

## THE IMPACT OF CYBER SECURITY CULTURE ON MALAYSIAN ADULTS' SUSCEPTIBILITY TO PHISHING EMAILS IN THE BANKING SECTOR

Nurul Insyirah<sup>A</sup>, Kannan Asokan<sup>B</sup>, Iqbal Singh<sup>C</sup>, Dr. Dhamayanthi Arumugam<sup>D</sup>

### ABSTRACT

The study focused on the connection between Malaysian adults' knowledge of email phishing and cyber security awareness issues. The study is restricted to adult Malaysians who have bank accounts. Cybercriminals are likely to target adults who regularly get emails from banks as soft targets since they can send phishing emails. This study used quantitative research techniques and required the gathering of primary data. The study adopted a deductive methodology based on accepted notions. Utilizing SPSS, questionnaires were used to gather and evaluate the data. The ideal sample size for this study is 97 participants. Potential study participants were found using a convenience sampling technique. The respondents were contacted either personally or via social media. The results showed that characteristics such as cyber security awareness, how frequently a person uses online banking services, and cyber security culture had a substantial impact on the likelihood that an adult Malaysian banking customer may receive a phishing email pertaining to banking. The results also showed that cyber security awareness and cyber security culture have a big impact on the likelihood that adult banking clients in Malaysia will receive a phishing email with an aim of financial fraud. **Keywords:** Cyber Security Awareness; Cybercriminals; Cyber Security Culture; Frequency of Online Banking; Phishing Email.

---

<sup>A</sup> Research Scholar, Asia Pacific University. Email: [insyirahiqbal01@gmail.com](mailto:insyirahiqbal01@gmail.com)

<sup>B</sup> Lecturer, Asia Pacific University. Email: [kannan.asokan@apu.edu.my](mailto:kannan.asokan@apu.edu.my) Orcid: <https://orcid.org/0009-0008-4459-867X>

<sup>C</sup> Lecturer, Asia Pacific University. Email: [iqbal.munjal@apu.edu.my](mailto:iqbal.munjal@apu.edu.my)

<sup>D</sup> Senior Lecturer, Asia Pacific University.. Email: [dhamayanthi@apu.edu.my](mailto:dhamayanthi@apu.edu.my)

## **INTRODUCTION**

Cybercrime awareness was a critical factor in thwarting criminal activities targeting bank customers online. In Malaysia, the cybercrime rate was alarmingly high, with Kaspersky products having detected and blocked tens of thousands of phishing attempts aimed at banking and e-commerce transactions. Despite efforts by the Commercial Crime Investigation Department (CCID) to raise awareness, cybercriminals continuously adapted and found new ways to succeed. In 2021, reported cyber threats in Malaysia encompassed fraud, intrusion, malicious code, and cyber harassment, affecting over 10,000 adults, highlighting the low cybercrime awareness among Malaysians.

Since 2015, phishing websites had surged by 51%, a concerning trend. Email phishing accounted for 29% of cyberattacks compromising privacy, with 45% targeting businesses. Banu and Banu (2013) noted that the increase in new internet users lacking knowledge about cybercrimes contributed to the persistence of phishing attacks, which exploited this ignorance.

Phishing activities thrived due to low digital literacy levels in society. If cybercriminals hadn't found success, they wouldn't have invested so much effort. Addressing this issue required educating the public to bridge the knowledge gap, with a particular focus on email phishing, which was twice as prevalent as other forms (Alabdan, 2020). Weak cybersecurity culture and a lack of awareness among adults about email phishing were significant contributors to the problem.

As many Malaysians relied on online banking, they were exposed to various cybercrimes, including email phishing. Whether a user fell victim to phishing attempts hinged on their exposure and understanding of the risks. Cybercriminals often impersonated trusted entities to deceive targets into sharing personal information. Given the widespread use of online banking among Malaysian adults, this research aimed to evaluate their awareness of email phishing risks, seeking to address this critical cybersecurity issue.

## **LITERATURE REVIEW**

Internet banking was projected to be the primary banking channel in Malaysia by 2030 due to its convenience (Supayah & Ibrahim, 2016). However, the rise of online banking also increased cybersecurity risks, particularly identity theft through phishing activities. These activities, which included spear phishing, pharming, and evil twins, significantly affected internet banking in Malaysia. Email phishing scams were common, where fraudsters posed as legitimate entities and tricked victims into clicking malicious links that installed malware on their devices. This allowed the fraudster to access sensitive information and potentially steal money from the victim's bank account. As such, bank customers were advised to be vigilant when handling banking information online and to ignore any emails requesting personal information (Mohd Zaharon et al., 2021). Bank employees were also advised to treat emails requesting personal login details with suspicion to protect customer data. Banks were encouraged to install protective anti-phishing solutions in mail servers to detect emails from suspicious sources.

## **PHISHING CONCEPT AND ITS PERPETRATION**

Phishing aims to misrepresent identity to persuade a target victim to provide helpful information to cybercriminals. Phishing targeting bank customers requires cybercriminals to masquerade as bank representatives so that the customers can unknowingly share their banking information, enabling the perpetrators to access bank accounts and siphon money from customers' accounts. Phishing activities have evolved, while customer awareness lags. The most common form of phishing is perpetrated through identity theft. Cybercriminals use different tactics to acquire customers' personal banking data and access their accounts illegally.

