Cyber Secure

Module 2

Phishing

Author: George Nicholl

Student ID: 50095130

Phishing is one of the most widespread and effective cyber threats, targeting individuals and organisations through deceptive emails, texts and websites. These attacks are designed to trick victims into revealing sensitive information such as login credentials, financial details or personal data. Understanding how phishing works and how to prevent it is essential in reducing cybersecurity risks.

According to the Anti-Phishing Working Group (APWG), phishing reached 989,123 in the fourth quarter of 2024, highlighting the increasing prevalence of these threats.

This module compliments the associated training video and offers a more in-depth exploration of phishing methods, examples and prevention strategies to reinforce learner understanding.

What is Phishing?

Phishing is a form of cyberattack that relies heavily on social engineering. It manipulates into clicking malicious links, downloading infected attachments, or giving up confidential data under false pretences.

Common phishing methods include:

- **Email phishing** – Attackers send emails that appear to be from legitimate sources, containing malicious links or attachments. Phishing accounts for nearly 39.6% of all email-based cyber threats.
- **Spear phishing** – A targeted attack aimed at a specific individual or organization, often using personalized details to increase credibility.
- **Smishing (SMS phishing)** – Fraudulent messages sent via SMS or messaging apps to trick users into clicking malicious links.
- **Vishing (Voice phishing)** – Attackers use phone calls to impersonate a trusted organization and convince victims to share sensitive information.
- **Clone phishing** – A legitimate email is copied and modified to include malicious links or attachments, then sent from an address that looks similar to the original sender.

An estimated 3.4 billion phishing emails are sent each day, demonstrating the sheer scale and persistence of this cyber threat.

Common Threats or Mistakes

A. Clicking Suspicious Links

- Users often click without verifying the source
- Attackers use urgency, fear or curiosity to lure victims

B. Downloading Infected Attachments

- Attachments may contain malware or ransomware
- Often disguised as invoices, receipts or job offers

C. Providing Sensitive Information

- Fake login pages harvest usernames and passwords
- Victims may reveal credit card details or personal data

D. Failing to Recognise Deceptive Messages

- Poor grammar or suspicious URL's are overlooked
- Generic greetings like "Dear customer" go unnoticed

Together, these behaviours make phishing highly successful and difficult to eradicate without consistent awareness and proactive security measures.

Real-World Examples

- **Google and Facebook Scam (2013–2015)** – A hacker impersonated a legitimate vendor and tricked both companies into transferring over $100 million.
- **Sony Pictures Hack (2014)** – A phishing attack compromised employee credentials, allowing hackers to access and leak sensitive data.
- **Twitter Bitcoin Scam (2020)** – Attackers used social engineering and phishing to gain control of high-profile Twitter accounts, posting fraudulent cryptocurrency offers.
- **Ubiquiti Networks Breach (2015)** – Cybercriminals posed as executives and manipulated employees into wiring $46 million.

Phishing remains the leading cause of cyberattacks, with 79% of UK businesses that experienced cyber incidents in 2023 identifying phishing as the primary attack method.

Reducing Phishing

Organisations and individuals can take several steps to protect themselves against phishing attempts:

A. Recognise Phishing Attempts

- Double check sender email addresses and domains
- Avoid clicking on suspicious or unexpected links
- Be cautious with messages that create urgency or fear

B. Technical Safeguards

- Enable Multi-Factor Authentication (MFA)
- Use robust email filtering and anti-phishing tools
- Keep software and systems full updated

C. Employee Training & Awareness

- Conduct regular phishing simulations
- Educate teams on identifying threats
- Encourage open reporting of suspicious messages

D. Incident Response Measures

- Report suspected phishing immediately to IT/Security
- Reset credentials and enable extra security
- Monitor accounts for suspicious activity

Key Takeaway

Phishing is not just a technical problem – it's a human one. Attackers rely on psychological manipulation, not just skill behind a computer. This means that no matter how strong your technical defences are, a single lick from an unaware individual can still open the door to significant harm. Phishing remains one of the biggest cybersecurity threats, relying on human error and deception to succeed. With 67.4% of phishing attacks now utilizing artificial intelligence, they are becoming increasingly sophisticated. Understanding Phishing tactics, recognising the signs and encouraging a security-first mindset across an organisation is essential to closing the human gap in cybersecurity.

Why This Matters for You

Phishing attacks exploit trust, routine and distraction. The more familiar individuals become with the signs of a phishing attack, the less likely they are to fall for them. This module supports both technical and non-technical individuals in building stronger reflexes against manipulation and deception.

Quick Recap: Phishing Best Practices

DO:

- ✓ Always verify sender addresses before engaging with emails
- ✓ Hover over links to confirm where they lead
- ✓ Use multi-factor authentication to reduce risk if credentials are stolen
- ✓ Report suspicious emails rather than deleting them silently

DON'T

- X Don't download unexpected attachments, even from known contacts
- X Don't respond to urgent requests without verifying legitimacy
- X Don't reuse passwords across accounts

References

Anti-Phishing Working Group (APWG) (2024) *Phishing Activity Trends Report Q4 2024*. Available at: https://apwg.org/trendsreports/ (Accessed: 2 April 2025).

IBM (2023) *Cost of a Data Breach Report 2023*. Available at: https://www.ibm.com/security/data-breach (Accessed: 2 April 2025).

National University (2024) *Cybersecurity Statistics 2024*. Available at: https://www.nu.edu/blog/cybersecurity-statistics/ (Accessed: 2 April 2025).

Egress (2024) *Must-Know Phishing Statistics for 2025*. Available at: https://www.egress.com/blog/security-and-email-security/must-know-phishing-statistics-for-2025 (Accessed: 2 April 2025).

GetAstra (2024) *Phishing Attack Statistics 2024*. Available at: https://www.getastra.com/blog/security-audit/phishing-attack-statistics/ (Accessed: 2 April 2025).

Hoxhunt (2024) *Phishing Trends Report 2024*. Available at: https://hoxhunt.com/guide/phishing-trends-report (Accessed: 2 April 2025).

AAG IT (2024) *The Latest Phishing Statistics*. Available at: https://aag-it.com/the-latest-phishing-statistics/ (Accessed: 2 April 2025).