

ONE PAGE SUMMARY

IT & Software > Cyber Security > Security Awareness

Introduction to Security Awareness

Empower Yourself with Essential Security Awareness Skills

DEFINITION

Security awareness is understanding the risks and best practices to protect information. It helps individuals recognize threats and respond appropriately to safeguard data.

KEY CONCEPTS

Phishing

Phishing is a deceptive attempt to obtain sensitive information by pretending to be a trustworthy source.

Password Security

Using strong, unique passwords and changing them regularly helps protect accounts from unauthorized access.

Social Engineering

Social engineering manipulates individuals into divulging confidential information, often through psychological tricks.

Malware Awareness

Malware is malicious software designed to harm or exploit devices; awareness helps in avoiding infection.

Data Privacy

Data privacy involves protecting personal information from unauthorized access and ensuring it is used responsibly.

EXAMPLES

- Receiving an email asking for your password from an unknown sender.
- Using '123456' as a password for multiple accounts.
- Clicking on a suspicious link in a text message.

MEMORY TIPS

- ★ Remember 'PPSM' for Phishing, Passwords, Social Engineering, Malware.
- ★ Use the phrase 'Strong Passwords Protect' to recall the importance of password security.
- ★ Think of 'Data Privacy' as 'Protecting Your Digital Self'.

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 and organizational data. Key concepts include recognizing phishing attempts, maintaining password security, and understanding social engineering tactics. Stay informed and vigilant to mitigate risks.