Beyond User Error: Psychological Manipulation in Phishing Attacks

John M. Booth
Independent Cyber Security Researcher
research@jmbooth.co.uk
ORCID: 0009-0005-1765-4646
DOI: https://doi.org/10.5281/zenodo.20364058

Abstract

This paper investigates how traditional phishing training centred around spotting patterns and components of a phishing email may be antiquated in the modern threat landscape. It looks at how users who have had this training can still fall victim to phishing attacks as modern complex phishing attacks focus on emotive response and emotional exploitation. With one example of such tactics being "Amygdala Hijacking" (Chemudupati and Valecha, 2024) where an attacker may use consequence tactics or plausible reasoning to force a user into an emotive state to perform actions like responding to the email or downloading or inputting personal information when ordinarily without the use of these tactics they would not. This paper does not explore in depth into psychological, neurological or biological causation it discusses "Amygdala Hijacking" (Chemudupati and Valecha, 2024) as a concept in the context of phishing. This paper also advises training considerations that could assist in the mitigation of this threat.

Keywords: phishing, amygdala hijacking, social engineering, phishing training, cybersecurity awareness

1. Introduction

Phishing is one of the most utilised vectors of initial access a threat actor will employ when trying to attack a victim. For those outside cyber security and some even in industry, there can be assumptions made around the cause of phishing attacks succeeding. Assumptions are made around user error or a lack of education regarding the key signs of a phishing email. While a lack of basic education can contribute, that does not explain how those who have had said education can still fall victim to phishing attacks even when knowing the common signs of one. Over the years

phishing attacks have become more complex and advanced, now exploiting emotional states and exploiting inter-organisational relationships and perceived status to be more effective.

2. Emotional manipulation and amygdala hijacking in phishing emails

In the past phishing attacks were simpler such that education could be focused effectively for users, teaching them common signs of a potential malicious email such as spelling mistakes, broken English, calls to action, potentially malicious attachments and links to websites that don't look legitimate. While these tactics are still employed there has been an advancement in the language and ways attackers manipulate users. A more advanced phishing attack targets an emotional response utilising language not too dissimilar from scare tactics. This language is designed to add pressure to the victim. Eventually via these tactics threat actors plan to have the victim succumb to the attack in the heat of the moment. This language is designed for psychological manipulation.

A 2024 study theorised that the amygdala part of the brain, which is the part of the brain used for emotional processing, alarm and emotion regulation. Said emotions may include fear and anxiety. These emotions may be being exploited during a phishing attack (Chemudupati and Valecha, 2024). Specifically the use of consequence (Chemudupati and Valecha, 2024), exploiting the amygdala fear and anxiety complex is utilised to initiate an emotive response that the subject would be unlikely to do if these tactics were not employed, this is paired with how users under stress are more likely to make decisions without the initial thoughts of consequences (Lininger and Vines, 2005). The three areas it was theorised were a threat of punishment, a threat to territory and a threat of status (Chemudupati and Valecha, 2024)

2.1. Punishment Threat

Examples of a punishment threat occur when an attacker threatens repercussions for inaction. For example, a victim's account is to be closed, sanctions added to a victim's personal account like limiting services or even threats to a victim's employment or personal circumstances.

2.2.Territory Threat

Threats of territory revolve around access. An attacker may try to provide reasoning or rationale to provide perceived legitimacy for the action being asked. Usually using language around how an account may have had unauthorised access or unauthorised communications, leading a victim to believe they have potentially already been compromised.

2.3 Status Threat

A threat to status focuses on both public and intra-organisational statuses of both the company and the victim. An example includes a threat actor threatening a senior member of staff that inaction could be shown as incompetence.

3. Organisational Impact

Organisational impact from successful phishing attacks is well documented. Another impact has been found pertaining to a “double hit” with both financial and psychological impacts (Cazanis et al., 2025), after people fall victim. There can be correlations made to a reduction in staff morale with many victims feeling shame from the fear of blame (Cazanis et al., 2025). A study showed victims of scams like phishing feel blamed and mocked by friends and family (Cazanis et al., 2025).

4. Training Considerations

As mentioned, a lack of traditional training can contribute to an attack. Training that focuses solely on visual elements of a phishing email is antiquated. A better training regime would be to implement emotional analysis training helping users understand how these emails can affect their emotional response and how to look out for that, how to understand the three emotional manipulation categories utilised in these attacks and the organisational realities. Organisational procedures and policies following industry best practice frequently differ from the rationales attackers give in their phishing emails. It would also be deemed pertinent that an organisation would educate employees around how their information technology and cyber security procedures work. This helps mitigate rationales threat actors give, if employees know how internal organisational administration works then it makes these assumed pressure rationales easier to identify.

5. Conclusion

This paper reviews how traditional end user training focused on identifying components of a phishing email is useful, though in the current threat landscape that training alone is antiquated. Modern complex phishing attacks target emotional response and emotional manipulation utilising techniques such as “Amygdala Hijacking” to pressure victims into quick, out of character, responses to phishing attacks usually leading to credential, personal information or device compromise. Considerations need to be made by organisations at how to develop training that can assist their employees to understand how these attacks are targeting their emotions and how to utilise education on organisational procedures to help employees recognise the inconsistencies in attacker rationales.

References

Cazanis, A., Carminati, J.-Y., Chew, K., Cross, C., Ponsford, J. and Gould, K.R. (2025). 'Falling into a Black Hole': A Qualitative Exploration of the Lived Experiences of Cyberscam Victim-Survivors and Their Social Support Networks. *Victims & Offenders*, pp.1–20. doi:https://doi.org/10.1080/15564886.2025.2481267.

Chemudupati, S. and Valecha, R. (2024). *Phishing Email Detection Through Amygdala Hijack Threats*. [online] AIS Electronic Library (AISeL). Available at: https://aisel.aisnet.org/neais2024/8.

Lininger, R. and Vines, R.D. (2005). *Phishing : cutting the identity theft line*. Indianapolis, Ind.: Wiley Pub.