EMAIL PHISHING: RECOGNISE, RESIST, AND REPORT

In the digital age, understanding and combating email phishing is more critical than ever. This presentation will equip you with the knowledge to identify, avoid, and report these insidious cyber threats.

INTRODUCTION TO EMAIL PHISHING

Email phishing is a fraudulent practice where cybercriminals attempt to trick individuals into divulging sensitive information or performing actions that compromise their security. These attacks often mimic legitimate organisations or trusted contacts, exploiting human trust and urgency.

The consequences of falling victim to a phishing scam can range from financial losses and identity theft to reputational damage and data breaches for businesses. Staying vigilant and informed is your first line of defence.

HOW DOES EMAIL PHISHING WORK?

Phishing attacks typically follow a well-orchestrated process, designed to exploit vulnerabilities at every step.

1. DECEPTIVE EMAIL

Attackers send emails that appear to be from legitimate sources, such as banks, social media platforms, or IT support.

2. URGENCY & FEAR

The email often contains urgent language, threats, or enticing offers to prompt immediate action without critical thought.

3. MALICIOUS LINK/ATTACHMENT

Victims are directed to click a link leading to a fake website or download a malware-infected attachment.

4. INFORMATION THEFT

On the fake site, users are prompted to enter credentials, financial details, or other personal data, which is then stolen.

Spearning

Phishing

Smishng

Vi-shing

COMMON TYPES OF PHISHING

Phishing attacks are diverse and constantly evolving. Here are some of the most prevalent forms you should be aware of:

SPEAR PHISHING

Highly targeted attacks aimed at specific individuals or organisations, often leveraging personal information for credibility.

WHALING

A sophisticated form of spear phishing targeting senior executives and high-profile individuals to gain access to valuable company assets.

SMISHING

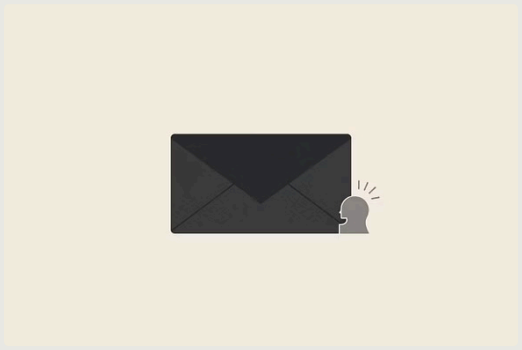
Phishing attempts conducted via SMS text messages, often containing malicious links or requests for personal information.

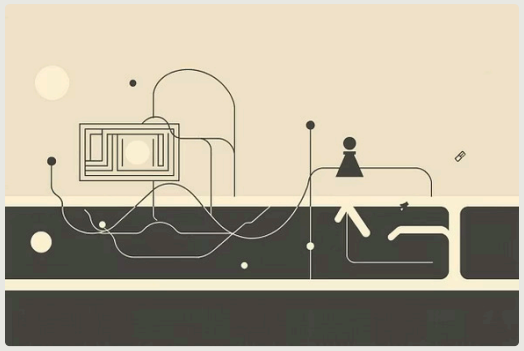
VISHING

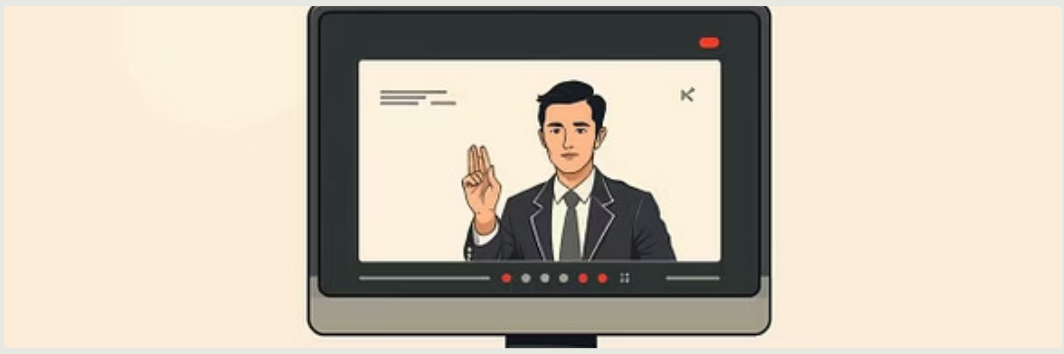
Voice phishing, where attackers use phone calls to impersonate legitimate entities and extract sensitive data.

