wide Web, (pp. 657–666). ACM. https://doi.org/10.1145/1242572.1242661

Herley, C. (2009). So long, and no thanks for the externalities: The rational rejection of security advice by users. *Proceedings of the 2009 New Security Paradigms Workshop*, 133–144. https://doi.org/10.1145/1595676.1595690

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106–125. https://doi.org/10.1057/ejis.2009.6

John Hopkins University. (2025). What is Qualtrics? John Hopkins University. Retrieved June 4, 2025, from https://uis.jhu.edu/qualtrics/what-is-qualtrics/

Novakovic, L., McGill, T. J., & Dixon, M. W. (2009). Understanding user behavior towards passwords through acceptance and use modelling. International Journal of Information Security and Privacy, 3(1), 11–29. https://doi.org/10.4018/jisp.2009010102

Pearman, S., Thomas, J., Naeini, P. E., Habib, H., Bauer, L., Christin, N., Cranor, L. F., Egelman, S., & Forget, A. (2017). Let's go in for a closer look: Observing passwords in their natural habitat. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 295–310. https://doi.org/10.1145/3133956.3133973

Richmond, H. L., Tome, J., Rochani, H., Fung, I. C.-H., Shah, G. H., & Schwind, J. S. (2020). The use of penalized regression analysis to identify county-level demographic and socioeconomic variables predictive of increased COVID-19 cumulative case rates in the state of Georgia. *International Journal of Environmental Research and Public Health, 17*(21), 8036. doi: 10.3390/ijerph17218036

Rhee, H.-S., et al. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers & Security, 28(8): 816-826. DOI: 10.1016/j.cose.2009.05.008

Special Eurobarometer 390: *Cyber security (v1.00)*. (2014). European Commission, Directorate-General for Communication. https://data.europa.eu/data/datasets/s1058_77_2_ebs390?locale=en

Turan, M. S., Barker, E. B., Burr, W. E., & Chen, L. (2010). *Recommendation for Password-Based Key Derivation––Part 1: Storage Applications* (NIST Special Publication 800-132). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-132

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, 27(3), 425-478. https://doi.org/10.2307/30036540

Wang, Z., Li, S., Zhou, X., & Zhu, S. (2025). An iterative conditional variable selection method for constraint-based time series causal discovery. *Chemometrics and Intelligent Laboratory Systems, 260*, 105361. https://doi.org/10.1016/j.chemolab.2025.105361

What is Cybersecurity? (2021, 09/10/2024). https://www.cisa.gov/news-events/news/what-cybersecurity

APPENDIX A

Survey Questions

Construct	Code	Item	Possible Response
Demographics	D1	What gender do you identify as?	Male, Female, I do not wish to specify
Demographics	D2	What is your age?	18-24, 25-34, 35-44, 45-54, 55-64, 65 or older
Demographics	D3	What is your ethnicity?	Hispanic/Latino, Black/African American, White/Caucasian, Native American/American Indian, Asian/Pacific Islander, Other
Demographics	D4	What is your highest degree or level of education you've completed?	High School Degree, Bachelor's Degree, Master's Degree, Doctorate Degree
Demographics	D5	What is your current employment status?	Full-Time, Part-Time, Internship, Retired, Non-employed, Other
Demographics	D6	Where is your home located?	Africa, Asia, Australia, Caribbean/Pacific Island, Europe, North America/Central America, South America, Other
Demographics	D7	What is your marital status?	Single, Married, Divorced, Widowed
Perceived Utility of Complex Passwords	PU1_1	Do you feel that using complex passwords improves the security of your personal information? (Davis, 1989)	7-point Likert Scale for Agreement (Brown, 2010)
Perceived Utility of Complex Passwords	PU1_2	How confident are you that complex passwords protect sensitive data? (Davis, 1989)	7-point Likert Scale for Agreement (Brown, 2010)
Perceived Utility of Complex Passwords	PU1_3	To what extent do you believe complex passwords are necessary for protecting your accounts from cyber threats? (Davis, 1989)	7-point Likert Scale for Agreement (Brown, 2010)
Perceived Utility of Complex Passwords	PU2_1	Do you think using complex passwords helps prevent unauthorized access to your accounts? (Davis, 1989)	7-point Likert Scale for Agreement (Brown, 2010)
Perceived Utility of Complex Passwords	PU2_2	How easy is it for you to create and remember complex passwords? (Davis, 1989)	7-point Likert Scale for Agreement (Brown, 2010)
Perceived Utility of Complex Passwords	PU2_3	Do you find it frustrating to comply with complex password requirements? (Davis, 1989)	7-point Likert Scale for Agreement (Brown, 2010)

