WILEY

SYBEX
A Wiley Brand

CompTIA IT Fundamentals Study Guide (FC0-U61)

Chapter 10:

Security Best Practices

SYBEX
A Wiley Brand

Chapter 10: Security Best Practices

- Explain methods to secure devices and best practices
  - Securing devices (mobile/workstation)
    - Antivirus/anti-malware
    - Host firewall
    - Changing default passwords
    - Enabling passwords
    - Safe browsing practices
    - Patching/updates
  - Device use best practices
    - Software sources
      - Validating legitimate sources
      - Researching legitimate sources
      - OEM websites vs. third-party websites
    - Removal of unwanted software
    - Removal of unnecessary software
    - Removal of malicious software
- Summarize behavioral security concepts
  - Expectations of privacy when using
    - The Internet
      - Social networking sites
      - Email
      - File sharing
      - Instant messaging
    - Mobile applications
    - Desktop software
    - Business software
    - Corporate network
  - Written policies and procedures
  - Handling of confidential information
    - Passwords
    - Personal information
    - Customer information
    - Company confidential information

WILEY

Chapter 10: Security Best Practices (con't.)

- Explain password best practices
  - Password length
  - Password complexity
  - Password history
  - Password expiration
  - Password reuse across sites
  - Password managers
  - Password reset process
- Explain common uses of encryption
  - Plain text vs. cipher text
  - Data at rest
    - File level
    - Disk level
    - Mobile device
  - Data in transit
    - Email
    - HTTPS
    - VPN
    - Mobile application

Device Hardening

- Updating devices and using system passwords
- Protecting against network threats
- Removing and disabling software and services

Web Browsing Preparation and Maintenance

- Internet browser versions
- Plugins, toolbars, and extensions
- Autofill
- Browser security settings
- Cookies

Safe Internet Browsing

- Do not visit questionable sites
- Limit the use of personally identifiable information (PII)

Recognizing Secure Websites

- Secure sites use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to secure transmissions

- https:// vs. http://
- Lock icon
- Green address bar

Recognizing Suspicious Sites, Links, and Ads

- Look for signs of security
- Incorrect spelling
- Bad grammar
- Threats
- Too good to be true

Managing Users

- Account types
  - Administrators
  - Users
  - Guests
- Expectations and behaviors
  - Expectations of privacy
  - Handling confidential information

Managing Passwords

- Creating effective passwords
  - Long
  - Complex
  - Unusual
- Password changes

Using Data Encryption

- Encrypting data at rest
  - File level
  - Disk level
- Encrypting data in transit
  - Email
  - Internet – HTTPS
  - Virtual Private Network (VPN)
  - Mobile applications