PHISHING ATTACKS: AWARENESS & PREVENTION

Aashly K Azeez

INTRODUCTION

Phishing attacks are a form of cyber threat where attackers trick individuals into providing sensitive information by pretending to be trustworthy entities. These attacks often occur through emails, fake websites, or social engineering tactics.

WHAT IS PHISHING?

Phishing is a fraudulent attempt to obtain sensitive information, such as usernames, passwords, and credit card details, by disguising as a trustworthy entity in electronic communications.

COMMON PHISHING TECHNIQUES

1. Email Phishing: Fake emails that appear to come from legitimate sources.
2. Spear Phishing: Targeted phishing attacks aimed at specific individuals or organizations.
3. Whaling: Phishing attacks targeting high-profile individuals, such as executives.
4. Smishing (SMS Phishing): Phishing attempts via text messages.

Vishing (Voice Phishing):

Scammers using phone calls to extract information.

Clone Phishing:

Duplicating legitimate emails with malicious links.

HOW TO IDENTIFY PHISHING EMAILS

1. Check the sender's email address for inconsistencies.
2. Look for grammatical errors and urgent requests.
3. Hover over links to check their actual destination before clicking.
4. Be cautious with unexpected attachments.
5. Verify with the sender through official channels if in doubt.

HOW TO AVOID PHISHING ATTACKS

- Enable Multi-Factor Authentication (MFA).
- Use strong and unique passwords.
- Keep software and security patches up to date.
- Educate yourself and your team on phishing threats.
- Never provide sensitive information through emails or phone calls.

REAL-WORLD EXAMPLES

- Google Docs Phishing Scam – Attackers sent fake Google Docs invites to steal credentials.
- PayPal Phishing Emails – Fake invoices prompting users to enter login details.
- COVID-19 Scams – Fraudulent emails posing as health organizations.

WHAT TO DO IF YOU SUSPECT PHISHING

1. Do not click on any links or download attachments.
2. Report the email to your IT department or email provider.
3. Mark the email as spam or phishing.
4. Change your passwords immediately if you've clicked on a phishing link.
5. Monitor your accounts for suspicious activity.

THANK YOU