What are they?

Fraudulent communications sent to individuals, organizations or employees (IBM, 2023).
They attempt to coerce individuals or employees into:

- Downloading malware or ransomware
- Sharing personal or business sensitive information

This can then expose the individuals or the organisations they represent to cyber attacks. They are conducted through various channels but most commonly email (Gupta, 2020).

Common phishing methods

- BEC - Business Email Compromise. Attackers will impersonate an executive within the organisation, vendors, and or a supplier (CISCO, 2024). Allowing them to receive false payments and steal login credentials. Allowing extraction of further data and instigation of damage
- Spear fishing - targets a specific individual within an organisation rather than a wider group of people this allows attackers to have a targeted focus that will lead to further access (Farrier, 2023)
- Whaling - The individual targeted will be a high ranking executive known as a whale due to their organisational importance. The attackers will falsify payments needing approval, attempt to obtain login credentials and will use the officials seniority to provide access to a wider array of sensitive information (IBM, 2024)



Effects of phishing attacks on organisations

- Financial loss & negative effects on share prices when a Phishing attack is realised and reported
- Unauthorized access and modification of data (loss of integrity)
- Data breaches (loss of confidentiality)
- Compromised credentials
- Malware infections (loss of availability)
- Training methodology of raised suspicion surrounding emails can hinder workplace productivity

A successful phishing attack can effect all three aspects of the CIA triad

Phishing attacks in the real world

- The first notable phishing attack was performed on AOL users in 1995 (Amos, 2023)
- The FBI reported that in 2020 phishing attacks caused the loss of $1.8 billion in the U.S.A (Hillman, Harel and Toch, 2023)
- Below are some recent instances of major phishing attacks with the reported approximate financial damages (Irwin, 2021)

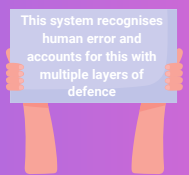
Colonial Pipeline (£2.9 billion)	Facebook & Google (£77 million)	Sony Pictures (£68 million)	Crelan Bank (£65 million)	FACC (£36 million)
2021	2013-2015	2014	2016	2016

Prevention methodology and key security points

It is important that organisations do not solely rely on employee's abilities to detect fraudulent correspondence as many are well executed and indistinguishable from genuine communications (Office for National Statistics, 2022).

The National Cyber Security Centre suggests a 'multi-layered' approach to preventing phishing threats from becoming a full attack (NCSC, 2018).

"There's no silver bullet with cybersecurity; a layered defense is the only viable option." — James Scott. (DigitalDefynd, 2023).



Layer 1 - Ensure attackers cannot reach users easily (filtering and anti spoofing)

Layer 2 - Provide adequate training (train staff to spot phishing emails, instil a no blame culture)

Layer 3 - Protect from phishing communication that is not detected (multi factor authentication)

Layer 4 - Respond quickly if an attack occurs

SAMUEL HOLMES (BI6401)

Reference List

Amos, Z. (2023). *Phishing Case Studies: Lessons Learned From Real-Life Attacks* Available at: https://cyberexperts.com/phishing-case-studies-lessons-learned-from-real-life-attacks/. [Accessed 20/01/2024].

CISCO (2024). *What Is Phishing? Examples and Phishing Quiz*. Available at: https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#:~:text=Phishing%20works%20by%20luring%20a%20victim%20with%20legitimate-looking [Accessed 03/02/2024].

DigitalDefynd, T. (2023). *100 Inspirational Cybersecurity Quotes [2024]*. Available at: https://digitaldefynd.com/IQ/inspirational-cybersecurity-quotes/. [Accessed 24/01/2024].

Farrier, E. (2023). *Spear phishing: Definition + protection tips*. Available at: https://us.norton.com/blog/online-scams/spear-phishing. [Accessed 25/01/2024].

Gupta, P. (2020). *Council Post: Top Phishing And Security Threats Every Business Should Be Aware Of*. Available at: https://www.forbes.com/sites/forbestechcouncil/2020/10/07/top-phishing-and-security-threats-every-business-should-be-aware-of/ [Accessed 18 Jan. 2024].

Hillman, D., Harel, Y. and Toch, E. (2023). *Evaluating Organizational Phishing Awareness Training on an Enterprise Scale*. Computers & Security , 132. doi:https://doi.org/10.1016/j.cose.2023.103364.

IBM (2023). *What is phishing? | IBM*. Available at: https://www.ibm.com/topics/phishing. [Accessed 19/01/2024].

IBM (2024). *What is whale phishing? | IBM*. Available at: https://www.ibm.com/topics/whale-phishing. [Accessed 01/02/2024].

Irwin, L. (2021). *The 5 biggest phishing scams of all time*. Available at: https://www.itgovernance.eu/blog/en/the-5-biggest-phishing-scams-of-all-time. [Accessed 02/02/2024].

Office for National Statistics (2022). *Phishing attacks – who is most at risk? - Office for National Statistics*. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/phishingattackswhoismostatrisk/2022-09-26. [Accessed 20/01/2024].