Phishing Awareness and Training Report

Chameleon Security Team

Author:

Name:	Student ID:	Team:
Rewniz Patell	221267802	Chameleon Security

Table of Contents

Summary:

This report was written and research by Rewniz Patell from the Chameleon Security Team. This report involves building awareness and understanding of phishing attacks within the Chameleon organization. This report is aimed at any individual within Chameleon, and therefore is written to ensure that members with less Cyber Security/IT knowledge can understand and become aware of phishing attacks. This report aims to define phishing attacks, highlight the increased prevalence of phishing attacks in recent years, showcase individuals within Chameleon can do to become aware of these attacks, and what strategies Chameleon can implement to train members and ensure proper methods are in place to combat phishing attacks.

Introduction:

A phishing attack involves a malicious attacker tricking a victim into taking action that benefits the attacker. The act of 'phishing' is when the attacker attempts to steal sensitive or confidential information such as passwords, documents, bank information, or other important information from a victim, or enable the attacker to gain access to certain systems or permissions, that they are not authorized to access. Attackers would usually attempt to masquerade as a trusted source such as a large or authorized organization, a person of importance, or another member within the same organization as a victim [1].

Phishing attacks can be conducted from multiple different vectors. This includes emails, text messages, application messages (such as Microsoft Teams, Discord), phone calls or fake/unauthorized websites. Successful phishing attacks can lead to identity theft, bank fraud, ransomware attacks, data breaches, and damage to IT and security infrastructure for companies and organizations [2]. Furthermore, phishing attacks can target a single individual or a whole organization. A single individual within an organization may be targeted as the attackers believe that this individual would be a potential victim of an attack, they may have information or context to the individual which could assist with the attack such as understanding their role within an organization, knowing background information on the target, or having a means of communication with the target. Additionally, a whole organization or a large group of individuals in an organization may be targeted, such as a group of members within a certain critical department, a department that does not work in a digital field (in an attempt to target individuals that are unaware of phishing attacks), or sending mass messages to an organization's employees in attempt to find a single victim that falls for the attack.

To combat phishing attacks, employees would need to be educated and trained, to decrease the chances of successful phishing attacks to occur and to increase the chances of these attacks being reported and investigated. This is referred to as phishing awareness, where individuals are educated on phishing, and common phishing techniques and vectors of attack. Additionally, phishing training involves training individuals to identify phishing attacks, report them through the correct channels, and utilizing strategies to avoid phishing attacks. This would involve phishing awareness and training to occur at the individual employee levels, where each member of the organization is educated and trained to avoid becoming victims to phishing attacks, and the organization as a whole employing methods and mitigation strategies to ensure that phishing attacks are not successful, and minimize damage if an attack does occur [3].

Phishing Awareness:

Prevalence of Phishing Attacks:

Phishing attacks have had an increased prevalence in recent years. Many factors have contributed to the rapid rise of phishing attacks including,

- Email and text messaging (common vectors for phishing attacks) being widespread and used frequently by a large amount of people.
- Phishing attacks require simple targeting and little context information. All information that is required is a destination email address/phone number.
- A small amount of technical skills to set up phishing attacks, such as sending mass emails and text messages. No requirement of knowledge for hacking, or information technology skills.
- Potential for a wide target reach, can send emails and texts in mass numbers, allowing a scattered approach to finding targets.
- Low cost of entry just requires some devices, emails (which are free), and one person to send the emails/messages. This means that few victims are required for the perpetrator to see profits from the attack.

[4].

Due to these factors, phishing attacks have become increasingly common at an individual level. During 2022, phishing attacks were by far the largest reported scam within Australia, with 74,573 reported phishing attacks within the year. This was more than double second and third place, with other scams and false billing having 28,203 and 27,488 reports during the year of 2022 [5].

