|  |
| --- |
| Samuel Holmes  Student ID: BI64OI  Module Code: CETM69 |

Phishing Attacks – Examining Their Prevalence and the Potential Implications for Organisations

Table of contents

Introduction

1

1

2

2

4

5

7

8

9

Rationale for subject choice

Target Audience

Importance of Issue to Cybersecurity

Impact on Society

Professional and ethical issues

Conclusions

References

Appendix

Introduction

The online technological landscape has steadily developed since the 1970s, starting with the invention of the internet in 1969 following the development of ARPANET (National Science and Media Museum, 2020). This gradual progression led to the creation of the World Wide Web (World Wide Web Consortium, 2009), shaping the familiar web landscape that we know today. With society rapidly adopting multiple forms of electronic communication, there are intrinsic threats to security for individuals and organisations. Reliance on electronic communication methods continues to grow, understanding the threats that exist is imperative to protect end users and mitigate risk where possible.

Phishing attacks, a common method of exploitation used by cybercriminals, are primarily conducted through electronic communication streams. ‘Phishing scams trick users into divulging sensitive data, downloading malware, and exposing themselves or their organisations to cybercrime’ (IBM, 2023). With 30% of adults worldwide encountering phishing scams in 2022 and 1.35 million unique phishing sites detected in the fourth quarter the same year (Petrosyan, 2024). The frequency rates of these incidents indicate the need for individuals and organisations to understand phishing attacks. As the electronic landscape has evolved, so too have the methods of attack used by cybercriminals. It is necessary for professionals, individuals, and organisations to be prepared with adequate knowledge to defend themselves against these dynamic threats.

Rationale for subject choice

The selection of phishing attacks for this report and the preceding infographic (Figure 1, Appendix) stems from an awareness of their prevalence, the widespread impact these attacks have, and the evolving tactic employed by their instigators. Within a professional capacity and daily life many of us will encounter phishing attack training or even an attempted attack. The manipulation of human vulnerability that underpins this area adds a sinister element to their modus operandi. Whilst the importance of recognition and education should not be underestimated, it is important that the infographic and report demonstrate the need of a layered security system. This approach accepts that human error can and will occur, and proposed defence mechanisms should not solely rely on employee’s ability of threat identification. Highlighting the ways in which technology can be utilised to supplement weaknesses posed by the human element of the targeted enterprises is imperative.

Considering the evolution of phishing attacks from scattered email assaults to more targeted approaches such as Business Email Compromise (BEC), spear-fishing, and whaling, demonstrates the adaptability of attackers. Emphasizing the need for malleability of organisations, individuals, and the cybersecurity defences they employ to combat this issue. With 79% of 2,263 UK businesses surveyed in 2023 facing phishing attacks over a twelve-month period, the extent of organisations effected is the majority (Binns, 2023). It remains a contemporary and relevant topic for anyone with an interest in the field of cybersecurity.

Target Audience

The goal of the previous infographic was to be accessible to a varied audience, with the aim of introducing and explaining the technical aspects of phishing attacks in an accessible and digestible manner. The information contained was intended to be beneficial to both organisations and individuals. However, it emphasized the implications for organisation’s as opposed to individual users. This was to remain aligned with the idea that prevention of phishing attacks should not solely be the responsibility of the individual (end user employees of an organisation). It highlights the critical need to remove over reliance on human identification of fraudulent communications as a primary defence mechanism. The infographic aims to educate organisations about the nature of phishing attacks, the common methods employed by attackers, their impact on businesses, and key security. The infographic concludes with the recommendation of a layered defensive mechanism, this is supported by the NCSC (2018) who suggest layers of mitigation. See Figure 2 (appendix) for an illustration of how this system will look and act within an organisation’s cybersecurity defence.

Importance of Issue to Cybersecurity

Phishing attacks remain a significant issue within the field of cybersecurity due to their delivery methods, frequency, and the key cybersecurity principles they seek to undermine. With the shift in workplace practices accelerated by the Covid 19 pandemic email communication has become a main correspondence for working professionals (Carroll, Adejobi and Montasari, 2022) involved in remote working practises. Within the context of a workplace setting, it is easier for fraudulent emails to appear as legitimate ones.

Phishing attacks themselves, have evolved from broader scattered approaches to highly targeted operations. With spear-phishing and whaling encompassing attacks pursuing specific individuals within an organisation. Oftentimes, those with seniority status and with-it higher security and authorisation clearance. With the level of scrutiny that goes into planning such attacks the likelihood of detection becomes even slimmer. The focus on an individual target also allows attackers opportunity to bypass more traditional defence mechanisms such as access controls and multi-factor authentication and instigate further damage.

Some of the key cybersecurity principles that phishing attacks contradict are the CIA triad, accountability, and non-repudiation. Examining the ways in which these principles are undermined allows understanding as to why this is a prevalent issue within the contemporary cybersecurity landscape. Firstly, concerning the CIA triad, confidentiality, integrity, and availability. Regarding confidentiality, phishing attacks are designed to steal sensitive business information. Examples of such information include login credentials, personal information, and financial data. This exposes the organisation non-compliance issues with General Data Protection Regulations (GDPR) (Gov.UK, 2018), financial fraud and identity theft of employees.