Below is an account of phishing and identity theft and a discussion of the various steps involved in a typical phishing attack.

### **Identity Theft Eroding Users' Trust**

An increase in internet coverage and usage by bank customers has been at the heart of the rising phishing crimes. Identity theft occurs when the perpetrators use the internet to target bank customers and mischievously persuade them to share personal details. The banking stakeholders are increasingly becoming sensitive about identity theft as it is the leading cause of digital-related crimes in the United States of America.

In Malaysia, there is a rise in the number of fraudulent computer activities reported, as disclosed by statistics from Malaysian Computer Emergency Response (MyCERT). In 2021, cyber threats incidents reported were broadly classified into fraud, intrusion, malicious codes, cyber harassment, and intrusion attempts, amongst others affecting over 10,000 adults in Malaysia. During the first 6 months of 2022, Kaspersky products also detected and blocked 27,458 phishing-related attempts targeting banking-related transactions and 91,895 targeting e-commerce shops in Malaysia. Phishing victims reported that the perpetrators used deceptive mechanisms to direct them to fake websites, where their usernames and passwords are stolen and used to the perpetrators' advantage. The increase in these crimes results in the breaching of information security by compromising the integrity of confidential personal data.

### **Phishing Modus Operandi**

According to (Basit et al., 2020), phishing emails before the mid-2003s were sent to target clients' emails in the form of text emails, where the perpetrators faked the logo of the target company to persuade customers to click the emails. However, in 2004, cybercriminals started deploying novel programming tactics and replaced the URL of the targeted company to resonate with the one displayed on the target's victims' address bar to be similar to the company they impersonated. The effect was that the cases of cybersecurity concerns reported globally increased, leading to losses of millions by victims.

Furthermore, since this was a new tactic, the victims were easily persuaded to provide their personal information because the cyber awareness culture did not match the evolving tactics the cybercriminals used in their practices. Jampen et al. (2020) found that since 2004, adult American citizens have received millions of emails from Phishers annually. These are significantly huge numbers, which indicates that email phishing poses a significant challenge in combating banking-related cyber-crimes.

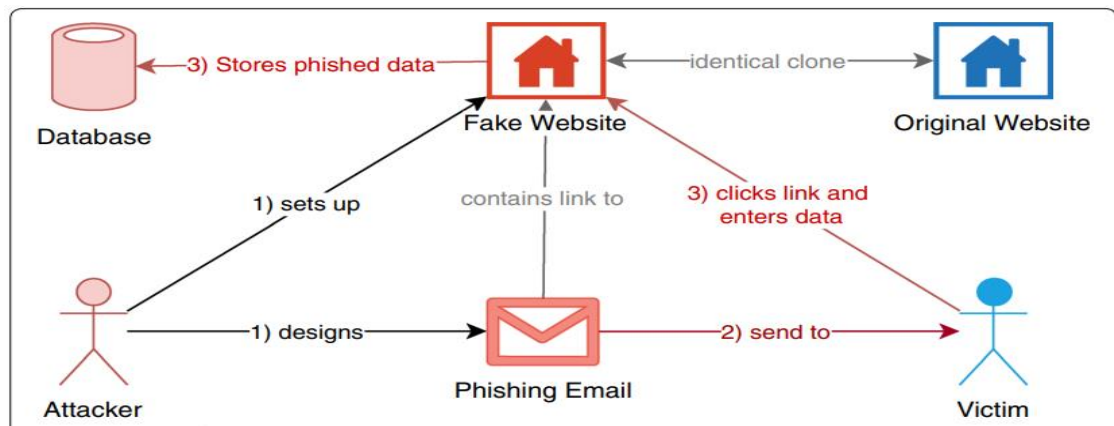
### **Use of fraudulently acquired data to perpetrate crimes.**

There are six stages that cyber criminals sequentially follow to execute a phishing attack. These are planning, launching, gathering data, determining ways to use the collected data, perpetrating the crime, and laundering the proceeds (Guan Gan et al., 2008).

### **Planning the attack**

At this phase, the phishing perpetrators usually determine their target clients and evaluate the nature of the data they want to acquire to achieve the intended goals. The attack method and messaging are selected at this stage. Examples of standard attack methods include email phishing, deceptive downloads, and pharming (Stafford & Capstone, 2020). Nowadays, there exist websites that offer cybercriminals assistance by providing them with links they use to perpetrate crimes.

**Figure 1 - Example of an email-based phishing attack**



*Source: Jampen et al., (2020)*

Figure 1 shows how cybercriminals use fake websites to send phishing emails to banking customers. They set up a website identical to clone websites similar to the bank's and use it to send emails to the customers. Since they use bank logos and fake letterheads, unsuspecting victims click on the email and provide the cyber criminals with the data they require to perpetrate cybercrimes. Cybercriminals store the data acquired in a database and can use it to execute criminal activities like money laundering or siphoning customer accounts. Unless customers understand cybersecurity threats, the attackers can easily persuade them to provide their banking details, increasing cybercrime propensity amongst the banking customers.

### **Launching attacks**

The launching phase entails sending out the information, referred to as the bait, to the target victims. The most common form of bait are emails and deceptive downloads (Stafford & Capstone, 2020). Other perpetrators recruit insiders to help with information harvesting from unsuspecting banking customers. Once installed, the downloads monitor the customers' details, which the perpetrators later use to execute crimes.

