Lesson 5.1.1 End User System Security
USER SECURITY AWARENESS

User Security Awareness

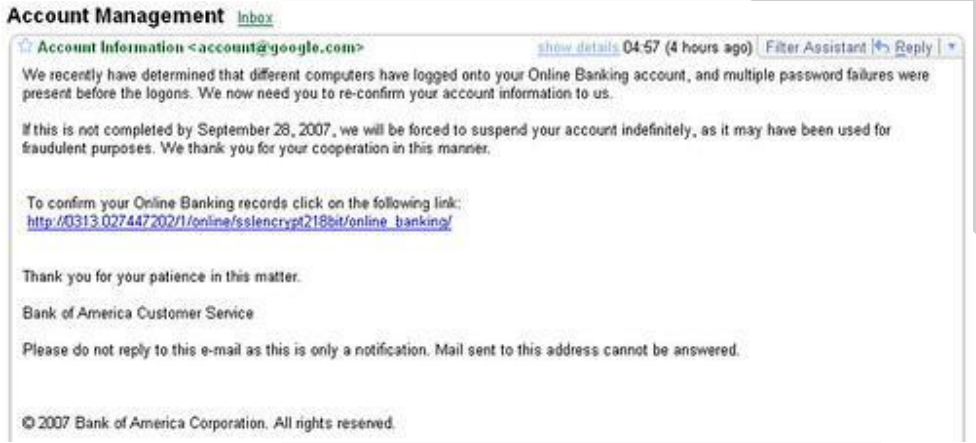
- In Cybersecurity, the weakest link is normally the end user.
- User education is incredibly important as end-users are the first line of defense against cybersecurity attacks
  - "The Human Factor"
- In this lesson we will explore end-user security principles, types of attacks, and how to prevent and recover from them

Unauthorized Access

- Administrative Access
  - A level of access above that of a normal user
  - Should be used sparingly
- Dumpster Diving
  - A technique used to retrieve information that could be used to carry out an attack on a computer network or learn personally identifiable information (PII).
    - Code
    - Passwords
    - Sticky Notes
- Shoulder Surfing
  - A technique used to obtain PII by looking over the victim's shoulder
    - Passwords
    - Personal Identification Numbers (PIN)

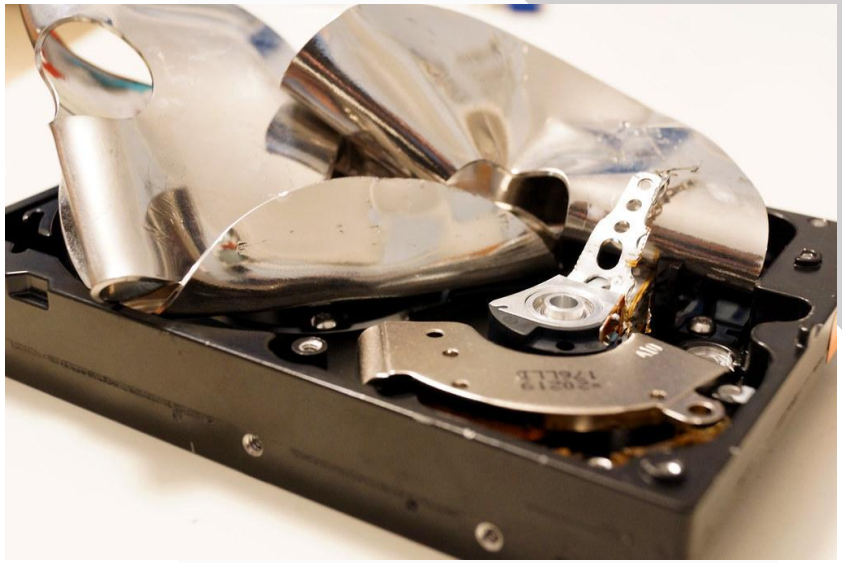
Social Engineering

- Telephone Scam
  - The use of telecommunications products or services to try to get money or personal identification to commit identity theft.
- Phishing Scam
  - A technique where a social engineer sends an email that appears to come from a fellow employee asking the recipient to download an attachment or click on a link.
    - Examples of scams
      - Imposter scams
      - Debt relief/credit repair scams
      - Business and investment scams
      - Charity Scams
      - Extended warranties
      - “Free” trials
      - Prizes/ lotteries
      - Time shares
      - Arrest Warrants