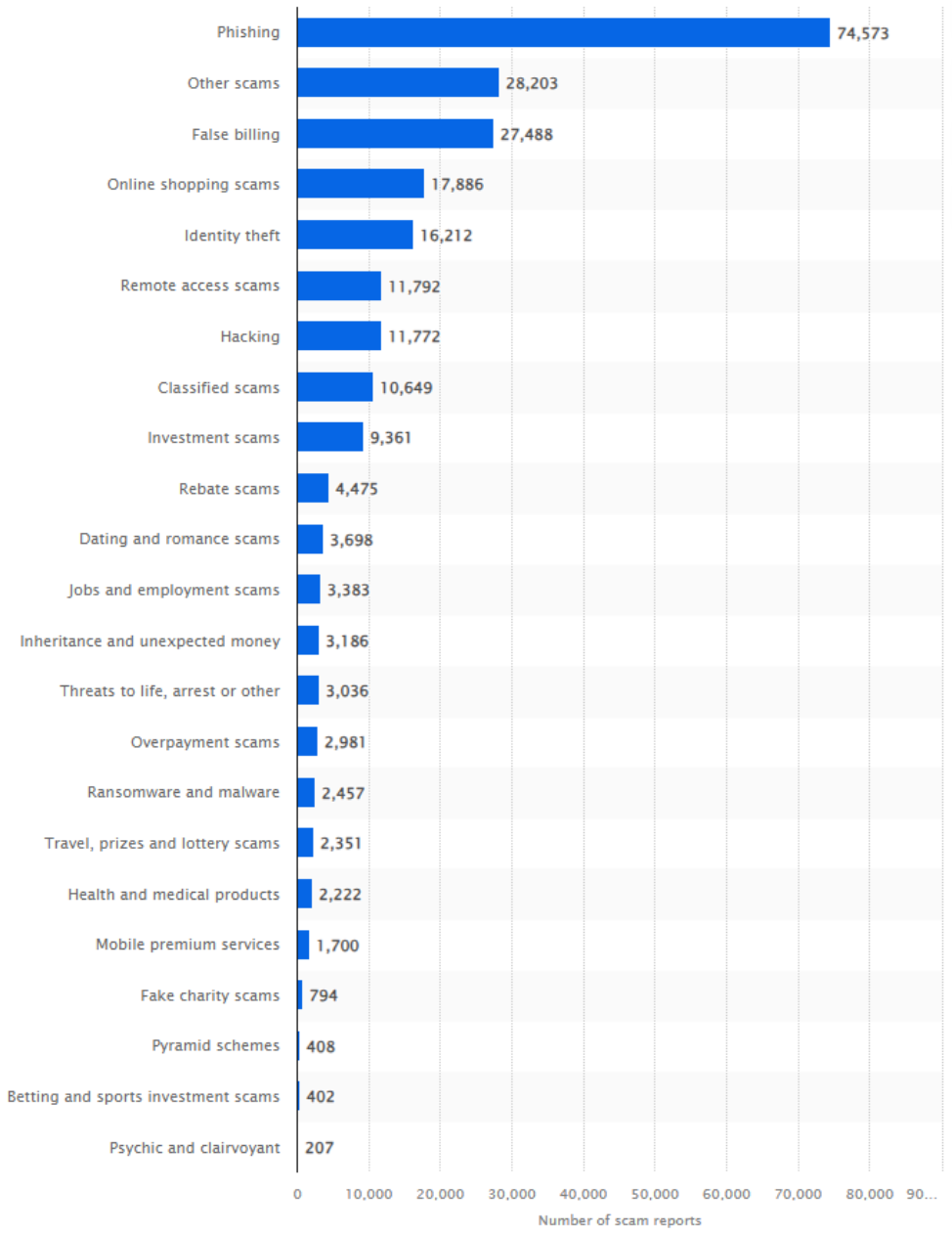

Figure 1: Number of Reported Scams In Australia in 2022, by Category. [5]

Furthermore, organizations such as companies and government departments are also seeing an increase in phishing attacks. In a survey conducted amongst a mix of companies and government departments within Australia, 63% of respondents reported that they were a victim to phishing attacks in 2022. This was the highest of all cyber-attacks, and 8% higher than the second most common attack, which was ransomware [6].

