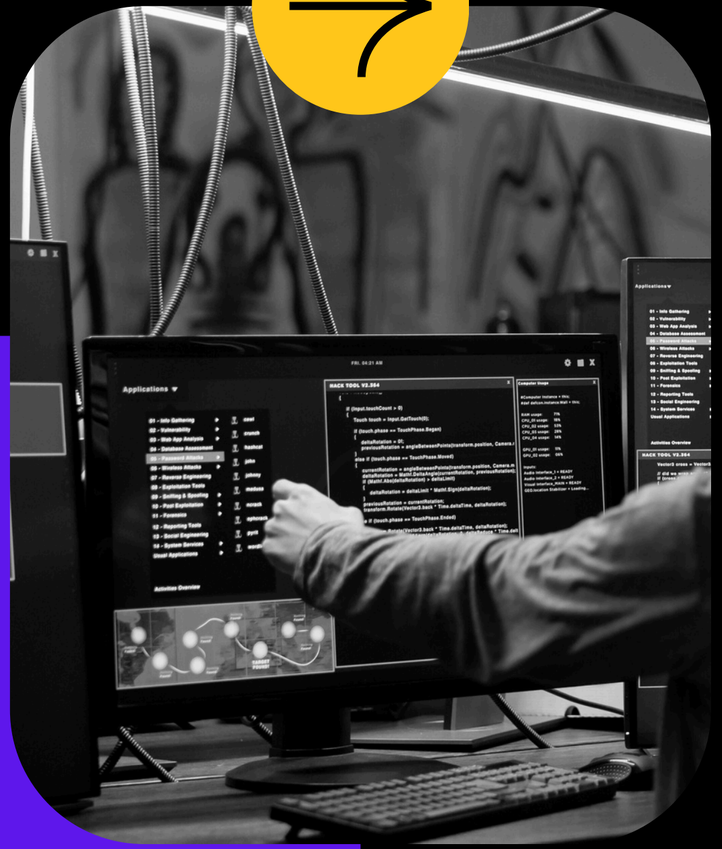
PHISHING AWARENESS TRAINING

Securing Your Digital World

What is phishing?

Phishing is a cyberattack that uses fraudulent communications to trick people into sharing sensitive information, downloading malware, or exposing themselves to other cybercrimes



Why is this important?

Phishing attacks are among the most common cybersecurity threats, leading to significant data breaches and financial losses.

Phishing remains a primary attack method, as most cyberattacks begin with a phishing email.
According to GreatHorn, 57% of organizations face phishing scams weekly or daily. Nearly 1.2% of all emails sent are malicious, accounting for 3.4 billion phishing emails daily.

Types of Phishing Attacks

Email Phishing: Fraudulent emails that appear to come from legitimate sources.

Spear Phishing: Targeted emails aimed at specific individuals or organizations, often using personal information.

Whaling: High-level phishing attacks directed at senior executives, often designed to steal sensitive corporate data.

Vishing (Voice Phishing): Phishing conducted via phone calls, where attackers impersonate trusted entities

Smishing (SMS Phishing): Phishing via text messages, often with malicious links or urgent requests.

Phishing mail example

Important: Your Password will expire in 1 day(s) Inbox x

MyUniversity 12:18 PM (50 minutes ago)

to me

Dear network user,

This email is meant to inform you that your MyUniversity network password will expire in 24 hours.
Please follow the link below to update your password
myuniversity.edu/renewal

Thank you
MyUniversity Network Security Staff

How to recognize phishing mails.

- Check the email domain for typos or strange names
- Phishing emails often use non-specific greetings (e.g., "Dear Customer").
- Messages that create a sense of urgency or fear (e.g., "Your account will be locked!
- Many phishing emails contain noticeable errors
- Be cautious of unexpected attachments and hover over links to check URLs before clicking.

Common Indicators of Phishing Websites

01 Look for misspelligs in URL or unfamiliar domains.

02 Ensure the site uses HTTPS; however, this alone does not guarantee safety.

03 Be wary of unexpected pop-ups asking for personal information.

04 If in doubt, go directly to the official website by typing the URL into your browser.

Social Engineering Tactics

Social Engineering refers to manipulation techniques used to trick individuals into divulging confidential information.

Common Techniques:

- Impersonation: Attackers may pose as trusted figures (e.g., IT personnel).
- Urgency: Messages that pressure you to act quickly, such as “Immediate action required!”.
- Familiarity: Attackers try to build rapport with victim in order to establish relationship, leading to an attack.

Best practices to stay safe.

- Always check the sender's email address before clicking links or downloading attachments.
- Enable Multi-Factor Authentication (MFA)
- Inform your IT department about any suspicious emails.
- Regularly update your operating system and security software to protect against vulnerabilities.

Conclusion

Though cybercriminals can’t be completely avoided, we stand a higher chance of securing ourselves from their schemes.

When take conscious steps towards safety.

THANK YOU!