Explain Methods to Secure Devices and Security Best Practices



Phil Chapman
Senior Instructor and Subject Matter Expert

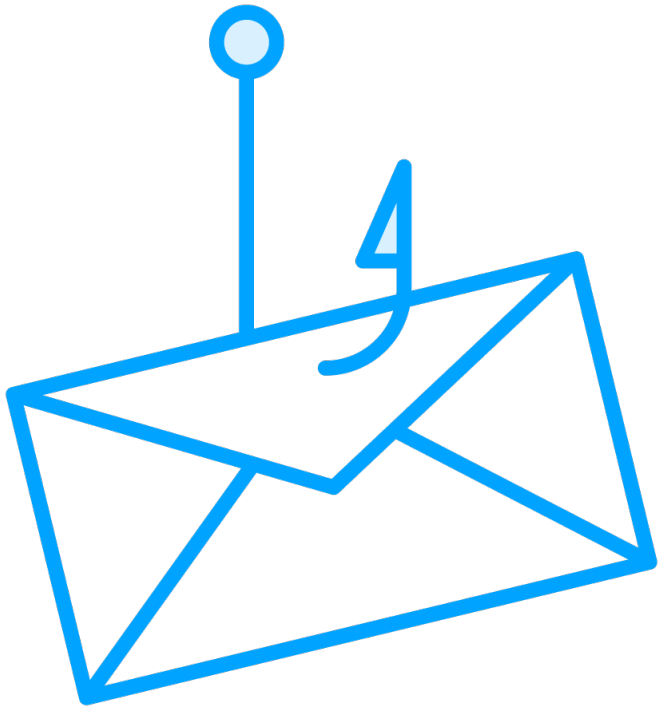
www.cyberphil.co.uk

Overview

Explain methods to secure devices and security best practices

- Understanding security awareness
- Securing devices
- Securing software
- Understanding safe browsing and privacy

Understanding Security Awareness



What is social engineering?

A broad term used to describe various nefarious activities used by malicious actors

The key aim of a social engineering attack is to trick an individual into giving away sensitive information or to perform an act which allows unauthorized access to a system or location

Social Engineering Tactics



Authority



Trust



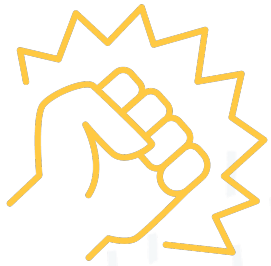
Urgency



Flattery

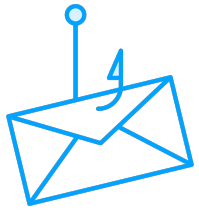


Greed



Threat

Social Engineering Techniques



Phishing



SMiShing



Spear phishing



Vishing

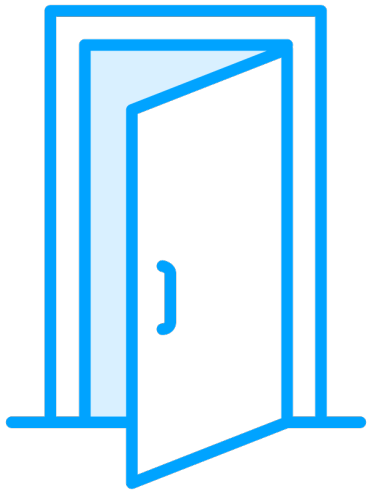


Whaling



QRishing

Physical Social Engineering Techniques



Tailgating / piggy-backing



Dumpster diving



Impersonation



Key aims of social engineering

- Solicit personal identifiable information
- Install malicious content
  - Remote access
  - Key logging
  - Compromised content

Mitigated by

- Procedural controls
  - User awareness and training
  - Security policies
- Technical controls
  - Spam/junk filters
- Physical controls
  - ID Badges

Up Next:

Securing Devices

Securing Devices



Gaining access

- Authentication and authorization
  - Multi-factor authentication
- Level of access (accounts)
  - Local administrator
  - Local user (standard user)
  - Network administrator and user
  - Computer account
- Centralized AAA server
  - Domain controller (Active Directory)



Device protection

- Antivirus and antimalware
- Firewall
- Built-in security features
  - Lock screens
  - Drive encryption
  - Protected system files

Patching and Maintenance



Devices should be well maintained



Updates and patches

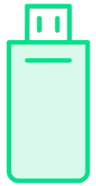


Upgrades

Physical Device Security



Cable locks (Kensington locks)



USB locks (disable ports)