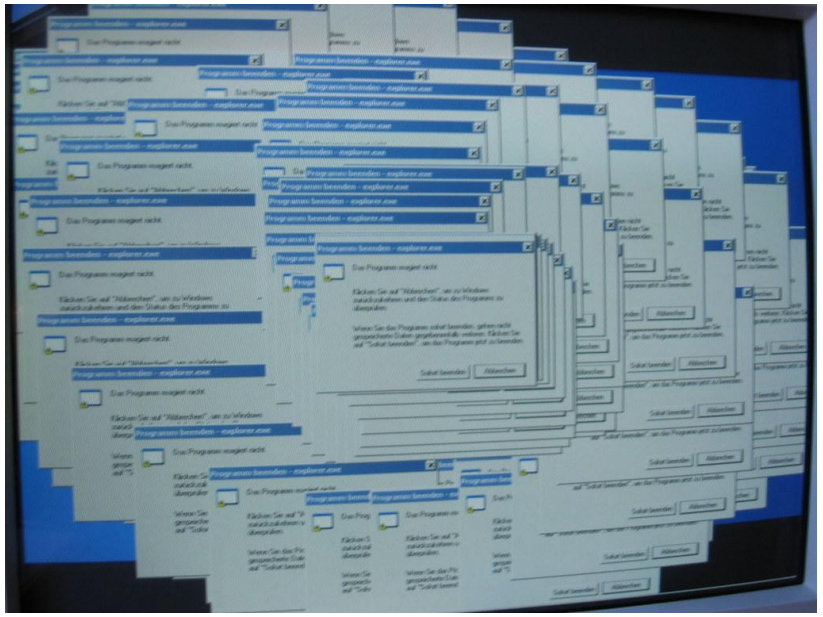


Data Destruction

- 48 percent of second-hand hard drives contained data leftover from the previous year
- 75 percent of those drives already had a deletion attempt made on them
- When you delete a file, drag it to the Recycle Bin, or reformat a drive the information is still there!
  - Pointers to files are deleted, but not the actual files themselves
  - The most effective way to delete data is to physically destroy the drive with a hard drive shredder
  - This ensures the data could never be recovered



Hardware Failure



- The term “crash” is often uttered in frustration by end users when a variety of issues occurs
- Failures related to hardware are especially frustrating as they seem to come on suddenly
- If a hard drive fails, all of the information contained on it may be at risk of being lost
  - Windows Operating System and license key
  - User documents, music, videos, pictures
  - Software Installations and licenses
  - Settings
- Repairing a component like a hard drive means the entire system basically needs to be recreated from scratch. To the end user, it's as though the computer was just taken out of the box for the first time and needs to be setup all over again.

Physical Theft

- Especially for mobile devices, it's very easy to leave a laptop or phone behind in a public place and they are also very easy to steal. Anyone who can access these devices has a wealth of information about it's users
- Best practices to lock down your personal computer
  - Minimum Password Length
    - The longer and more complex password, the better
  - Account Lockout Threshold
    - Disable the ability to continue trying to login after x number of bad attempts
  - Disable Windows Installer
    - Prevent any users from installing .msi packages via the registry
  - Printer Browsing
    - Disable the ability to look for network printers via the registry

Virus and Threat Protection Software

- Install Anti-malware software
  - Ensure Anti-malware/anti-virus updating definition files, and scanning actively
  - Ensure any new files that are downloaded are scanned before they are executed and checked against the known virus database (checksum)
- Careful clicking
  - User awareness goes a long way in keeping yourself safe online
  - Hover over links before you click them
  - Watch for typos like “Micros0ft.com”
  - Learn to recognize ads and spam
  - Exercise healthy suspicion
    - Recovery
      - Recognize and Quarantine virus
      - Search and Destroy threat
      - Remediate harm done

Summary – User Security Awareness

- User Security Awareness
  - Administrative Access
  - Dumpster Diving
  - Shoulder Surfing
  - Telephone Scam
  - Phishing Scam
  - Data Destruction
  - Hardware Failure
  - Physical Threat
  - Virus and Threat Protection Software