

Basic Security Awareness Training

Introduction:

Upholding cybersecurity is essential in today's digital world to safeguard confidential data and provide a secure working environment. The goal of this training module is to provide you a basic understanding of security so you can properly identify and counter typical cyberthreats.

1. Phishing Awareness

Definition:

Phishing is a type of cyber attack in which scammers send fraudulent emails or messages in an attempt to trick you into disclosing private information like passwords, financial details or downloading malicious software

Why It's Important:

Phishing attacks are frequent and can result in financial loss, identity theft, and data breaches. It is possible to safeguard personal and corporate information by recognising and preventing phishing attempts.

Practical Advice:

- Be cautious of emails or messages asking for personal information, especially if they seem urgent or threatening.
- Check the sender's email address and hover over links to see their actual destination before clicking.
- Verify unexpected requests for sensitive information through a trusted communication channel, such as a phone call to the requester.
- Report any suspicious emails or messages to your IT department immediately.

2. Strong Password Practices

Definition:

Creating strong passwords is crucial to safeguarding sensitive data and online accounts. They are made to be difficult for other people to guess or crack.

Why It's Important:

Weak passwords can be easily guessed or cracked by cybercriminals, leading to unauthorized access to your accounts and potential data breaches.

Practical Advice:

- Create passwords that include a mix of letters (both uppercase and lowercase), numbers, and special characters.
- Avoid using easily guessed information, such as birthdays, names, or common words.
- Use a password manager to generate and securely store complex passwords. This helps manage unique passwords for different accounts.
- Change your passwords regularly and avoid reusing passwords across multiple sites.

3. Safe Browsing Habits

Definition:

Safe browsing involves practices that help protect you from online threats and ensure a secure browsing experience.

Why It's Important:

Unsafe browsing habits can expose you to malware, phishing scams, and other online dangers that may compromise your security and privacy.

Practical Advice:

- Only visit websites that you trust and verify their security by looking for “https” in the URL.

- Avoid downloading files from unknown or suspicious sources, as they may contain malware.
- Be cautious of pop-ups and advertisements that seem too good to be true. These can be attempts to lure you into malicious sites or downloads.
- Keep your browser and plugins updated to benefit from the latest security patches.

4. Device Security

Definition:

Device security involves measures to protect your computers, smartphones, and other devices from unauthorized access and malware.

Why It's Important:

Unsecured devices are vulnerable to attacks, which can lead to data breaches, loss of personal information, and potential damage to your device.

Practical Advice:

- Keep your operating system, software, and applications updated to protect against known vulnerabilities.
- Install and regularly update antivirus software to detect and remove malicious threats.
- Use a strong password or PIN to lock your device and ensure that it is not left unattended in public areas.
- Enable encryption on your device to protect data in case of loss or theft.

Conclusion:

Understanding and implementing these basic security measures can significantly improve your personal and workplace security. For additional help, please contact your IT department for further assistance. Remain alert and contribute to the security of our digital environment!