### **Gathering data**

In this stage, the perpetrators define the mechanisms of gathering personal data from an unsuspecting victim. When cybercriminals perpetrate cyberattacks, they aim to steal data (Narayanan et al., 2018). Methods used in data gathering include users entering the data in a spoofed website or email, using malicious software to capture data by monitoring the keystrokes made by the bank customers, and spying on data input on customer screens, amongst other options.

### **Determine the usage of gathered data.**

After acquiring the customer's data, the next step is deciding how to use it to access their banking information. The perpetrators must study the information required for authorization of online banking to enable them to use it without detection (Jaccard & Nepal, 2014). They also examine the credit limits set and transaction history to avoid flagging their activities by the banking system (Zong et al., 2019). Lastly, they contain the value of their target customers' accounts so that they get maximum returns from their crimes.

### **Perpetrate fraudulent activities.**

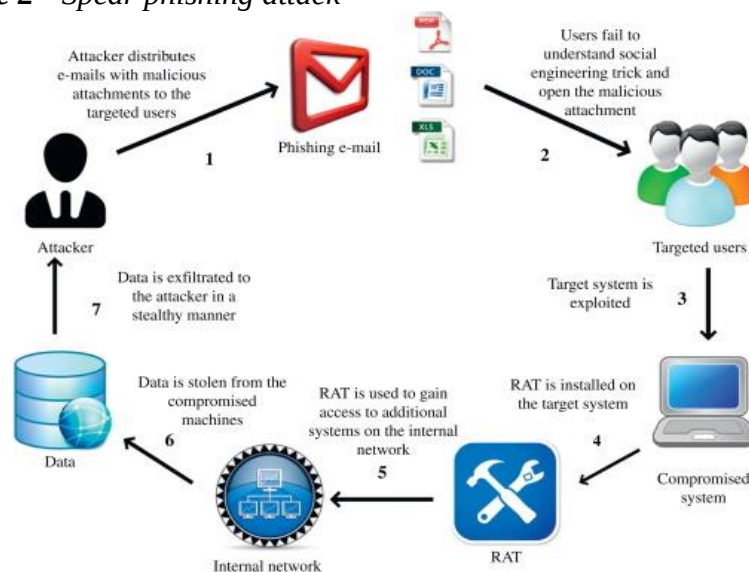
The fraud committed by perpetrators varies depending on various circumstances. The banking information may compel the victims to make lumpsum payments so that the

perpetrators do not share their personal information on different platforms. On the other hand, they could use it to siphon money out of customer accounts, leading to financial loss (Humayun et al., 2020). The perpetrators could use the information on credit cards and debit cards to make unauthorized purchases without their victim's knowledge.

### **Laundering proceeds**

Once the perpetrators of cybercrimes successfully execute their activities, their next focus is hiding their identity to avoid being detected by the authorities. The existence of money in virtual form enables the perpetrators to transfer it to different platforms and channels to mislead the authorities about their identity. This cash movement complicates tracking and tracing cybercriminals because they use fake accounts across other financial networks, making it difficult for the authorities to trace them (Guan Gan et al., 2008).

**Figure 2 - Spear phishing attack**



**Source:** (K Sood & Enbody, 2014)

Figure 2 shows how cybercriminals use emails as an avenue to perpetrate cyber-related fraud. An email with an attachment is sent out randomly by the attacker. If the user fails to detect that the email is malicious and opens it, the system targeted by the attacker is prone to further attacks perpetrated by installing RAT (Remote Access Trojan) in the target system. RAT becomes the avenue the cybercriminal uses to access internal networks and steal data from the compromised device. The attacker then infiltrates the data and uses it in a compromised manner. Cybersecurity awareness, especially on email phishing and the perpetration of cybercrimes using email phishing, is a critical subject today because of the advanced use of online banking services. Besides, the communication received from the bank in the form of emails is a suitable avenue that cybercriminals could use to persuade banking customers to provide them with personal data while masquerading as legit communication from the bank.

### **RELATED RESEARCH AND FINDINGS**

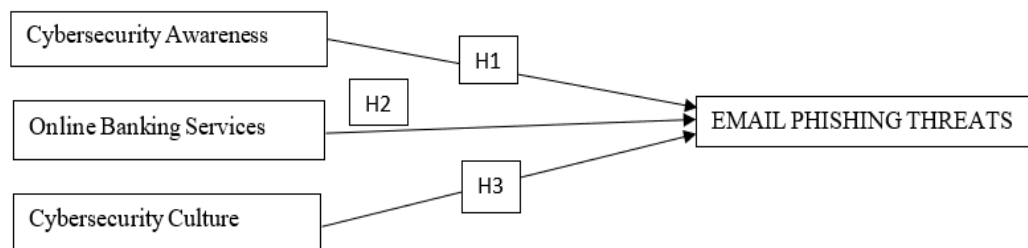
Cybercrime success is largely due to victims' unawareness of phishing attacks, despite security measures implemented by institutions (Ifeanyi Akazue et al., 2022). Technological advancements often outpace these measures, enabling criminals to continue their activities. Email phishing, the most prevalent form, involves sending deceptive emails that appear to come from legitimate organizations (Hodge et al., 2019). Increasing public awareness about phishing

is crucial in combating these crimes. Current security features for email authentication are easily guessable, often using client account numbers or identity details, leading to weak password management and increased phishing threats (Lee & Yim, 2020). Banks should consider alternative encryption methods for email communication to maintain confidentiality and regain trust from customers who have previously fallen victim to phishing attacks (Aonzo et al., 2018).

