ISSN: 2473-4901
v11 n6343

# Perceived Usefulness of Password Complexity: A Methodology Approach

Kyle Herman
kh00054@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 cybersecurity and the critical role of strong, unique passwords amid advancing threats. The study highlights the importance of user perceptions in driving secure behavior and contributes to understanding how theoretical frameworks like TAM can guide effective cybersecurity practices.

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

ISSN: 2473-4901
v11 n6343

# 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 the 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.

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

Cyber security is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that would disrupt the established legal ownership and control of digital assets (Craigen, Diakun-Thibault et al., 2014). Similarly, the Cybersecurity & Infrastructure Security Agency (CISA) defines cybersecurity as the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information (What is Cybersecurity?, 2021). Cybersecurity covers not only the software but the hardware that it runs on and the data that is processed and stored. Passwords play a crucial role in cybersecurity as they serve as the first line of defense against unauthorized access.

In NIST Special Publication 800-132, dated December 2010, a password or passphrase is a string of characters (including letters, numbers, and specific special characters) used to gain access to a restricted resource. It serves as a means of authentication, which establishes the identity of the user. The strength of a password is primarily based on its length and randomness (Turan, Barker, Burr, & Chen, 2010). CISA emphasizes the importance of using unique passwords for each account. Passwords with fewer than 10 characters are considered weak, and longer passwords lose their effectiveness if they contain predictable patterns such as "123456," "password2025," or personal information such as names and birthdays like "John1985" or "Sarah!12." These types of passwords are commonly used, easily guessed, and often included in password-cracking dictionaries, making them highly vulnerable to brute-force and social engineering attacks. Additionally, passphrases consisting solely of letters should exceed 20 characters in length. When passwords are used to generate cryptographic keys, it is crucial to assume that attackers may perform offline attacks on the key derivation process using more powerful systems than the one used by the user. Consequently, the number of possible guesses required to crack a password from the derived key is a critical factor in its security (Turan, Barker et al., 2010).

Password-Based Key Derivation Functions (PBKDF) can be used to stretch short keys (passwords) into long keys. It is an efficient method to achieve increased security without changing a system. SALT is a basic approach for designing a PBKDF. Key = H^(c)(p||s) where "H" is a function such as a hash, keyed hash or block cipher, "c" is the iteration count, "p" is the password, and "s" is a random know value (called salt) (Yao & Yin, 2005). PKCS#5 is considered the de facto standard for password-based cryptography (wolfSSL, 2018).

A data breach allows an attacker to perform offline attacks with unlimited attempts to decrypt the data (Turan, Barker et al., 2010). This pits the encrypted data against the computational power that an attacker has available. The computational power available for brute-forcing passwords continues to grow significantly from year to year. In October 2010, the Tianhe-1A was the world's fastest supercomputer with a peak computing rate of 2.507 petaFLOPS (China builds the world's fastest supercomputer, n.d.). A petaflop is defined as a measure of computing performance equal to 10^15 floating-point operations per second (1,000 teraFLOPS). Twelve years later in June 2022, the Frontier system at Oak Ridge National Laboratory (ORNL) in the United States reached a peak of 1.1 exaFLOPS (Frontier supercomputer debuts as world's fastest, breaking exascale barrier, 2022). One exaFLOP equals 10^18 flops (1,000 petaflops). This means the Frontier supercomputer was approximately 429 times more powerful than the Tianhe-1A, highlighting the rapid advancements in computational capabilities in just over a decade.

Protecting data in transit can be accomplished using Secure Sockets Layer (SSL) or its successor, Transport Layer Security (TLS). SSL, introduced by Netscape in 1995, was designed to secure data transmitted over the internet by encrypting communication between a client and a server. This encryption ensures both the confidentiality and integrity of the data in transit. TLS, introduced in 1999, builds upon SSL and is now the modern standard for secure communications. Although the terms SSL and TLS are still often used interchangeably, TLS is an updated, more secure version of SSL. While these protocols provide a secure channel for data transmission, the overall security of a system also relies on robust authentication methods, such as strong passwords. When used within SSL/TLS sessions, passwords support data confidentiality by authenticating users securely over encrypted connections, thereby preventing unauthorized access, and reducing the risk of credential interception (Baier, 2015).