Attitude Toward Use	A2	How comfortable are you using complex passwords for your accounts? (Venkatesh et al., 2003)	6-point Likert scale for Likelihood (Brown, 2010)
Attitude Toward Use	A1_1	Would you prefer simpler password policies even if they meant less security? (Venkatesh et al., 2003)	7-point Likert Scale for Agreement (Brown, 2010)
Attitude Toward Use	A1-2	Do you feel more secure when using complex passwords? (Venkatesh et al., 2003)	7-point Likert Scale for Agreement (Brown, 2010)
Behavioral Intention to Use	BITU1	How likely are you to adopt or continue using complex passwords for your accounts in the future? (Venkatesh et al., 2003)	6-point Likert scale for Likelihood (Brown, 2010)
Behavioral Intention to Use	BITU2	Would you recommend using complex passwords to others? (Venkatesh et al., 2003)	7-point Likert Scale for Agreement (Brown, 2010)
Password Compliance Behavior	PCB1_1	I use unique passwords for each account. (e.g. online banking, social media, email) (Anwar et al., 2017) (Donalds & Osei-Bryson, 2017) (Special Eurobarometer 390: Cyber security (v1.00), 2014)	6-point Likert scale for Likelihood (Brown, 2010)
Password Compliance Behavior	PCB1_2	I have changed my passwords in the past 12 months. (Anwar et al., 2017) (Donalds & Osei-Bryson, 2017) (*Special Eurobarometer 390: Cyber security (v1.00)*, 2014)	6-point Likert scale for Likelihood (Brown, 2010)
General Security Compliance Behavior	GSCB1_1	I never send sensitive information in plaintext via email or social media (e.g. bank account numbers, pins, passwords) (Anwar et al., 2017) (Donalds & Osei-Bryson, 2017) (*Special Eurobarometer 390: Cyber security (v1.00)*, 2014)	6-point Likert scale for Likelihood (Brown, 2010)
General Security Compliance Behavior	GSCB2_2	I only visit websites that I know or trust. I only click on URL links if I know where the URL will take me. (Anwar et al., 2017) (Donalds & Osei-Bryson, 2017) (*Special Eurobarometer 390: Cyber security (v1.00)*, 2014)	6-point Likert scale for Likelihood (Brown, 2010)
General Security Awareness	GSA1_1	I understand the concerns of cyber security threats and the risks that they pose. (Bulgurcu et al., 2010) (Donalds & Osei-Bryson, 2017)	6-point Likert scale for Likelihood (Brown, 2010)
General Security Awareness	GSA1_2	I am aware of potential information/cyber security threats and their negative consequences. i.e. I know about different types of cyber security threats such as phishing emails, social engineering, and/or denial of service attacks, etc. (Bulgurcu et al., 2010)	6-point Likert scale for Likelihood (Brown, 2010)

		(Donalds & Osei-Bryson, 2017)	
General Security Awareness	GSA2_1	I have sufficient knowledge of the costs of cyber security threats. (Bulgurcu et al., 2010) (Donalds & Osei-Bryson, 2017)	6-point Likert scale for Likelihood (Brown, 2010)
General Security Awareness	GSA2_3	I read cyber security bulletins or newsletters. (Donalds and Osei-Bryson 2017)	6-point Likert scale for Likelihood (Brown, 2010)
General Security Orientation	GSO1_1	Cyber security incidents concern me, and I try to take action to prevent them. (Donalds and Osei-Bryson 2017)	7-point Likert Scale for Agreement (Brown, 2010)
General Security Orientation	GSO1_2	I am mindful about computer security. (Donalds and Osei-Bryson 2017)	7-point Likert Scale for Agreement (Brown, 2010)
Security Self-Efficacy	SSE1_1	I feel confident that I can update operating systems using security patches. (Donalds & Osei-Bryson, 2017) (Anwar et al., 2017) (Rhee et al., 2009)	7-point Likert Scale for Agreement (Brown, 2010)
Security Self-Efficacy	SSE1_2	I feel confident that I can set a web browser security level. sei-Bryson, 2017)	7-point Likert Scale for Agreement (Brown, 2010)
Security Self-Efficacy	SSE1_3	I feel confident that I can use different programs to protect my information and information system. (Donalds & Osei-Bryson, 2017) (Anwar et al., 2017) (Rhee et al., 2009)	7-point Likert Scale for Agreement (Brown, 2010)
Security Self-Efficacy	SSE1_4	I feel confident in handling virus infected files and ridding my system of malware. (Donalds & Osei-Bryson, 2017) (Anwar et al., 2017) (Rhee et al., 2009)	7-point Likert Scale for Agreement (Brown, 2010)
Security Self-Efficacy	SSE1_5	I feel confident that I can learn methods to protect my information and information system. (Donalds & Osei-Bryson, 2017) (Anwar et al., 2017) (Rhee et al., 2009)	7-point Likert Scale for Agreement (Brown, 2010)