Morris et al. (2020) analyzed the evolution of phishing methods, noting that technological advancements have facilitated the prevalence of phishing. The rise of cloud computing and mobile phone usage necessitates anti-phishing techniques to mitigate cybercrime risks. Browser vulnerabilities and an increase in phishing websites are primary contributors to phishing attacks. Athulya and Praveen (2020) studied various phishing attacks and their emergence, suggesting that internet users adopt anti-phishing strategies to detect online phishing activities. Bhardwaj et al. (2020) observed that phishers continually innovate their tactics, making detection difficult. They propose that educating internet users about phishing is the most effective countermeasure.

## RESEARCH FRAMEWORK

**Figure 3**



**Source:** Own creation

Figure 3 shows the research framework and the relationship between the three hypotheses and the research model examined in the study. Cybersecurity awareness, frequency of online banking services, and cybersecurity culture are the independent variables in the research used to examine the susceptibility of banking customers to phishing email threats.

## RESEARCH GAPS

A review of past research shows that there is an agreement among researchers that the level of phishing awareness among internet users is wanting. The evolution of phishing activities complicates efforts to address phishing threats amongst internet users. However, it is unclear from previous research whether age affects the propensity to phishing attacks. In addition, though there is research done on the impact of phishing on banking data, the generalization of the findings does not shed light on the success rate of email-related phishing activities that target obtaining banking customers' data. In the Malaysian market, a few research have been conducted targeting email-phishing exposure in adults receiving regular communication from banks. These research delve into phishing challenges in Malaysia, but none has focused on how the adults that subscribe to internet banking are likely to become victims of email cybersecurity threats perpetrated through email phishing. This finding validates the need to research the susceptibility of banking email phishing targeting adult Malaysian citizens.

## DATA AND METHODOLOGY

The study utilized a research methodology grounded in pragmatism, emphasizing the importance of aligning research methodologies with the nature of the research subject. In this study, a quantitative methodology was employed to examine the influence of cyber security culture on the vulnerability of adults in the banking industry in Malaysia towards phishing emails. The primary data for this study was obtained by conducting a survey. The researchers aimed to get responses from a sample size of 97 participants, which was selected via convenience sampling. This method involved reaching out to potential respondents through both in-person interactions and social media platforms. The data collection instrument utilized in this study was Google Forms, which effectively maintained the anonymity of participants while allowing them to contribute valuable insights regarding their knowledge of email phishing threats, the prevailing cybersecurity culture, and other relevant aspects. The data analysis was performed using the Statistical Package for the Social Sciences (SPSS), adopting an explanatory research approach to clarify the relationships between the variables. In order to assess these associations in a rigorous manner, a meticulously designed survey consisting of 31 questions was constructed. The survey employed a 5-point Likert scale to gauge participant replies. The utilization of closed-ended questions was employed in order to get precise and detailed information. The survey encompassed demographic information in addition to enquiries pertaining to the factors under investigation. The study employed a cross-sectional design with a time frame of one month for data collection. This approach allowed for the examination of the dependent variable, susceptibility to email phishing threats, along with its independent variables, which included cyber security awareness, frequency of internet banking service usage, and cyber security culture. The primary objective of this comprehensive methodology was to offer significant insights into the research topic, with the intention of benefiting government entities, customers, and banking institutions in their efforts to mitigate financial risks linked to email phishing threats.

## RESULTS AND DISCUSSION

### DESCRIPTIVE STATISTICS

**Table 1** - Result of descriptive statistic

| Descriptive Statistics                     |                |                      |                      |                   |                             |           |            |           |            |
|--------------------------------------------|----------------|----------------------|----------------------|-------------------|-----------------------------|-----------|------------|-----------|------------|
|                                            | N<br>Statistic | Minimum<br>Statistic | Maximum<br>Statistic | Mean<br>Statistic | Std. Deviation<br>Statistic | Skewness  |            | Kurtosis  |            |
|                                            |                |                      |                      |                   |                             | Statistic | Std. Error | Statistic | Std. Error |
| Susceptibility to phishing emails          | 121            | 1.500000000          | 5.000000000          | 3.747933884       | .7087795008                 | -.299     | .220       | .145      | .437       |
| Cybersecurity Awareness                    | 121            | 2.166666667          | 5.000000000          | 3.929752066       | .6486282056                 | -.646     | .220       | -.127     | .437       |
| frequency of using online banking services | 121            | 2.000000000          | 5.000000000          | 3.716253444       | .6234776378                 | .082      | .220       | -.281     | .437       |
| Cybersecurity Culture                      | 121            | 2.166666667          | 5.000000000          | 3.695592287       | .6471725133                 | -.046     | .220       | -.495     | .437       |
| Valid N (listwise)                         | 121            |                      |                      |                   |                             |           |            |           |            |

*Source: Primary Data*

A descriptive analysis was carried out in order to evaluate the normality of the data that were utilized in this research. Descriptive statistics were a technique used in data analysis to provide a high-level overview of information associated with a dataset variable. These data were shown in a way that made it easier to visualize what the information was conveying. The standard deviation (a measure of variability) was used to show how the variables were

distributed and how they varied from one another in terms of variation. This offered a more in-depth explanation of the way in which the mean and the variable were connected to one another. Moreover, it was notable that Skewness and Kurtosis, as presented in Table 4.7, had significant importance within the realm of descriptive statistics. The concept of skewness was employed to assess the level of symmetry in a distribution that encompassed values that might be positive, negative, or zero. An ideal distribution was characterized by zero skewness, indicating that the mean was equal to the median. However, a positive skewness was observed when the data was concentrated towards the left side. Additionally, rightward skewing of the data was known as negative skewness.