Data at rest can be effectively protected through encryption, which prevents unauthorized access to stored information. Two common approaches are file-level encryption and full disk encryption (FDE). File-level encryption encrypts each file individually with a unique key, so if one file is compromised, the security of other files remains intact. In contrast, FDE encrypts the entire contents of a storage device, offering a more comprehensive solution for securing data at rest (The Ultimate Guide to File Encryption vs. Disk Encryption: Which One Is Best for You?, 2023).

On Windows systems, BitLocker is a built-in full disk encryption feature that enhances security by leveraging the Trusted Platform Module (TPM), a hardware-based security component. When BitLocker is enabled, the system's normal startup process is paused until the user provides an approved authentication method. This mechanism prevents unauthorized users from bypassing encryption by attempting to boot the system from another device or operating system (*BitLocker Overview*, 2025).

For macOS users, FileVault provides full disk encryption using the AES-XTS (Advanced Encryption Standard with XTS mode) algorithm to encrypt the entire disk. When enabled, FileVault requires users to enter a password before the operating system boots. After startup, users must authenticate again at the login screen to access their account, ensuring that both system-level and user-level access remain protected (Intro to FileVault, 2024).

While technical measures are essential to securing passwords, understanding user behavior is equally important in improving overall password security. Research shows that despite awareness of strong password practices, many users struggle to consistently apply them due to factors such as convenience, cognitive load, and habit. For example, Herath and Rao found that employees' positive attitudes toward security policies do not always translate into compliant behavior because users often prioritize ease of use and time savings over strict adherence (Herath and Rao, 2009). This gap between attitude and action, sometimes called the attitude–behavior gap, means that even well-designed password policies may fail if they do not consider user motivation and habits (Vance, Siponen, & Pahnila, 2012). Users commonly reuse passwords across multiple accounts or choose simpler passwords to reduce memory burden, increasing vulnerability to credential-stuffing attacks and other compromises.

To address these challenges, researchers have explored the balance between password complexity and usability. Studies indicate that overly complex password requirements can lead to user frustration and insecure coping strategies, such as writing passwords down or reusing them

(Adams & Sasse, 1999). Using passphrases instead of random character strings has been shown to improve memorability while maintaining strong security, making them a recommended alternative (Bonneau et al., 2012). Additionally, the adoption of password managers has been promoted to ease the cognitive load by securely storing and generating strong passwords, reducing risky behaviors (Das et al., 2014). Organizational support, including user training and realistic policies that consider human factors, is crucial to fostering compliance and enhancing the effectiveness of password-based security (Herley, 2009). Together, these findings emphasize that improving password security requires both robust technical controls and a deep understanding of human behavior.

## 3. RESEARCH QUESTION

Based on the literature, a strong password can be used to greatly enhance information security. The question is, what leads users to adopt strong password behavior? Adoption of complex passwords is an important consideration which needs to be understood to improve the behavior of complex password use. Based on this, we propose the following research objectives and use TAM as an initial baseline: Adoption of complex passwords is an important consideration which needs to be understood in order to improve the behavior of complex password use. Based on this, we propose the following research objective: Determine which factors are salient in adoption of complex password behavior. Survey questions were adopted from Fred Davis's TAM model (Davis, 1989) and Donalds and Osei-Bryson's Model (Donalds, 2020), see Appendix A: Survey Questions.

## 4. METHODS

Data was collected using Qualtrics, a cloud-based platform for creating and distributing surveys that also provides built-in analysis tools (What is Qualtrics?, 2025). The web-based survey was administered from October 24, 2024, to 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.

Research questions were derived from questions administered by Donalds and Osei-Bryson (Donalds and Osei-Bryson, 2017) and Fred Davis and the Technology Acceptance Model (TAM) (Davis, 1989). While TAM traditionally uses the construct Perceived Usefulness (PU) to reflect the degree to which a user believes a system enhances their job performance, our items were revised to reflect more practical, real-world considerations specific to password security. The modified questions focused on participants' perceived effectiveness, confidence, and behavioral tendencies regarding the use of complex passwords, rather than on their contribution to productivity or performance. As a result, we relabel the construct Perceived Usefulness to Perceived Utility to better reflect the broader personal value and perceived benefit associated with the use of complex passwords. This relabeling allows for a more accurate representation of how participants assess the personal and practical merit of password complexity in a security context, rather than the narrow performance enhancement focus implied by the original TAM terminology.

