CSC 170 - Introduction to Computers and Their Applications

Lecture 10 – Digital Security

Encryption

- ***Encryption*** transforms a message or data file in such a way that its contents are hidden from unauthorized readers.
- An original message or file that has not yet been encrypted is referred to as ***plaintext*** or cleartext.
- An encrypted message or file is referred to as ***ciphertext.***

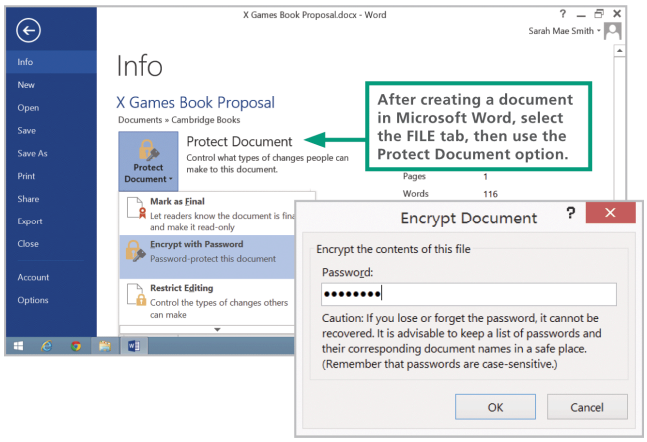
Encryption

- The process of converting plaintext into ciphertext is called **encryption**; the reverse process—converting ciphertext into plaintext—is called ***decryption.***

Encryption

- Data is encrypted by using a cryptographic algorithm and a key.
  - A **cryptographic algorithm** is a procedure for encryption or decryption.
  - A **cryptographic key** (usually just called a key) is a word, number, or phrase that must be known to encrypt or decrypt data.
- There are various encryption methods, and some are more secure than others; **AES** (Advanced Encryption Standard) is the encryption standard currently used worldwide.

Encryption



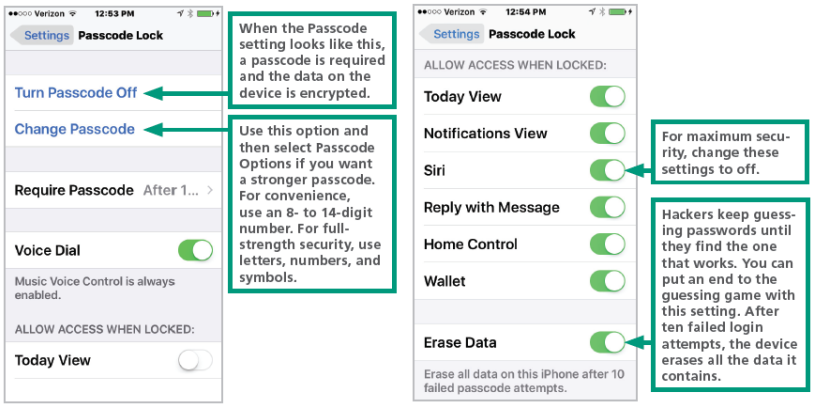
Authenication

- ***Authentication protocols***, such as passwords, PINs, and fingerprint scans and facial recognition are the first line of defense against data thieves and snoopers.
- iPhones and iPads should be configured to require a login password, called a passcode, each time the device is used; the standard iOS security setting establishes a four-digit numeric passcode, similar to a PIN (personal identification number).

Authenication

- Android devices have an overwhelming number of security settings.
  - Android devices do not automatically encrypt data stored on the device when a user activates the login password.
  - Configuring a password and activating encryption are two separate steps

Authenication



Authenication

- Windows offers several password options that can be configured using the Accounts utility, which is accessed from the Start menu or Control panel; Windows devices can be encrypted using Microsoft's BitLocker or third-party utilities.
- Macs offer several password settings, which are accessed from the Security & Privacy preferences; a feature called Automatic Login allows access to a device without a password.

Strong Passwords

- A ***strong password*** is difficult to hack.
- Conventional wisdom tells us that strong passwords are *at least eight characters* in length and include one or more *uppercase letters*, *numbers*, and *symbols*.

Strong Passwords

- A ***brute force attack*** uses password-cracking software to generate every possible combination of letters, numerals, and symbols. Because it exhausts all possible combinations to discover a password, it can run for days before a password is cracked.