Table 1 showed that the dependent variable for phishing email susceptibility had a negative skewness of -0.299. The skewness for the independent variables, on the other hand, showed values of -0.646, 0.082, and -0.046 for cybersecurity culture, frequency of utilizing online banking services, and cybersecurity awareness. The fact that every variable had a negatively skewed distribution may therefore be explained, with the exception of the frequency of utilizing online banking services, which exhibited a positive skewness. Kurtosis was used to determine if the data set had a heavy or light tail in comparison with a normal distribution. High kurtosis had heavy tails and more outliers than low kurtosis, which had light tails and fewer outliers. The dependent variable, which was "Susceptibility to Phishing Email," had a kurtosis value of 0.145. The kurtosis values came in at -0.127, -0.281, and -0.495 in terms of the independent variables, respectively.

## **FINDINGS AND DISCUSSIONS**

### **PEARSON'S CORRELATION TESTING**

The correlation is a statistical method employed to evaluate the potential linear relation between the dependent variable and the independent variables. The model is classified as the most straightforward and uncomplicated in the interpretation of collected data. The numbers depicted further elucidate that a value of 1 indicates a perfect correlation between the two variables. Moreover, in the case when  $r$  is equal to 0, there will be no apparent relationship between the two variables. In addition, the positive relationship between the two variables is shown when the value is greater than 0. Values below 0 or -1 represent a negative relationship between the two variables. In order to assess the association between Susceptibility to phishing emails, Cybersecurity Awareness, Frequency of using online banking services and Cybersecurity Culture this study utilized Pearson correlation analysis.



**Table 2 - Pearson Correlation Analysis**

|                                            |                     | Cybersecurity Awareness | Frequency of using online banking services | Cybersecurity Culture | Susceptibility to phishing emails |
|--------------------------------------------|---------------------|-------------------------|--------------------------------------------|-----------------------|-----------------------------------|
| Cybersecurity Awareness                    | Pearson Correlation | 1                       | .478**                                     | .618**                | .612**                            |
|                                            | Sig. (2-tailed)     |                         | <.001                                      | <.001                 | <.001                             |
|                                            | N                   | 121                     | 121                                        | 121                   | 121                               |
| Frequency of using online banking services | Pearson Correlation | .478**                  | 1                                          | .575**                | .404**                            |
|                                            | Sig. (2-tailed)     | <.001                   |                                            | <.001                 | <.001                             |
|                                            | N                   | 121                     | 121                                        | 121                   | 121                               |
| Cybersecurity Culture                      | Pearson Correlation | .618**                  | .575**                                     | 1                     | .537**                            |
|                                            | Sig. (2-tailed)     | <.001                   | <.001                                      |                       | <.001                             |
|                                            | N                   | 121                     | 121                                        | 121                   | 121                               |
| Susceptibility to phishing emails          | Pearson Correlation | .612**                  | .404**                                     | .537**                | 1                                 |
|                                            | Sig. (2-tailed)     | <.001                   | <.001                                      | <.001                 |                                   |
|                                            | N                   | 121                     | 121                                        | 121                   | 121                               |

\*\* . Correlation is significant at the 0.01 level (2-tailed).

*Source: Primary Data*

#### **Correlation between cybersecurity awareness and the susceptibility of adult Malaysian citizens to phishing emails.**

The correlation coefficient of cybersecurity awareness and susceptibility to phishing emails was 0.612. The p-value was 0.000 (lower than 0.05). Therefore, we conclude that the relationship of cybersecurity awareness and susceptibility to phishing emails factors is positive and significant. We conclude that there is a relationship between cybersecurity awareness and the possibility of adult banking customers in Malaysia receiving a banking-related phishing email.

#### **Correlation between the frequency of using online banking services and the susceptibility of adult Malaysian citizens to phishing emails.**

Frequency of using online banking services and susceptibility to phish emails had a correlation coefficient of 0.404. P-value was established at 0.000. This, we conclude that the relationship of frequency of using online banking services and susceptibility to phishing emails factors is positive and significant. We therefore conclude that there is a relationship between the frequency of using online banking services and the possibility of adult banking customers in Malaysia receiving a banking-related phishing email.

#### **Correlation between cybersecurity culture and the susceptibility of adult Malaysian citizens to phishing emails.**

Correlation coefficient of cybersecurity culture and susceptibility to phishing emails was 0.537. The p-value was 0.000 (lower than 0.05). Therefore, we conclude that the relationship of cybersecurity culture and susceptibility to phishing emails factors is positive and significant. We conclude that there is a relationship between cybersecurity culture and the possibility of adult banking customers in Malaysia receiving a banking-related phishing email.

### MULTIPLE REGRESSION TESTING

The connection between the dependent (Susceptibility to phishing emails) and independent variables (Cybersecurity Awareness, frequency of using online banking services and Cybersecurity Culture) is investigated using multiple regression analysis.