In this work, we employ a custom Iterative Independent Variable Selection (IIVS) process as diagramed in Figure 1. Variable selection methods refer to a method to systematically select the most important variables for a specific purpose, such as regression (Chaurasia & Harel, 2012). Regression has been employed for identification of dependent variables in (Richmond et al., 2020) and via path analysis in (Wang, Li, Zhou, & Zhu,2025). Our IIVS process follows standard variable selection methods in a stepwise selection method via a backwards elimination procedure (Chowdhury & Turin, 2020) whereby we start with all possible dependent variables and after each pass eliminate those which are not significant. We repeat this IIVS procedure for both possible dependent variables as well as averaging all constructs. IIVS is being presented as an alternative method to eliminate factors to be used in conjunction with methods such as factor analysis. Finally, we employ SmartPLS 4 as a mechanism to confirm our findings from standard regression whereby we perform the IPVS process against the latent variable scores generated by SmartPLS 4.

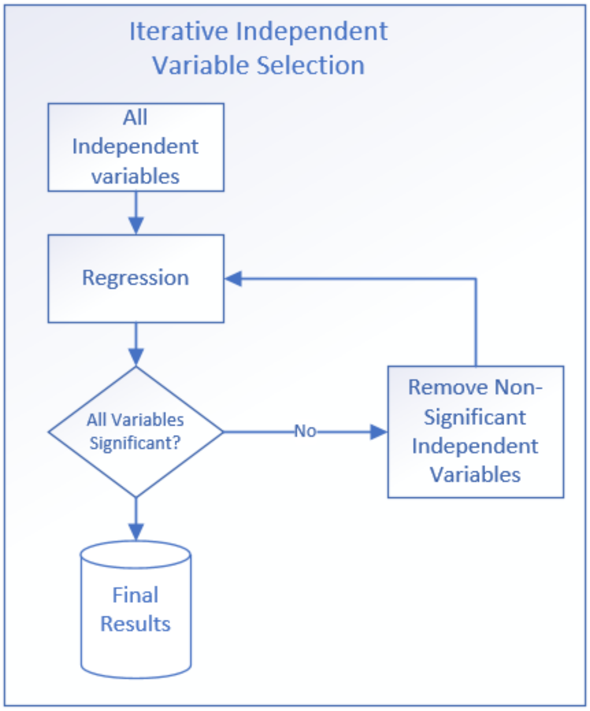

Iterative Independent Variable Selection
All Independent variables
Regression
All Variables Significant?
No
Remove Non-Significant Independent Variables
Final Results

***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 built to identify significant predictors of BITU. Non-significant constructs were removed in iterative analyses. The final model retained three key predictors: Attitude towards Use (AT), General Security Orientation (GSO), and Perceived Usefulness (PU). All three demonstrated statistically significant relationships with behavioral intention, and the model explained over 50% of the variance in BITU across multiple dependent variable configurations.

## 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 Usefulness, 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.

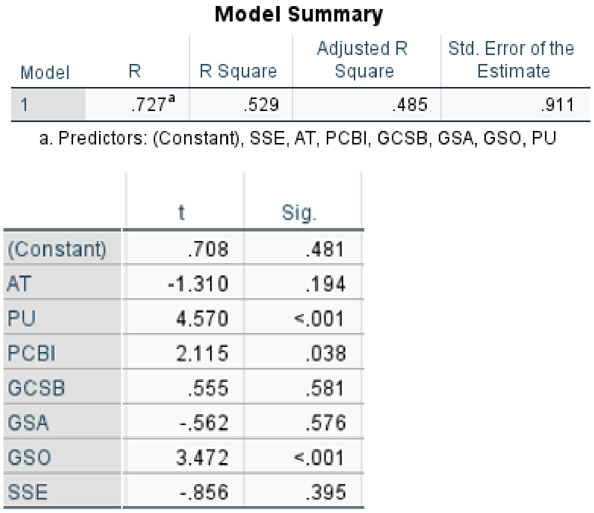
Of the 84 responses, 49 responses were acquired using Amazon Mechanical Turk. 32 were male, 21 reported an age range of 35-44 and an additional 21 reported an age range of 45-54. 36 reported as white/Caucasian. 21 reported having completed a bachelor’s degree. 34 were full-time employees, 30 reported 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 Figure 2). The coefficient of determination (R²) 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).

