Security Awareness 2024

Module 1: Email Security and Phishing

In today's digital landscape, email remains the primary vector for cyber attacks. Phishing emails are designed to deceive you into revealing sensitive information or installing malicious software.

Key Takeaway:

If you receive an email that looks suspicious, has unusual attachments, or requests urgent action/credentials: DO NOT CLICK ANYTHING. The best course of action is to report it immediately to the IT Security team.

Module 2: Password Management

Passwords are the first line of defense for your accounts. Weak passwords can be easily cracked by automated tools used by attackers.

Best Practices:

- Use long, complex passwords or passphrases.
- Do not reuse passwords across multiple accounts.
- Use a password manager to securely store your credentials.
- Update your password regularly, especially if you suspect a breach.

Our company policy requires all employees to update their system passwords regularly or whenever prompted by our security monitoring systems.

Module 3: Protecting Your Credentials

Your login credentials (username and password) are personal and tied to your identity. Sharing them puts both you and the entire organization at risk.

The Golden Rule:

NEVER share your password with anyone—not even your manager, IT support, or HR.

Legitimate support staff will never ask for your password. If someone asks for it, report the incident to the Security Operations Center (SOC) immediately.