**Table 3 - Model Summary**

| Model Summary <sup>b</sup> |                   |          |                   |                            |
|----------------------------|-------------------|----------|-------------------|----------------------------|
| Model                      | R                 | R Square | Adjusted R Square | Std. Error of the Estimate |
| 1                          | .646 <sup>a</sup> | .418     | .403              | .5477552284                |

a. Predictors: (Constant), Cybersecurity Culture , frequency of using online banking services, Cybersecurity Awareness

b. Dependent Variable: Susceptibility to phishing emails

*Source: Primary Data*

The resulting R-squared score was 0.418. This suggests that cybersecurity awareness, frequency of using online banking services and cybersecurity culture account for 41.8% of the variation in Susceptibility to phishing emails.

**Table 4 - ANOVA**

| ANOVA <sup>a</sup> |            |                |     |             |        |                    |
|--------------------|------------|----------------|-----|-------------|--------|--------------------|
| Model              |            | Sum of Squares | df  | Mean Square | F      | Sig.               |
| 1                  | Regression | 25.180         | 3   | 8.393       | 27.974 | <.001 <sup>b</sup> |
|                    | Residual   | 35.104         | 117 | .300        |        |                    |
|                    | Total      | 60.284         | 120 |             |        |                    |

a. Dependent Variable: Susceptibility to phishing emails

b. Predictors: (Constant), Cybersecurity Culture , frequency of using online banking services, Cybersecurity Awareness

*Source: Primary Data*

If the p-value is less than or equal to 0.05, then the relationship between the two variables is significant, and the null hypothesis will be rejected; if the p-value is greater than 0.05, then there is no significance between the variables, and the null hypothesis will be accepted. The F-value and p-value for the regression analysis were 27.974 and 0.000, respectively. A p-value of less than 0.05 demonstrates that the cybersecurity awareness, frequency of using online banking services and cybersecurity culture factors have a significant influence on possibility of adult banking customers in Malaysia receiving a banking-related phishing email.

#### 5.2.1 Relationship between cybersecurity awareness and the possibility of Malaysian banking customers receiving phishing email.

**H<sub>01</sub>:** There is no relationship between cybersecurity awareness and the possibility of adult banking customers in Malaysia receiving a banking-related phishing email.

**H<sub>a1</sub>:** There is a relationship between cybersecurity awareness and the possibility of adult banking customers in Malaysia receiving a banking-related phishing email.

In this research, the null hypothesis, H<sub>01</sub> is rejected but the alternative hypothesis, H<sub>a1</sub> is accepted. Cybersecurity Awareness has a positive impact on Susceptibility to phishing emails among banking customers. Additionally, research by Taylor and Antonucci (2014) showed that training initiatives aimed at raising cybersecurity awareness had a favorable influence on people's capacity to recognize phishing emails. These programs advise users about typical phishing tactics, offer tips for spotting strange emails, and stress the significance of avoiding clicking on dubious links or disclosing personal information. It is crucial to promote a culture of cybersecurity awareness among users and inside companies to successfully battle phishing threats. Regular training programs, awareness campaigns, and the sharing of best practices can help with this. Organizations and people may improve their protection against phishing email threats and lower their risk of financial loss, data breaches, and other negative outcomes by spreading cybersecurity knowledge.

**Relationship between the frequency of using online banking services and the possibility of Malaysian banking customers receiving phishing email.**

**H<sub>02</sub>:** There is no relationship between the frequency of using online banking services and the possibility of adult banking customers in Malaysia receiving a banking-related phishing email.

**H<sub>a2</sub>:** There is a relationship between the frequency of using online banking services and the possibility of adult banking customers in Malaysia receiving a banking-related phishing email.

The null hypothesis is rejected, H<sub>02</sub> and the alternative hypothesis, H<sub>a2</sub> is accepted as the relationship between the variables are significant. Frequency of using online banking services has a positive impact on Susceptibility to phishing emails among banking customers. Similarly, Florêncio and Herley (2009) noted that those who often use online banking services may be more vulnerable to phishing schemes. Individuals who often use online banking services must exercise caution and take precautionary actions to reduce the hazards brought on by phishing email attacks. This include keeping security banking software up to date, using strong passwords, and being wary of dubious email communications. The frequency of utilizing online banking services and susceptibility to phishing email attacks may be related, according to research. People may be exposed to phishing attempts more frequently when they engage in online banking activities more regularly, making them more vulnerable to such risks. Phishing emails pretend to be from legitimate businesses in an effort to fool recipients into disclosing personal information like login passwords or financial information. The likelihood of running into phishing efforts increases as more people use internet banking.

**Relationship between cybersecurity culture and the possibility of Malaysian banking customers receiving phishing email.**

**H<sub>03</sub>:** There is no relationship between cybersecurity culture and the possibility of adult Malaysian citizens receiving a banking-related phishing email.

**H<sub>a3</sub>:** There is a relationship between cybersecurity culture and the possibility of adult Malaysian citizens receiving a banking-related phishing email.