User awareness and training



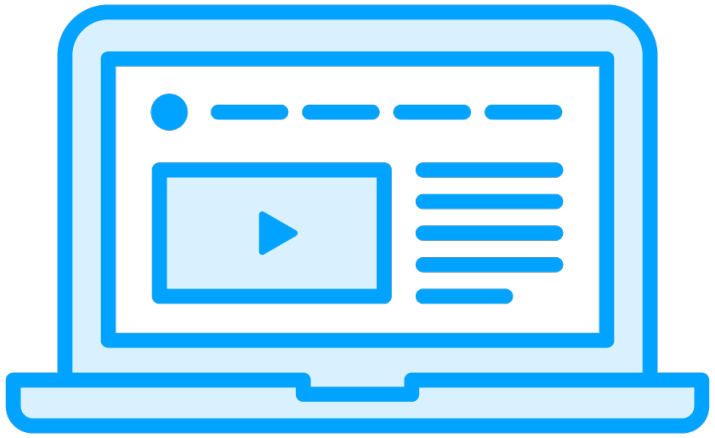
Licensing

- Open-source vs. proprietary
- Subscription vs. one-time
- Purchase vs. perpetual
- Product keys

Up Next:

Securing Software

Securing Software



Sources of software

- Operating systems
- Applications
- Research and validate legitimate sources
- Original equipment manufacturer (OEM) websites vs. third-party
- Application stores
  - Sideloading apps



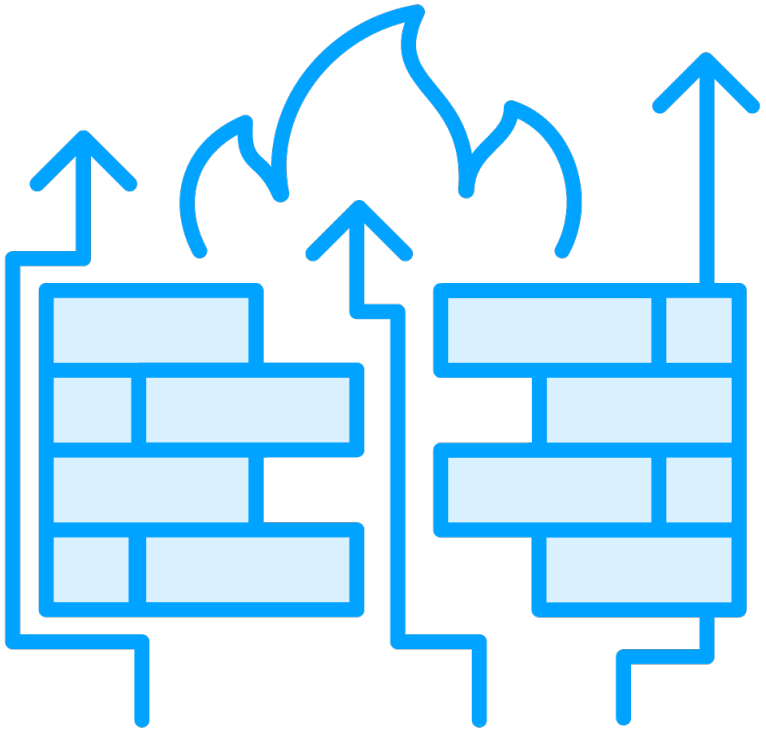
Software security best practices

- Remove unnecessary/unwanted applications and software
  - Potentially unwanted programs (PUP)
- Scan for malicious software (malware)
  - Virus
  - Worm
  - Trojan
- Do not use pirated software

Up Next:

Understanding Safe Browsing and Privacy

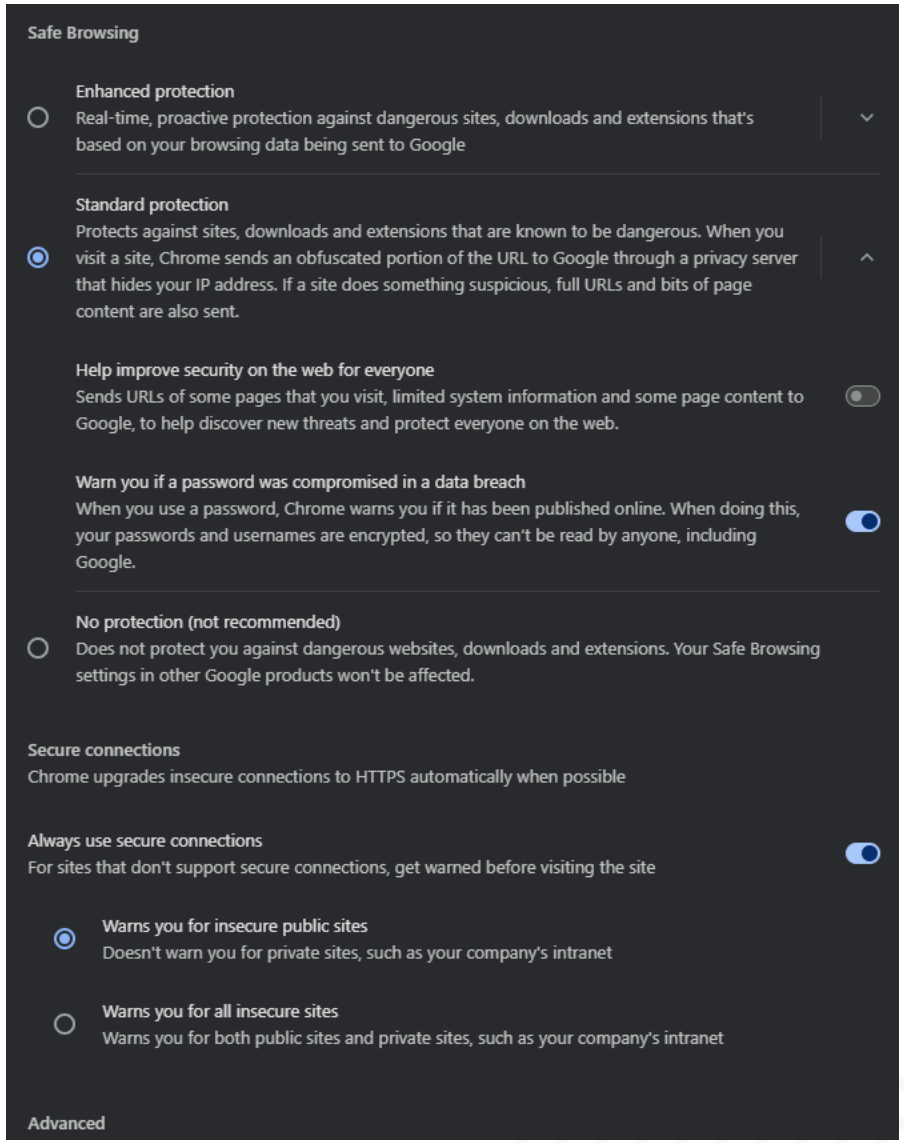
Understanding Safe Browsing and Privacy



Safe browsing

Firewalls and proxy services are used

- Content filters
- Allowed and disallowed sites
- Potential malicious connections
- Supported by policies



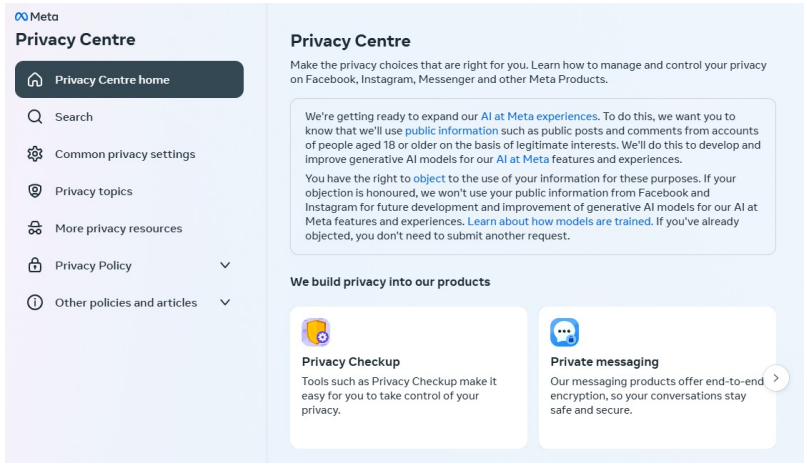
Browser security features are enabled

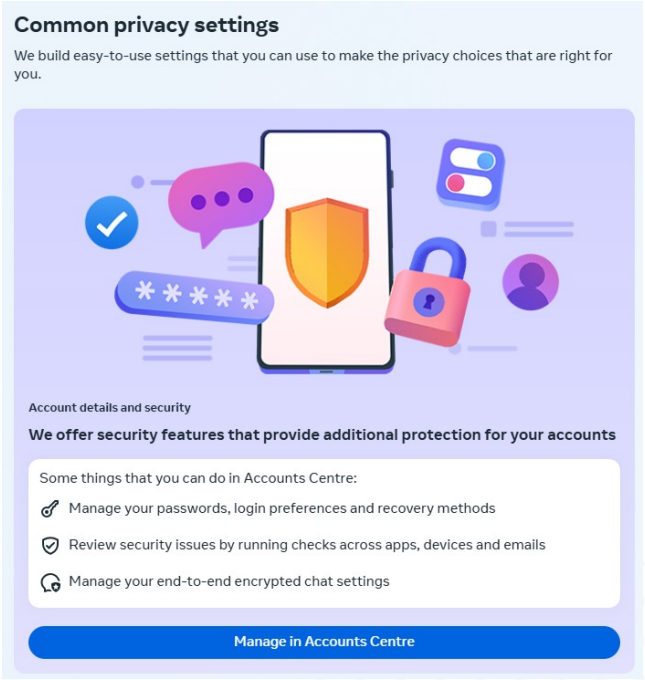
- Pop-up blocker
- Cookie handling
- Downloads control
- Secure connections



Certificate services

- Used to provide authentication and encrypted connections
- Establish a trust using a public key infrastructure (PKI)
  - Valid certificate
- HTTPS using Transport Layer Security (TLS)





Maintaining privacy

- Social networking sites
- Email
- File sharing
- Instant messaging
- Artificial intelligence (AI) tools
- Controlled by organizations
  - User awareness and training
  - Routinely updated

Up Next:

Explain Password Best Practices