MC
MONTGOMERY
COLLEGE

IT Fundamentals

CHAPTER 10:

SECURITY BEST PRACTICES

Device Hardening

01

Updating devices and using system passwords

02

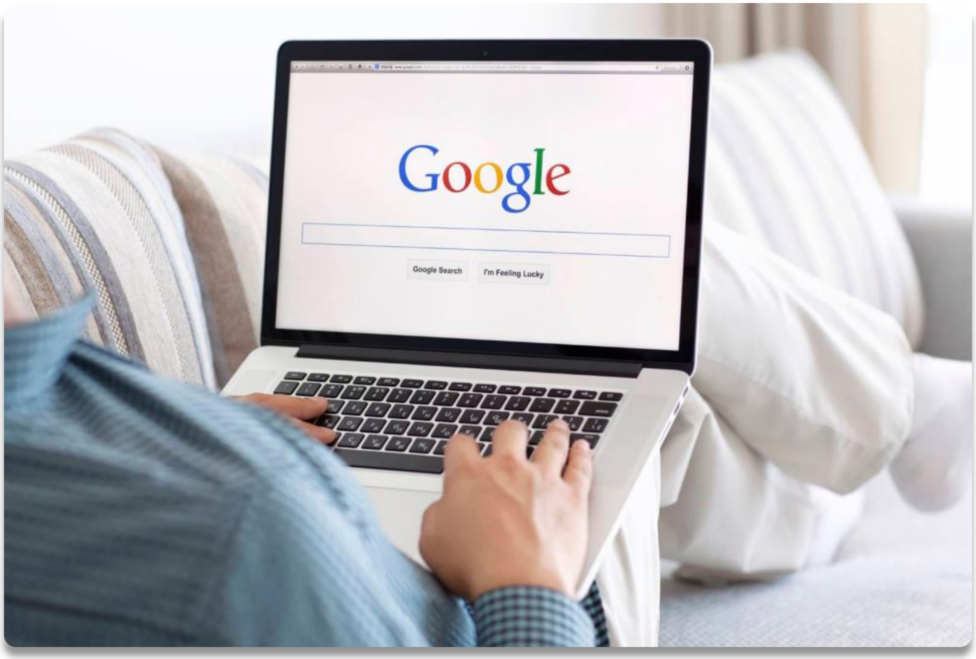
Protecting against network threats

03

Removing and disabling software and services

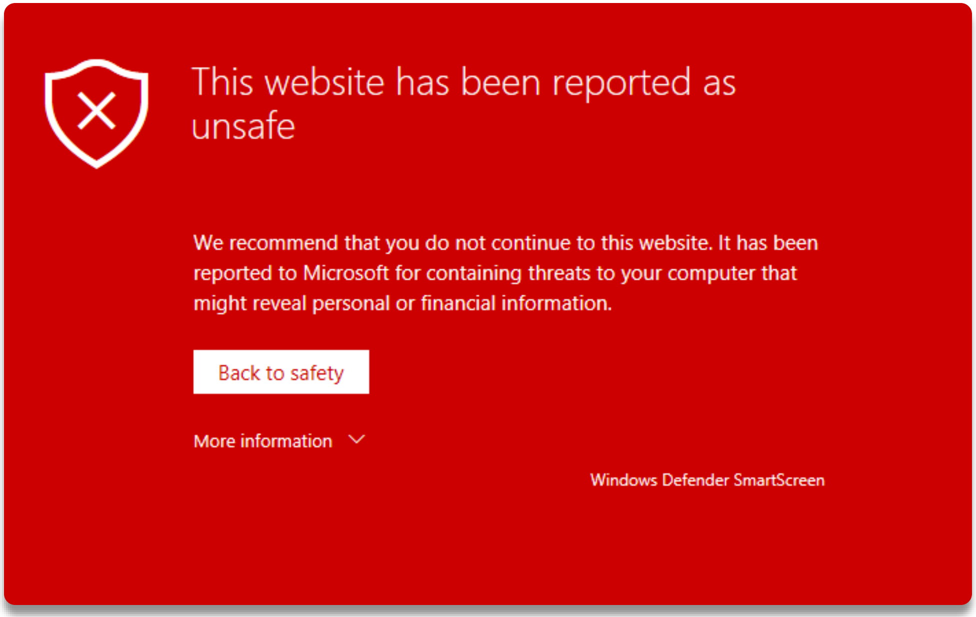
Web Browsing Preparation and Maintenance