In this research, the null hypothesis, H<sub>03</sub> is rejected but the alternative hypothesis, H<sub>a3</sub> is accepted. Cybersecurity Culture has a positive impact on Susceptibility to phishing emails among banking customers (Beta = 0.253, p-value of 0.020). Effective communication channels that enable staff to quickly report suspicious emails or security issues are characteristics of a good cybersecurity culture. According to research by (Alsharnouby et al., 2015), firms with established reporting processes were more likely to notice and stop phishing attempts. To effectively counter phishing email threats, firms must have a strong cybersecurity culture. Uchendu et al. (2021) study found that successful phishing attempts were less common in companies with a good cybersecurity culture. According to the study, customers at businesses with strong cybersecurity cultures were more likely to spot and report phishing emails, which reduced their vulnerability to such threats. This emphasizes the value of creating an environment that encourages cybersecurity awareness, education, and proactivity.

**Table 5 - Results of Hypotheses**

|                 | <b>Hypotheses</b>                                                                                                                                                                      | <b>Results of hypotheses</b> |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| H <sub>01</sub> | There is no relationship between cybersecurity awareness and the possibility of adult banking customers in Malaysia receiving a banking-related phishing email.                        | <b>Rejected</b>              |
| H <sub>a1</sub> | There is a relationship between cybersecurity awareness and the possibility of adult banking customers in Malaysia receiving a banking-related phishing email.                         | <b>Accepted</b>              |
| H <sub>02</sub> | There is no relationship between the frequency of using online banking services and the possibility of adult banking customers in Malaysia receiving a banking-related phishing email. | <b>Rejected</b>              |
| H <sub>a2</sub> | There is a relationship between the frequency of using online banking services and the possibility of adult banking customers in Malaysia receiving a banking-related phishing email.  | <b>Accepted</b>              |
| H <sub>03</sub> | There is no relationship between cybersecurity culture and the possibility of adult Malaysian citizens receiving a banking-related phishing email.                                     | <b>Rejected</b>              |
| H <sub>a3</sub> | There is a relationship between cybersecurity culture and the possibility of adult Malaysian citizens receiving a banking-related phishing email.                                      | <b>Accepted</b>              |

*Source: Own Creation*

## **RECOMMENDATION AND CONCLUSION**

### **Recommendation**

For future researchers, several suggestions and recommendations can be made to enhance the study on phishing sustainability in the context of Malaysian banking and beyond.

Expanding the sample size is a crucial first step to improve the accuracy of results. Increasing the respondent pool to encompass a more diverse cross-section of Malaysian bank account holders, including different age groups, genders, economic backgrounds, and regional populations, would yield a more comprehensive dataset. This would allow for the discovery of subtle relationships and patterns that smaller samples might overlook. Additionally, researchers should consider broadening the scope of the study to cover various sectors beyond banking, including e-commerce, social networking sites, and healthcare. Phishing is a pervasive issue in these areas, and studying its vulnerability across different industries can provide a more comprehensive understanding.

To enhance data reliability, adopting experimental designs such as using simulated phishing emails in a controlled environment is advisable. This approach minimizes potential errors resulting from self-reporting in surveys. Advanced analytical techniques, including machine learning algorithms like Random Forests, Neural Networks, or Support Vector Machines, could be employed to identify intricate patterns and non-linear correlations related to phishing vulnerability.

Qualitative research methods like interviews or focus group discussions should be integrated with quantitative analysis to gain deeper insights into individuals' experiences, attitudes, and decision-making processes regarding phishing emails. This holistic approach can offer valuable insights for organizational procedures and policymaking in the dynamic digital landscape. Frequent users of online banking are especially vulnerable to phishing, so banks should regularly update clients on new phishing schemes and promote safe internet behavior through various channels. Encouraging a strong cybersecurity culture within banks should be a priority, involving clients and staff in fostering responsible behavior, enforcing regulations, and reporting phishing attempts.

Lastly, partnerships with technology and cybersecurity firms can bolster defenses. Integration of cutting-edge technology like Artificial Intelligence can aid in identifying and preventing phishing attempts. Collaborations may also lead to innovative products, such as AI-powered chatbots guiding users through secure online banking or tools for detecting phishing emails.

### **Conclusion**

The research investigated the correlation between email phishing awareness and cybersecurity threats, with a focus on adult Malaysian banking customers. The findings affirmed a positive and significant relationship between cybersecurity awareness, the frequency of using online banking services, and cybersecurity culture, with susceptibility to phishing emails. Consequently, it was deduced that heightened awareness and adoption of secure online behaviors significantly reduced the risks associated with phishing emails.

Banks were advised to leverage these insights to implement controls that mitigated the threats posed by phishing emails to their clients' data. Bank Negara Malaysia could also have utilized these findings to enforce regulatory measures aimed at curbing cybercrimes perpetuated through email phishing. The study further elucidated the necessity for public education on email phishing, advising online banking users to routinely update their passwords. This research was not only a valuable resource for individuals who had never encountered phishing attempts but also served as a credible reference for future researchers exploring related topics. Ultimately, this study contributed significantly to the broader understanding of the cybersecurity initiatives needed to counter email phishing, thereby benefiting governments, financial institutions, and individual banking customers.