TOOLS AND TECHNIQUES USED IN EMAIL PHISHING

Cybercriminals employ a variety of sophisticated tools and psychological techniques to make their phishing attempts convincing.







- **EMAIL SPOOFING**

  Faking the sender's email address to appear as a trusted source.

- **MALICIOUS LINKS**

  Hyperlinks embedded in emails that redirect users to fraudulent websites.

- **MALWARE ATTACHMENTS**

  Infected files (e.g., PDFs, Word documents) designed to install viruses or ransomware.

- **SOCIAL ENGINEERING**

  Psychological manipulation to trick people into performing actions or divulging confidential information.

- **DOMAIN SQUATTING**

  Registering domain names similar to legitimate ones to trick users.

HOW TO DETECT PHISHING MESSAGES

Identifying phishing attempts requires a keen eye and a critical approach. Look out for these red flags:

SUSPICIOUS SENDER

Check the sender's email address carefully; legitimate organisations rarely use generic email accounts.

GENERIC GREETINGS

Emails that address you as "Dear Customer" instead of your name can be a sign of a bulk phishing attempt.

URGENT OR THREATENING LANGUAGE

Phishing emails often create a sense of urgency, threatening account closure or legal action to rush you into acting.

POOR GRAMMAR AND SPELLING

Professional organisations typically proofread their communications. Mistakes are a clear warning sign.

UNUSUAL LINKS

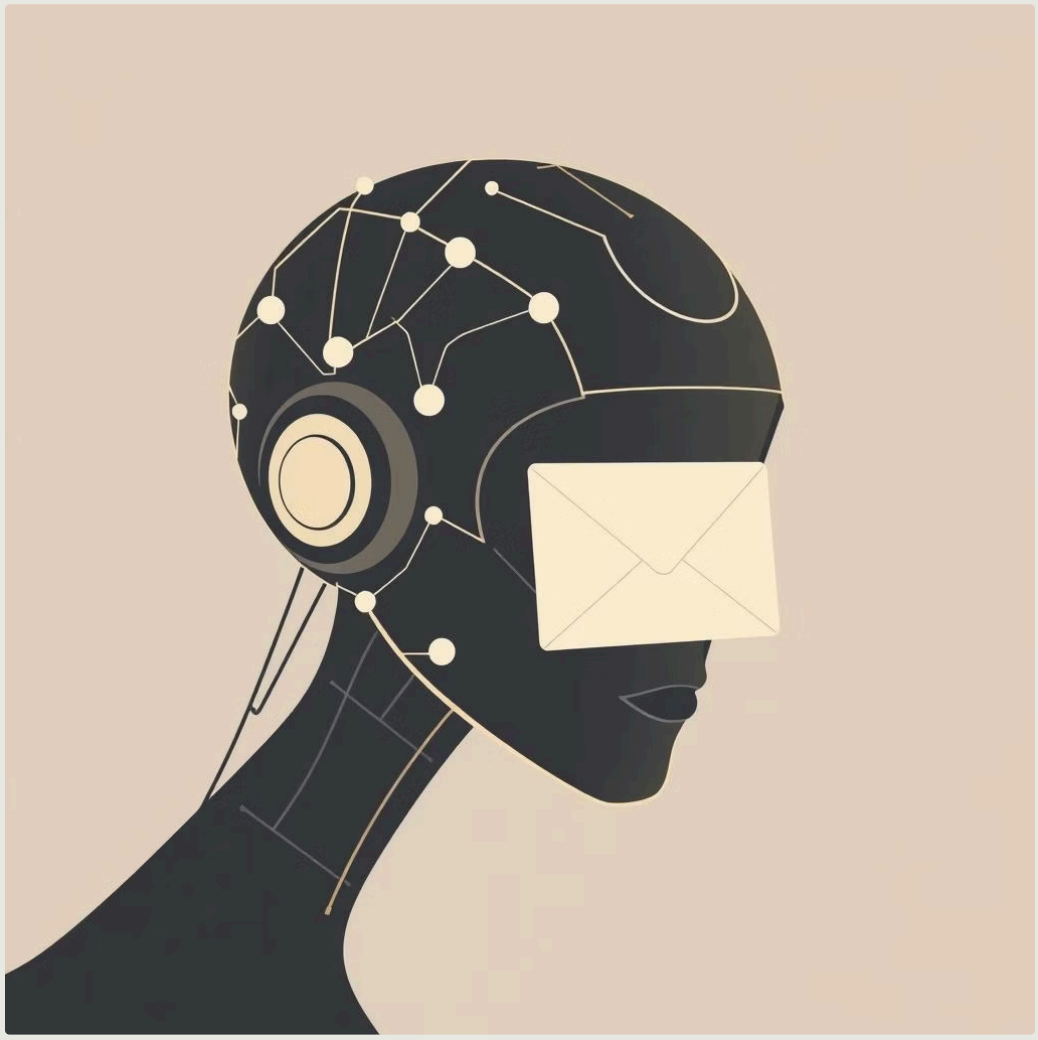
Hover over links to see the actual URL before clicking. If it looks suspicious or doesn't match the sender, don't click.