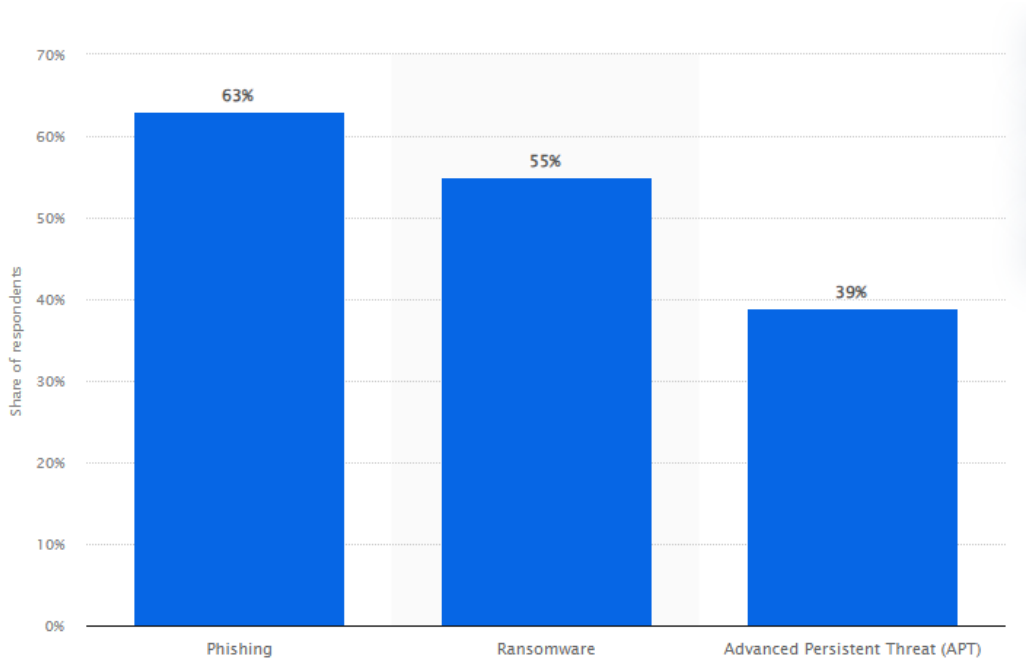

Figure 2: Cyber attack types organizations were most likely to fall victim to in Australia as of 2022. [6]

This highlights that phishing attacks are also extremely prevalent at an organizational level, underlining the importance of increasing training and awareness being required within Australian organizations in regard to phishing attacks.

Phishing Awareness strategies for Chameleon:

Phishing awareness involves teaching the individuals within the organization on prevalence of phishing, common phishing methods, identifying phishing attacks, and protecting themselves against phishing attacks [7].

Strategies that Chameleon could implement to ensure that all individuals within the organization, and the organization as a whole understand phishing attacks are,

- Teaching individuals the prevalence of the phishing attack, to highlight how common they are.
- Understanding what phishing attacks are, and how to identify a phishing attack.
- Teaching individuals how to report phishing attacks.
- How Chameleon Security can identify the difference between a common phishing attack, and phishing attacks that target the organization. Attacks that target the organization and its members implies that an attacker has information (such as names, emails, roles, etc) on certain individuals/departments within the organization, and are using that information to target individuals within the organization.
- What actions individuals within the organization can take if they are unsure if an email/message is legitimate or a phishing attack.

Increasing awareness for phishing attacks is important, as a single successful attack could cause extremely high amounts of damage to Chameleon infrastructure, or confidential information being accessed by the attacker. Therefore, increasing the awareness of phishing attacks at an individual level is highly important, as a single individual may be targeted by a phishing attack. Phishing awareness at an individual level would decrease the chances of a individual within Chameleon falling for a phishing attack.

Phishing Training within Chameleon:

Phishing training should be implemented at both an individual level, where each member of the organization is aware and trained to deal with phishing attacks, and an organizational level to ensure that the proper avenues for reporting and investigating attacks are implemented within Chameleon.

Company-wide Strategies:

For training of individuals to be successful, adequate, and proactive measures needs to first be implemented by the company. For example, an individual within Chameleon may know that they are required to report a phishing attack, but strategies need to be implemented to ensure that they have an avenue to report the attack, and that there are individuals who can investigate the attack within the organization. Company-wide strategies need to be multilayered, to ensure that all potential vectors for phishing attacks are protected and reviewed.

The first step that Chameleon Security should implement is ensuring that malicious phishing emails do not reach individuals within the organization. Taking a proactive step to limit the number of attacks would ensure that phishing attacks do not even reach an individual, causing the potential of risk. Methods to implement this include,

1. Email and message filtering: This will ensure that phishing attacks and spam emails/messages are filtered, with malicious emails not reaching the target. Tools such as SpamTitan and MailCleaner are paid tools which could be implemented, or the Chameleon Security team could manually implement their own filtering system within the mail server, or organization email/message platform.
2. Anti-phishing tools: These are tools that utilize machine learning and AI to analyze links and attachments within messages, and automatically warn the user that the contents of the email are dangerous.
3. Blocking techniques: When phishing attacks are reported and investigated, implementing blocking measures would ensure that future phishing attacks do not reach the destination target. Blocking known IP addresses, domain names, email address, messaging senders and known spam senders would help to ensure that the phishing attacks do not reach the target employee within Chameleon.

The second step would be to implement a reporting system and investigation team. Having a method to report emails to a member of Chameleon (such as a member of Chameleon Security) would ensure after individuals have been made aware of phishing attacks, and do report them, that there is an avenue for investigation. The investigation team can then investigate the email/message, decide whether the email is a phishing attack, potentially block the sender, and block the contents of the email from being accessed by a member within Chameleon if it's a known threat.