## REFERENCES

- Abdullah, F., Salwa Mohamad, N., & Yunus, Z. (2018). Safeguarding Malaysia's Cyberspace against Cyber Threats: Contributions by CyberSecurity Malaysia. *Journal of Cyber Security*, 1, 22–31.
- Alabdan, R. (2020). Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet*, 12(10), 1–37. <https://ideas.repec.org/a/gam/jftint/v12y2020i10p168-d421901.html>
- Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). *Why phishing still works: User strategies for combating phishing attacks*. <https://doi.org/10.1016/j.ijhcs.2015.05.005>
- Aonzo, S., Merlo, A., Tavella, G., & Fratantonio, Y. (2018). Phishing Attacks on Modern Android. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. <https://doi.org/10.1145/3243734.3243778>
- Athulya, A., & Praveen, K. (2020). *Towards the Detection of Phishing Attacks*. 337–343. [https://www.researchgate.net/publication/343034856\\_Towards\\_the\\_Detection\\_of\\_Phishing\\_Attacks](https://www.researchgate.net/publication/343034856_Towards_the_Detection_of_Phishing_Attacks)
- Banu, M. N. B., & Banu, S. M. (2013). *A Comprehensive Study of Phishing Attacks*. 783–786. <https://www.studocu.com/my/document/universiti-teknologi-mara/cyber-law/a-comprehensive-study-of-phishing-attacks/39244490>
- Basit, A., Zafar, M., Javed, A. R., & Jalil, Z. (2020). A Novel Ensemble Machine Learning Method to Detect Phishing Attack. *2020 IEEE 23rd International Multitopic Conference (INMIC)*. <https://doi.org/10.1109/inmic50486.2020.9318210>
- Bhardwaj, A., Sapra, V., Kumar, A., Kumar, N., & Arthi, S. (2020). Why is phishing still successful? *Computer Fraud & Security*, 2020(9), 15–19. [https://doi.org/10.1016/s1361-3723\(20\)30098-1](https://doi.org/10.1016/s1361-3723(20)30098-1)
- Florêncio, D., & Herley, C. (2009). *A Large-Scale Study of Web Password Habits*.
- Guan Gan, G. G., Ling, T. N., Yih, G. C. Y., & Eze, U. C. (2008). *Phishing: A Growing Challenge for Internet Banking Providers in Malaysia Communications of the IBIMA Phishing: A Growing Challenge for Internet Banking Providers in Malaysia*.
- Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arabian Journal for Science and Engineering*, 45(4), 3171–3189. <https://doi.org/10.1007/s13369-019-04319-2>

- Ifeanyi Akazue, M., Adimabua Ojugo, A., Elizabeth Yoro, R., Ogheneovo Malasowe, B., & Nwankwo, O. (2022). Empirical evidence of phishing menace among undergraduate smartphone users in selected universities in Nigeria. *Indonesian Journal of Electrical Engineering and Computer Science*, 28(3), 1756.  
<https://doi.org/10.11591/ijeecs.v28.i3.pp1756-1765>
- Jaccard, J. J., & Nepal, S. (2014). *A survey of emerging threats in cybersecurity*. 973–993.  
[https://www.researchgate.net/publication/260155713\\_A\\_survey\\_of\\_emerging\\_threats\\_in\\_cybersecurity](https://www.researchgate.net/publication/260155713_A_survey_of_emerging_threats_in_cybersecurity)
- Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: towards an effective anti-phishing training. A comparative literature review. *Human-Centric Computing and Information Sciences*, 10(1). <https://doi.org/10.1186/s13673-020-00237-7>
- K Sood, A., & Enbody, R. (2014). *Targeted Cyber Attacks*. SearchSecurity.  
<https://www.techtarget.com/searchsecurity/feature/Targeted-Cyber-Attacks>
- Lee, K., & Yim, K. (2020). Cybersecurity Threats Based on Machine Learning-Based Offensive Technique for Password Authentication. *Applied Sciences*, 10(4), 1286.  
<https://doi.org/10.3390/app10041286>
- Mohd Zaharon, N. F., Mohd Ali, M., & Hasnan, S. (2021). Factors Affecting Awareness of Phishing Among Generation Y. *Asia-Pacific Management Accounting Journal*, 16(2), 409–444. <https://doi.org/10.24191/apmaj.v16i2-15>
- Morris, D., Madzudzo, G., & Garcia-Perez, A. (2020). *Cybersecurity threats in the auto industry: Tensions in the knowledge environment*.  
<https://doi.org/10.1016/j.techfore.2020.120102>
- Narayanan, S., Ganesan, A., Joshi, K., Oates, T., Joshi, A., & Finin, T. (2018). Early Detection of Cybersecurity Threats Using Collaborative Cognition. | BibSonomy. [Www.bibsonomy.org](http://www.bibsonomy.org).  
<https://www.bibsonomy.org/bibtex/d1d340920b9b50efc0c133fdea5acefe>
- Stafford, C., & Capstone, A. (2020). *WEAKEST LINK: ASSESSING FACTORS THAT INFLUENCE SUSCEPTIBILITY TO FALLING VICTIM TO PHISHING ATTACKS AND METHODS TO MITIGATE*.
- Supayah, G., & Ibrahim, J. (2016). An Overview of Cyber Security in Malaysia. *Kuwait Chapter of Arabian Journal of Business and Management Review*, 6(4), 12–20.  
<https://doi.org/10.12816/0036698>

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, 109, 102387.

<https://doi.org/10.1016/j.cose.2021.102387>

Zong, S., Ritter, A., Mueller, G., & Wright, E. (2019). *Analyzing the Perceived Severity of Cybersecurity Threats Reported on Social Media*. <https://arxiv.org/abs/1902.10680>