PHISHING AWARENESS TRAINING

Protect Yourself from Cyber Threats

What is Phishing?

🛡️ Definition:

Phishing is a **cyber attack** where attackers impersonate trusted sources to trick individuals into **revealing sensitive information**, such as passwords, credit card details, or personal data.

🔍 How Does Phishing Work?

1. Attacker sends a fake email, message, or website link.
2. Victim clicks the malicious link or downloads an attachment.
3. User enters sensitive data or installs malware unknowingly.
4. Attacker gains access to confidential information or systems.

⚠️ Why is Phishing Dangerous?

1. Can lead to identity theft.
2. Can compromise financial data.
3. Can install malware or ransomware.

Types of Phishing Attacks

Phishing comes in different forms, targeting users through various channels. Here are the most common types:

1. Email Phishing

📩 Fake emails pretending to be from trusted sources (e.g., banks, social media).
🔹 Example: "Your account has been compromised! Click here to verify."

2. Spear Phishing

🎯 Targeted attacks aimed at specific individuals or organizations.
🔹 Example: A fake HR email sent to an employee requesting login credentials.

3.Vishing (Voice Phishing)

📞 Scammers use phone calls to extract confidential information.
🔹 Example: "This is your bank. Please confirm your PIN over the phone.“

4.Smishing (SMS Phishing)

📱 Attackers send fraudulent text messages with malicious links.
🔹 Example: "Your package delivery failed! Click here to reschedule."

Real-World Examples of Phishing Attacks

Case Study 1: Google & Facebook Scam ($100M Loss)

- A hacker impersonated a **legitimate hardware vendor** and sent fake invoices.
- Google & Facebook unknowingly **paid over $100 million** to the attacker.
- **Lesson:** Always verify payment requests and vendor emails before making transactions.

Case Study 2: The Twitter Bitcoin Scam (2020)

- Attackers **hacked Twitter employee accounts** via a phishing attack.
- They took control of accounts like **Elon Musk, Bill Gates, and Apple**.
- Tweets promised to **double Bitcoin deposits**, leading to major losses.
- **Lesson:** Never trust financial offers from unknown sources.

Case Study 3: The Target Data Breach (2013)

- Attackers **phished a third-party vendor** to gain access to Target's systems.
- **40 million** credit card details were stolen.
- **Lesson:** Even **indirect access points** can be vulnerable—implement strict cybersecurity policies.

How to Recognize Phishing Attempts?

Cybercriminals use various tactics to make phishing emails and websites look legitimate. Here's how to **spot the red flags**:

🚩 **Suspicious Sender Address:** Attackers use email addresses similar to legitimate ones

🚩 **Urgent or Threatening Language:** Phishing emails often create a sense of urgency to rush you into action.

🚩 **Unexpected Attachments or Links:** Malicious attachments may contain malware or ransomware.

🚩 **Poor Grammar & Spelling Mistakes:** Legitimate companies use professional communication.

🚩 **Too-Good-To-Be-True Offers:** Scammers lure victims with fake prizes, giveaways, or money rewards.

How to Protect Yourself from Phishing Attacks?

Knowing how to identify phishing is important, but taking proactive steps to protect yourself is even more critical.

🔄 **Keep Your Software & Browser Updated:**

Updates fix security vulnerabilities that hackers exploit.

🛑 **Don't Open Suspicious Attachments:**

Avoid opening unexpected attachments from unknown senders.

📛 **Never Share Sensitive Information Online:**

Legitimate organizations NEVER ask for passwords or OTPs via email or phone.

🛡️ **Enable Multi-Factor Authentication (MFA):**

Even if attackers steal your password, MFA adds an extra layer of security (e.g., OTPs, biometrics).

🔒 **Verify Emails & Links:**

Check sender email addresses carefully.

What to Do If You Fall for a Phishing Scam?

⚠️ **Disconnect from the Internet:**

If you clicked on a suspicious link or downloaded an attachment, disconnect your device from Wi-Fi or Ethernet to prevent further access.

🔐 **Change Your Passwords Immediately:**

If you entered your login credentials on a phishing site, change your password ASAP.

🛑 **Report the Attack:**

Report phishing emails to your IT team, email provider, or security department.

🔍 **Scan Your Device for Malware:**

Run a full antivirus scan to check for malware or keyloggers.

🛡️ **Monitor Your Accounts:**

Check for unauthorized transactions or login attempts.

Key Takeaways & Best Practices

🔍 **Think Before You Click:**

Always verify links and email senders before clicking.

🔐 **Use Strong Passwords & Enable MFA:**

Use unique, complex passwords for each account.

🚨 **Stay Alert for Phishing Red Flags:**

Be cautious of urgent requests, unexpected attachments, and grammatical errors.

🛡️ **Keep Software & Security Tools Updated:**

Regularly update browsers, operating systems, and antivirus software.

📢 **Report & Educate Others:**

Report phishing emails to your organization or email provider.

Conclusion & Resources

Cybercriminals are constantly evolving their phishing tactics. Staying informed and cautious is the key to protecting yourself and your organization.

🔑 **Key Reminders:**

Think before you click – always verify emails and links.
Use strong passwords & enable MFA for extra security.
Stay updated with the latest cybersecurity threats.
Report suspicious emails and educate others.

📩 **Helpful Resources:**

Google Safe Browsing: https://transparencyreport.google.com/safe-browsing
Microsoft Phishing Protection: https://www.microsoft.com/en-us/security/phishing
Report Phishing to Google: reportphishing@google.com
Report Phishing to Microsoft: phish@office365.microsoft.com

THANK YOU

AKSHAT JAKHMOLA