ONE PAGE SUMMARY

IT & Software › Cyber Security › Security Awareness

Introduction to Security Awareness

Stay Safe Online: Understanding Security Awareness

DEFINITION

> Security awareness is knowing how to protect yourself and your information online. It involves recognizing potential threats and taking steps to avoid them.

KEY CONCEPTS

Phishing

Phishing is a technique used by cybercriminals to trick individuals into providing sensitive information, often through deceptive emails.

Password Security

Using strong, unique passwords for different accounts helps prevent unauthorized access and data breaches.

Social Engineering

Social engineering manipulates people into divulging confidential information by exploiting human psychology.

Malware Awareness

Understanding malware types, such as viruses and ransomware, helps users recognize and avoid malicious software.

Secure Connections

Using secure connections, like HTTPS, ensures data is encrypted and protects against interception.

EXAMPLES

→ Receiving an email from a bank asking for personal information.

→ Using '123456' as a password for multiple accounts.

→ Clicking on a suspicious link in a social media post.

MEMORY TIPS

★ Remember 'PPSM' for Phishing, Passwords, Social Engineering, Malware.

★ Think of 'Strong Passwords' as a shield against attacks.

★ Visualize a lock for secure connections to remember HTTPS.

COMMON MISTAKES

✗ Ignoring suspicious emails or messages.

✗ Reusing passwords across multiple sites.

✗ Neglecting software updates and security patches.

QUICK RECAP

Security awareness is crucial for protecting personal information online. Key concepts include phishing, password security, and malware awareness. Always stay vigilant and practice safe online habits.