- Internet browser v ersions
- 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)

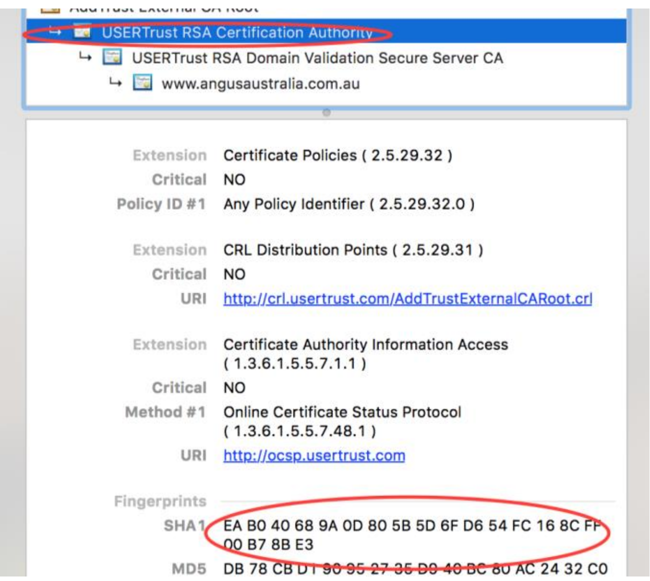


This website has been reported as unsafe

We recommend that you do not continue to this website. It has been reported to Microsoft for containing threats to your computer that might reveal personal or financial information.

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

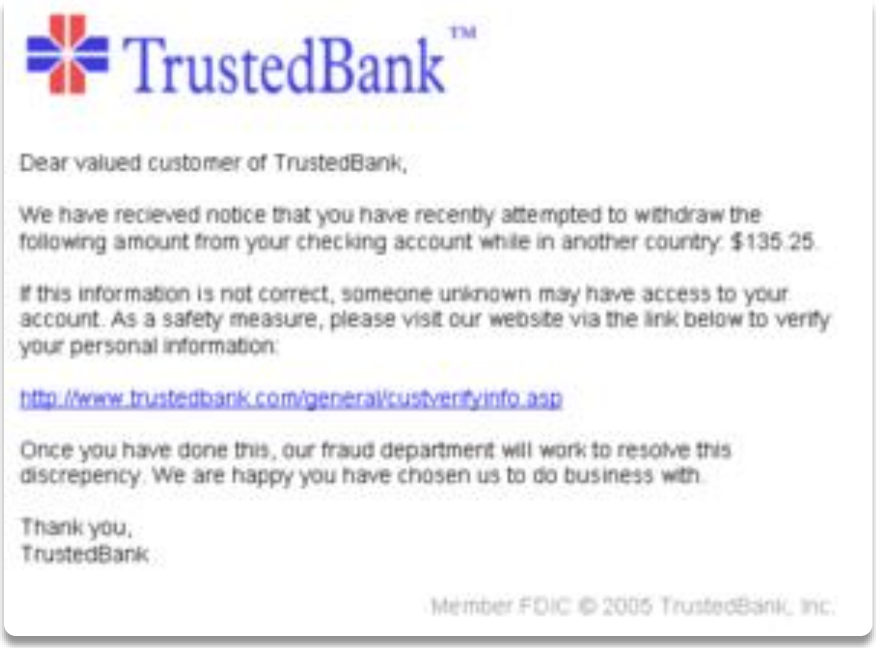


AddTrust External CA Root
↳ USERTrust RSA Certification Authority
↳ USERTrust RSA Domain Validation Secure Server CA
↳ www.angusaustralia.com.au

Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	Any Policy Identifier (2.5.29.32.0)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://crl.usertrust.com/AddTrustExternalCARoot.crl
Extension	Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical	NO
Method #1	Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
URI	http://ocsp.usertrust.com
Fingerprints	
SHA1	EA B0 40 68 9A 0D 80 5B 5D 6F D6 54 FC 16 8C FF 00 B7 8B E3
MD5	DB 78 CB D1 90 95 27 35 D0 40 BC 80 AC 24 32 C0

Recognizing Suspicious Sites, Links, and Ads

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



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Managing Users

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

Managing Passwords

- Creating effectiv e 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

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

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