Furthermore, integrity is threatened, with unauthorised access to data, integrity becomes a key concern. Attackers may seek to modify data through compromised login credentials or by introducing malware designed to destroy or corrupt data (National Cyber Security Centre, 2020). If this business-critical information becomes incorrect it can lead to improper operational decisions, harming business revenue and reputation. Lastly within the CIA triad, availability can be affected, often phishing attacks act as a gateway for the deployment of ransomware. Ransomware is utilised to lock end users out of the system and or to encrypt data needed by the organisation for general operations. This will be the case until the business pays the agreed sum, even then there is no guarantee access will be regranted. This can bring organisations to a standstill causing significant financial damage.

There are also some further implications not included within the ‘Effects of phishing attacks on organisations’ section of the infographic. Firstly, surrounding the principle of accountability. Phishing attacks aim to complicate the tracking and accountability of the malicious actions performed. Attackers often perform such actions under the guise of false identity provided by obtained login credentials, making these operations appear legitimate at initial inspection. This can make it difficult to associate malicious action with the true perpetrator and hold them accountable for their actions. Accountability further ties into the principle of non-repudiation, and how this is undermined by phishing attacks. Non-repudiation is a key cybersecurity principle used to ensure that the origin of data can be verified (NIST, 2023). This is achieved through cryptographic techniques such as digital signatures and secure timestamps. This allows for exact validation of the date and time of an action that has taken place. In the case of phishing attacks once access is gained attackers oftentimes delete or manipulate these digital logs. This ensures difficulty for the organisation when trying to prove occurrences of change, again complicating accountability proof and potential legal proceedings following an attack.

In addition to the threats to key cybersecurity principles the exploitation of human vulnerabilities within the security chain as opposed to the technological vulnerabilities that exist remains to be a key point of thought. The employment of social engineering tactics that rely on flaws in human behaviour make phishing attacks particularly difficult to defend against. As attackers continue to further refine their practices the need for more advanced and adaptive security protocols is exposed. This issue will remain prevalent within the field of cybersecurity for the near future, where there is human influence there is vulnerabilities and threats.

Impact on society

Phishing attacks that negatively affect businesses in turn destabilise economic health and overall societal welfare. Regarding organisations, phishing attacks impact various sectors including financial, operational, reputational, and legal. Some of these impacts are demonstrated throughout the diagrams contained in the infographic. It is also important to recognise that beneath these organisations is a societal structure that depends upon them, further highlighting the need to protect such organisations with cybersecurity measures.

From an economic standpoint financial loss is a major implication of a successful phishing attack. In 2022 the average BEC attack attempted to steal 132,559 U.S Dollars (Binns, 2023), phishing attacks are detrimental to overall business health due to the financial losses of such magnitude. To demonstrate the magnitude of certain attacks diagrams with the losses experienced were included in the infographic. Although financial losses are dangerous for any business it can be particularly difficult for small to medium sized enterprises to recover from such a loss. Often leading to failure of the business entirely. In addition to the costs seen due to immediate financial loss there are secondary costs to be considered. Remediation costs post attack can include, investigation of data breaches, implementing further and stronger security measures than previously seen, and restoration of corrupted data or damaged systems. Further to this, many companies today pay for cyber insurance, this is insurance specifically designed to help an organisation pay for any financial losses they may incur in cases of a cyberattack or a data breach. Organisations that fall victim to phishing attacks will see an increase in insurance costs in the form of higher premiums following such an event (BBC, 2024).

Furthermore, there is the implications for ability of conducting normal operations or BAU (business as usual). It is likely organisations will experience significant downtime during and after a phishing attack. Namely, due to ransomware, malware, and damage to business-critical data. This can be extremely destructive for businesses that provide essential services to society, this not only impacts the business but also the clientele it serves. There is also the compromise of the sensitive data itself, this affects not only the business from a legal standpoint but also the customers it serves in respect to confidentiality.

The issues have wider reaching impacts than just the business operations of the organisation in question. Phishing attacks can have consequences from a reputational perspective as well, lowering customer confidence. This can in turn effect employee morale and customer loyalty, potentially contributing to an overall increased level of distrust within society for digital exchanges and data stores. This is exacerbated by the fact those most susceptible to phishing attacks are those with less technological expertise. This can further enhance a digital divide and contribute to certain demographics resigning from involvement with technology.

Professional and ethical issues

As a cybersecurity professional there are multiple professional and ethical issues that should be considered regarding phishing attacks. Primarily, regarding issues from a professional viewpoint there are a few distinct examples worth reflection. As an authority there is an inherent duty to protect, it should be the prerogative and responsibility to implement security measures that provide protection for individuals and organisations against evolving phishing attacks. It is important that as professionals’ methods of continued professional development and concurrent research occur, this allows us to stay prepared and knowledgeable on the current threats posed.