The BITUA model yielded an R² value of .529. Perceived Utility (PU), General Security Orientation (GSO), and Password Compliance Behavior (PCBI) emerged as significant predictors. Additional regression models were tested using BITU2 and then BITU1 as dependent variables. The BITU2 model (excluding BITU1) resulted in an R² of .689, though only PU1_1 was statistically significant (p = .015). The BITU1 model (excluding BITU2) yielded the strongest fit (R² = .784), with three items — A2 (Attitude toward Use), PU2_3 (Perceived Usefulness), and SSE2_2 (Security Self-Efficacy).



**Model Summary**

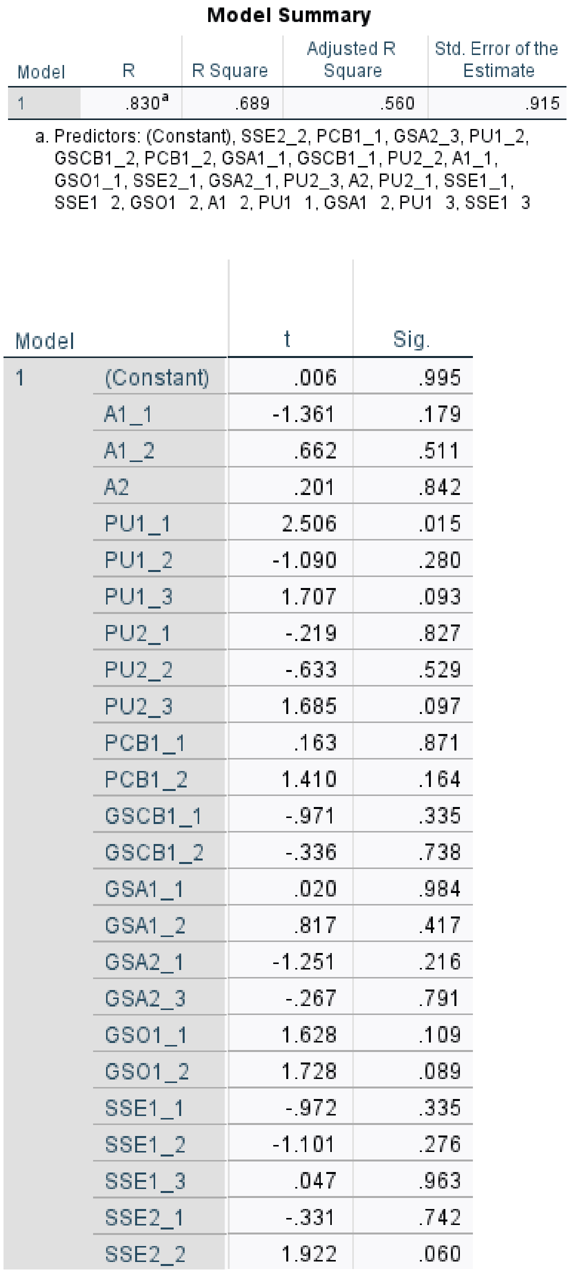
| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | .727[a] | .529 | .485 | .911 |

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 |
| GSO | 3.472 | <.001 |
| SSE | -.856 | .395 |

***Figure 2:*** **Linear Regression – Averaged Constructs**

In the second regression model, BITU2 was designated as the dependent variable, with all other constructs—excluding BITU1—entered as independent variables (see Figure 3). The model produced an R² 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 dependent variable.



**Model Summary**

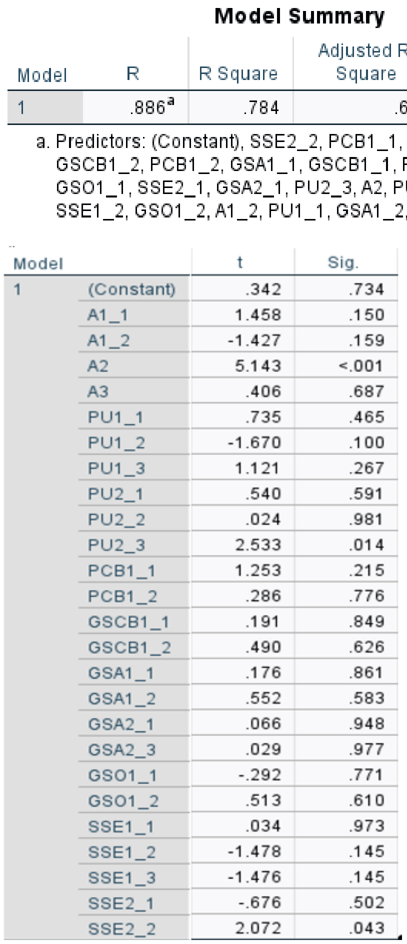
| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | .830[a] | .689 | .560 | .915 |

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, A1 2, PU1 1, GSA1 2, PU1 3, SSE1 3

| Model | | t | Sig. |
|---|---|---|---|
| 1 | (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 |

***Figure 3:*** **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 Figure 4). This model produced the highest R² 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 Figure 5), resulting in an R² 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.