The third step would be to ensure that if a phishing attack is successful, then measures are in place to limit the damage. Members within the organization should only have access, read, and write privileges that are required, to avoid attackers having permissions if they

gain access to a single account. Limiting what employees within Chameleon can do, such as download software, access admin accounts, and ensuring that members are on a 'need to know basis' ensures that attackers do not have access to valuable Chameleon information, or the ability to make changes to Chameleon infrastructure or projects.

The final strategy would be to ensure that phishing attacks are detected quickly, whether they are successful or not, and that they are investigated in a prompt manner. This would ensure that the organization is able to swiftly detect common phishing attacks, or targeted attacks before an individual within the organization falls for the attack. Furthermore, investigating attacks in a prompt manner would ensure that measures can be taken in the future to avoid an individual from falling for a phishing attack, such as blocking known spam addresses, blocking known phishing domain names, or training an employee that did fall for the attack [8].

Individual Training:

Once the company strategies are implemented and phishing awareness is conducted at an organizational level, individual training should be conducted. This ensures that individuals understand Chameleon strategies and know what is expected of them in regards to phishing attacks. Individual training could include phishing awareness and training when a new member is brought into Chameleon, having extensive training for individuals with high level of privileges or access to confidential information (such as senior members or leading members), and having regular awareness training so Chameleon members understand new and emerging phishing attacks. Individual training can commence after the awareness training, where members understand phishing attacks, the prevalence of phishing attacks and how to identify phishing attacks. Training methods could include,

1. After identifying a phishing attack, training the member to report the attack correctly.
2. Effective documenting of attacks before reporting, so that the investigation team understands the situation.
3. Training members to 'self-report' if they are a victim of phishing attacks. This way the organization can promptly respond and take effective measures early before the attacker has time to embed themselves within Chameleon infrastructure. This would involve ensuring that employees who do self-report are not punished or ridiculed, so that Chameleon members feel do not feel reluctant to report on themselves in case they face punishment.
4. Having easily accessible resources that individuals can refer to and know that they can access, in case they need to spot or compare a legitimate email/message with a phishing attack.

Conclusion:

Phishing attacks have had an extreme increase in prevalence in recent years. As a result, organizations like Chameleon need to take effective employee awareness and training measures to ensure that sensitive data is protected, consumer data is not accessed or leaked by attackers, and measures are in place to report and mitigate phishing attacks. Furthermore, if Chameleon does expand in the future, the organization may be susceptible to more attacks or targeted by more attackers, and therefore these strategies listed in the report to increase phishing awareness and training would help to combat this.

References (IEEE):

[1] Cloudfare (2021) 'What is a phishing attack?' [Website]. Available: https://www.cloudflare.com/learning/access-management/phishing-attack/

[2] IBM (Unknown date) 'What is phishing?' [Website]. Available: https://www.ibm.com/topics/phishing

[3] Cybersecurity & Infrastructure Security Agency (Unknown date) 'Teach Employees to Avoid Phishing' [Website]. Available: https://www.cisa.gov/secure-our-world/teach-employees-avoid-phishing

[4] Next (Sep 2023) 'Why do Phishing Attacks Happen?' [Website]. Available: https://www.nextdlp.com/resources/blog/why-do-phishing-attacks-happen#:~:text=These%20include%3A,out%20a%20password%20to%20succeed.

[5] C. Hughes (Aug 2023) Statista 'Number of Reported Scams in Australia in 2022, by Category' [Website]. Available: https://www-statista-com.ezproxy-f.deakin.edu.au/statistics/864989/australia-number-of-scam-reports-by-leading-category/

[6] C. Hughes (Jun 2023) Statista 'Cyber attack types organizations were most likely to fall victim to in Australia as of 2022' [Website]. Available: https://www-statista-com.ezproxy-f.deakin.edu.au/statistics/1342446/australia-cyber-attack-types-organizations-were-most-likely-to-fall-victim-to/

[7] Holm Security (Unknown date) 'Fundamentals: Phishing Awareness' [Website]. Available: https://www.holmsecurity.com/fundamentals/phishing-awareness

[8] National Cyber Security Centre (Feb 2024) United Kingdom Government 'Phishing attacks: defending your organization' [Website]. Available: https://www.ncsc.gov.uk/guidance/phishing#:~:text=Filter%20or%20block%20incoming%20phishing,ie%20in%20the%20mail%20client).