Furthermore, there should be the aim to provide training that empowers end users. Training should be constructed to give users the ability to recognise and report phishing attacks without making them overly fearful of falling victim to an attack. Over suspicion can lead to lowered productivity whilst complacency can lead to increased attack success and further damage. Finding this balance in training delivery will be an important contemplation for any expert imparting knowledge in this sector of cybersecurity. Tied into this principle there are issues surrounding accountability for breaches, this can be considered both an ethical and professional issue. This is the question of who is at fault where an attack is successful if adequate training has been provided, is the end user or the cybersecurity team within an organisation responsible. This also brings into question how this should be rectified and how many lapses of judgement from users should lead to disciplinary action if any.

Conclusions

Throughout the infographic and the following report, the significance of the dangers posed by phishing attacks has become increasingly apparent, their pervasive nature and evolving traits allow them to stay at the forefront of cybersecurity. Utilising cybersecurity frameworks such as the NIST framework (FTC 2018) and a zero-trust architecture are useful concepts for consideration. However, it is key that vigilance and resilience are maintained, and proper user training is given to employees within organisations. It is only through continued development, education, prompt incident response and layered defence mechanisms that impacts of phishing attacks can be reduced.

References

BBC (2024). *Why some cyber-attacks hit harder than others.* *BBC News*. [online] 23 Feb. Available at: https://www.bbc.co.uk/news/business-68225892.

Binns, R. (2023). *UK phishing statistics | The Independent*. [online] Independent Advisor. Available at: https://www.independent.co.uk/advisor/vpn/uk-phishing-statistics.

Carroll, F., Adejobi, J.A. and Montasari, R. (2022). *How Good Are We at Detecting a Phishing Attack? Investigating the Evolving Phishing Attack Email and Why It Continues to Successfully Deceive Society. SN Computer Science*, 3(2). doi:https://doi.org/10.1007/s42979-022-01069-1.

FTC (2018). *Understanding the NIST cybersecurity framework*. [online] Federal Trade Commission. Available at: https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework.

Gov.UK (2018). *Data Protection Act*. [online] Gov.uk. Available at: https://www.gov.uk/data-protection.

IBM (2023). *What is phishing? | IBM*. [online] www.ibm.com. Available at: https://www.ibm.com/topics/phishing.

National Cyber Security Centre (2020). *Mitigating malware and ransomware attacks*. [online] www.ncsc.gov.uk. Available at: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks.

National Science and Media Museum (2020). *A Short History of the Internet*. [online] National Science and Media Museum. Available at: https://www.scienceandmediamuseum.org.uk/objects-and-stories/short-history-internet.

NCSC (2018). *Phishing attacks: defending your organisation*. [online] www.ncsc.gov.uk. Available at: https://www.ncsc.gov.uk/guidance/phishing?ref=thestack.technology#section\_5.

NCSC (2019). *Email security and anti-spoofing*. [online] Ncsc.gov.uk. Available at: https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing.

NCSC (2021). *Introduction to Zero Trust*. [online] www.ncsc.gov.uk. Available at: https://www.ncsc.gov.uk/collection/zero-trust-architecture/introduction-to-zero-trust.

NIST (2023). *Non-repudiation - glossary | CSRC*. [online] csrc.nist.gov. Available at: https://csrc.nist.gov/glossary/term/non\_repudiation.

Petrosyan, A. (2024). *Phishing - Statistics & Facts*. [online] Statista. Available at: https://www.statista.com/topics/8385/phishing/#topicOverview.

World Wide Web Consortium (2009). *Tim Berners-Lee*. [online] W3.org. Available at: https://www.w3.org/People/Berners-Lee/.

Appendix

*A screenshot of a computer

Description automatically generatedFigure 1 – Phishing attacks infographic assessment task 1*

*Figure 2 – Detailed layered defence mechanism expanded from infographic*

|  |  |  |
| --- | --- | --- |
| Layer | Description | How does this help prevent phishing attacks or mitigate risk |
| 1 | Zero trust architecture | The system should be designed with zero trust principles employed. Inherent trust should be removed. Validation and verification should be at the forefront (NCSC, 2021) |
| 2 | This layer should reduce the ability of hackers to even contact employees within the organisation. This is achieved through anti spoofing and email filtering. | Email filtering ensures that many malicious emails do not reach the inbox of employees within the organisation. Further reducing likelihood of a threat becoming an attack. Anti spoofing prevents hackers from sending fraudulent emails from the company domain allowing them to impersonate trusted employees. This is achieved with a sender policy framework that only allows trusted IP addresses (NCSC, 2019) |
| 3 | Network segmentation instilled at the design phase of the infrastructure. | If a network is segmented prior to attack in a worst-case scenario it acts as a further access control. Potentially minimising damage done |
| 4 | Use of secure web gateways and application monitoring tools. | Secure web gateways allow for filtering of potentially malicious URLS. There are also various tools that can be used to monitor application use |
| 5 | Protection of devices | Ensure malware protection software is used. Schedule regular software updates of hardware and software as part of security protocols. |
| 6 | Incident response and reporting | Ensure effective incident response plans are established prior to an attack to minimise damage caused. Culture a no blame reporting and feedback loop to empower staff in feeling confident when dealing with threats. |