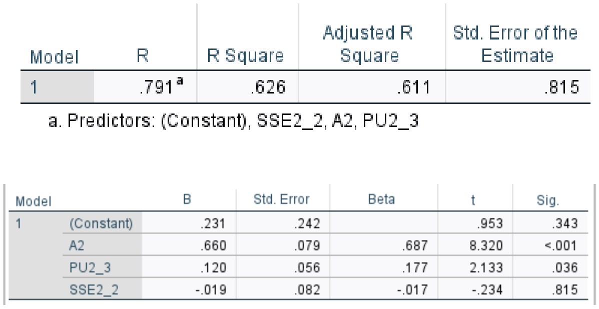
**Model Summary**

| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | .886[a] | .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, A1_2, PU1_1, GSA1_2, PU1_3, SSE1_3

| Model | | t | Sig. |
|---|---|---|---|
| 1 | (Constant) | .342 | .734 |
| | A1_1 | 1.458 | .150 |
| | A1_2 | -1.427 | .159 |
| | A2 | 5.143 | <.001 |
| | A3 | .406 | .687 |
| | 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 |

***Figure 4:*** **Linear Regression – BITU1 as dependent variable**



| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | .791[a] | .626 | .611 | .815 |

a. Predictors: (Constant), SSE2_2, A2, PU2_3

| Model | | B | Std. Error | Beta | t | Sig. |
|---|---|---|---|---|---|---|
| 1 | (Constant) | .231 | .242 | | .953 | .343 |
| | A2 | .660 | .079 | .687 | 8.320 | <.001 |
| | PU2_3 | .120 | .056 | .177 | 2.133 | .036 |
| | SSE2_2 | -.019 | .082 | -.017 | -.234 | .815 |

***Figure 5:*** **Linear Regression – BITU1 as dependent variable and only significant independent variables**

To further explore predictive relationships, Partial Least Squares Structural Equation Modeling (PLS-SEM) was conducted using SmartPLS 4 (see Figures 6 and 7). 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.

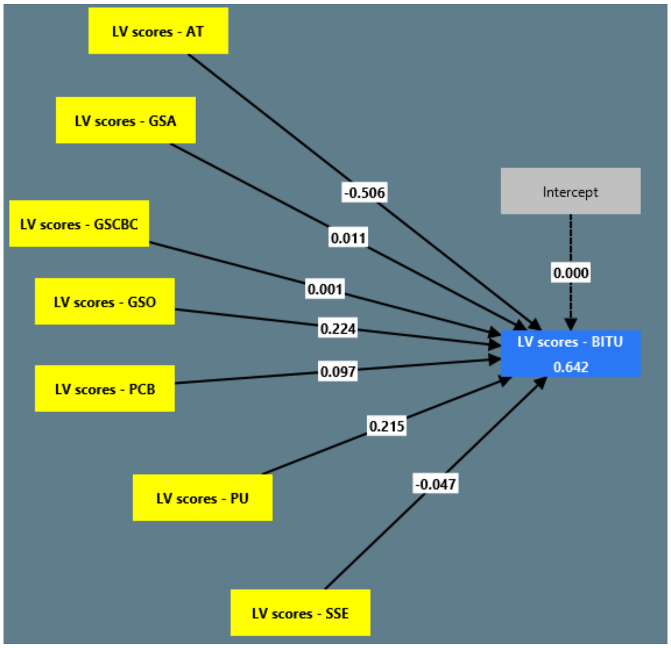


***Figure 6:*** **Exploratory Regression Model using SmartPLS 4**

| | 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 |

***Figure 7:*** **Calculated latent variable score 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 R² 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 cybersecurity.

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 Figure 8, the exploratory regression model using SmartPLS 4 supports the findings of the previous regression models run through IBM SPSS.