UNEXPECTED ATTACHMENTS

Never open attachments from unknown senders or if they seem out of context, as they may contain malware.

THE EVOLUTION OF PHISHING ATTACKS WITH AI

Artificial Intelligence is significantly changing the landscape of cyber threats, making phishing attacks more sophisticated and harder to detect.



1

ADVANCED SPOOFING

AI can generate more convincing fake email addresses and website designs, mirroring legitimate brands with higher accuracy.

2

HYPER-PERSONALISATION

AI analyses publicly available data to craft highly personalised spear phishing emails, making them extremely difficult to distinguish from genuine communications.

3

DYNAMIC CONTENT

AI-powered phishing emails can adapt their content in real-time based on user interaction, increasing their effectiveness.

4

VOICE & IMAGE SYNTHESIS

AI can create realistic deepfakes of voices and images, leading to more believable vishing and whaling attacks.

As AI tools become more accessible, the threat from AI-driven phishing will continue to grow, demanding even greater vigilance and advanced defence mechanisms.

FAMOUS PHISHING ATTACKS GLOBALLY

History is riddled with high-profile phishing incidents that highlight the severe impact these attacks can have.

1

2016: DNC EMAIL HACK

Spear phishing emails targeting Hillary Clinton's campaign manager led to a significant data breach, impacting the US presidential election.

2

2017: GOOGLE & FACEBOOK SCAM

A Lithuanian man successfully impersonated a Taiwanese manufacturer, tricking tech giants into wiring over $100 million in a sophisticated phishing scheme.

3

2018: MARRIOTT DATA BREACH

A phishing attack on a third-party vendor led to a massive data breach affecting 500 million Marriott customers, exposing personal information.

4

2020: TWITTER BITCOIN SCAM

High-profile Twitter accounts were compromised through a spear phishing attack, promoting a Bitcoin scam that defrauded users of thousands.

5

ONGOING: COVID-19 THEMED PHISHING

Cybercriminals extensively leveraged the pandemic, sending phishing emails disguised as health organisations or government agencies, leading to widespread fraud.

GENERAL ADVICE AND BEST PRACTICES AGAINST EMAIL PHISHING

RECOMMENDED ACTIONS	*ACTIONS TO AVOID*
• Verify the sender's email carefully	• Do not click on unknown or suspicious links
• Use multi-factor authentication	• Do not share passwords or verification codes via email
• Keep operating systems and applications up to date	• Do not trust urgent or threatening messages without verification
• Report suspicious emails to IT or security teams	• Do not rely on HTTPS as a sign of legitimacy
• Verify sensitive requests through a secondary communication channel before taking action	• Do not use the same password in all your accounts

ORGANIZATIONAL BEST PRACTICES

- Implement email filtering and and anti-phishing solutions
- Conduct regular phishing simulations
- Apply least-privilege access control
- Monitor and audit email activity continuously

THANK YOU FOR LISTENING

NOW WE WILL LEAVE YOU WITH THE SIMULATION TEAM TO SHOW YOU AN EXAMPLE OF HOW THIS ATTACKS HAPPEN