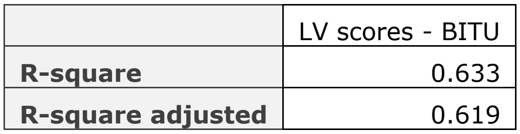
| Dependent Variable | Significant Independent Variables |
|---|---|
| BITUA (SPSS) | GSO, PCBI, PU |
| BITU2 (SPSS) | PU1_1 |
| BITU1 (SPSS) | A2, PU2_3, SSE2_2 |
| BITU (Smart PLS)) | AT, GSO, PU |

***Figure 8:*** **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 Figure 9 and Figure 10 the R-squared 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 |

***Figure 9:*** **Calculated latent variable score for only significant questions using SmartPLS 4**



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

***Figure 10:*** **BITU R²**

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 cybersecurity. As digital threats grow in scale and sophistication, strong, unique passwords continue to be a frontline defense for both personal and organizational systems. The adoption of advanced encryption standards like AES, secure transmission protocols like TLS, and disk encryption tools such as BitLocker and FileVault illustrate the ongoing evolution of data security practices. Password-based key derivation techniques (e.g., PBKDF with salt) further bolster resilience against offline attacks. 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 cybersecurity 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.

AxCrypt AB. (2023, May 22). *The ultimate guide to file encryption vs. disk encryption: Which one is best for you?* AxCrypt Blog. Retrieved June 16, 2025, from https://axcrypt.net/blog/the-ultimate-guide-to-file-encryption-vs-disk-encryption-which-one-is-best-for-you/

Baier, E. (2015, February 2). *The evolution of SSL and TLS*. DigiCert. Retrieved June 16, 2025, from https://www.digicert.com/blog/evolution-of-ssl

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.

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.

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.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, October.

Cybersecurity & Infrastructure Security Agency. (n.d.). *Use Strong Passwords.* Secure Our World. U.S. Department of Homeland Security. Retrieved August 9, 2025, from https://www.cisa.gov/secure-our-world/use-strong-passwords

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.

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

ICC USA. (n.d.). *China builds the world's fastest supercomputer*. Retrieved June 16, 2025, from https://www.icc-usa.com/china-builds-the-worlds-fastest-supercomputer

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

Intro to FileVault. (2024). Apple. Retrieved September 24, 2024, from https://support.apple.com/guide/deployment/intro-to-filevault-dep82064ec40/web

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

Microsoft. (2025, April 28). BitLocker overview. Microsoft Learn. Retrieved June 16, 2025, from https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/

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.

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.

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

U.S. Department of Energy, Oak Ridge National Laboratory. (2022, May 30). *Frontier Supercomputer Debuts as World's Fastest, Breaking Exascale Barrier*. Oak Ridge National Laboratory.

https://www.ornl.gov/news/frontier-supercomputer-debuts-worlds-fastest-breaking-exascale-barrier

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.

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.

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

wolfSSL Inc. (2018, March 22). *Intro to PKCS #5: Password-Based Cryptography Specification. wolfSSL*. Retrieved June 16, 2025, from https://www.wolfssl.com/intro-pkcs-5-password-based-cryptography-specification/

Yao, F. F., & Yin, Y. L. (2005). Design and analysis of password-based key derivation functions. *IEEE Transactions on Information Theory, 51*(9), 3292–3297. https://doi.org/10.1109/TIT.2005.853314

## 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 it 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)<br>(Donalds & Osei-Bryson, 2017)<br>(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)<br>(Donalds & Osei-Bryson, 2017)<br>(*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)<br>(Donalds & Osei-Bryson, 2017)<br>(*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)<br>(Donalds & Osei-Bryson, 2017)<br>(*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)<br>(Donalds & Osei-Bryson, 2017) | 6-point Likert scale for Likelihood (Brown, 2010) |
| General Security Awareness | GSA1_2 | I am aware of potential information/cybersecurity 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 cybersecurity threats.<br>(Bulgurcu et al., 2010)<br>(Donalds & Osei-Bryson, 2017) | 6-point Likert scale for Likelihood (Brown, 2010) |
| General Security Awareness | GSA2_3 | I read cybersecurity bulletins or newsletters. (Donalds and Osei-Bryson 2017) | 6-point Likert scale for Likelihood (Brown, 2010) |
| General Security Orientation | GSO1_1 | Cybersecurity 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)<br>(Anwar et al., 2017)<br>(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.<br>(Donalds & Osei-Bryson, 2017)<br>(Anwar et al., 2017)<br>(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)<br>(Anwar et al., 2017)<br>(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)<br>(Anwar et al., 2017)<br>(Rhee et al., 2009) | 7-point Likert scale for Agreement (Brown, 2010) |