Strong Passwords

- A ***dictionary attack*** helps hackers guess your password by stepping through a dictionary containing word lists in common languages such as English, Spanish, French, and German.

Strong Passwords

- Dictionary attacks are effective because many users choose passwords that are easy to remember and likely to be in the most commonly used list.

12345	000000	buster	coffee	eeyore
abc123	money	dragon	dave	fishing
password	carmen	jordan	falcon	football
p@sswOrd	mickey	michael	freedom	george
Pa55word	secret	michelle	gandalf	happy
passwordl	summer	mindy	green	iloveyou
!qaz2wsx	internet	patrick	helpme	jennifer
computer	service	123abc	linda	jonathan
123456	canada	andrew	magic	love

Strong Passwords

- Many of the clever schemes users devise to create passwords are obvious to hackers and the programmers who create password-cracking tools.

Strong Passwords

- Weak passwords include the following:
  - Words from a dictionary, including words that are in languages other than English
  - Doubled words such as passpass or computercomputer
  - Default passwords such as password, admin, system, and guest
  - Sequences of numbers formatted as dates or telephone numbers, such as 01/01/2000 and 888-5566

Strong Passwords

- Weak passwords include the following:
  - Words with a sequence of numbers at the end, such as Secret123 and Dolphins2018
  - Words with symbol or numeric mutations, such as p@ssw0rd and V01dem0rt
  - Any sequence that includes a user name, such as BillMurray12345
  - Any sequence that uses conventional capitalization, such as Book34 and Savannah912

Strong Passwords

- **Start with a phrase.** Base your high-security password on the first letters of a phrase that generates a password containing numbers and proper nouns.
  - Aim for a length of 8 to 12 characters because some sites limit password length.
  - Use uppercase letters somewhere other than at the beginning of the password.
  - Use numbers somewhere other than at the end of the password.
  - Some sites do not allow symbols, so you may not want to use them in a password that will be modified for use on many sites.

Strong Passwords

Here is an example of a phrase that produces a fairly secure password:

I went to Detroit Michigan when I was 23 years old IwtDMwiw23yo

- **Add the site name.** By inserting the name of the site, every password will be unique and you will be able to remember the site on which it is used, like this:

  I went to PayPal when I was 23 years old IwtPayPalwiw23yo

Strong Passwords

- **Make a low-security password.** A password achieves pretty good entropy when it is composed of four or more words. Create an everyday password using this method. Here is an example: **SpaBraidAmazonNuit**
- **Be careful what you write.** If you have to write down your passwords to remember them, keep them in a safe place that is not connected to your digital device. If your device is stolen, the passwords should not be located where they would also be stolen.

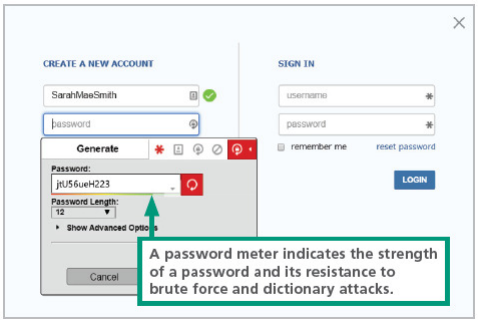
Strong Passwords

- **Use encryption.** If you want to store passwords on your device, make sure to encrypt the file in which they are stored.
- **Use a password manager.** If you feel more secure with a totally random and unique password for each of your logins, a password manager is an excellent option.

Password Managers

- The core function of a **password manager** (sometimes called a keychain) is to store user IDs with their corresponding passwords.
- Password managers may also include a **strength meter** that indicates password security—a feature that is useful if you create a custom password rather than using one generated by the password manager.

Password Managers



Malware Threats

- **Malware** refers to any computer program designed to surreptitiously enter a digital device
- The action carried out by malware code is referred to as a **malware exploit** or **payload**
- Common classifications of malware include:
  - Viruses
  - Worms
  - Trojans

Malware Threats

- Display irritating messages and pop-up ads Delete or modify your data
- Encrypt data and demand ransom for the encryption key
- Upload or download files
- Record keystrokes to steal passwords and credit card numbers
- Send messages containing malware and spam to everyone in an email address book or instant messaging buddy list
- Disable antivirus and firewall software

Malware Threats

- Block access to specific Web sites and redirect a browser to infected Web sites Cause response time slowdowns
- Allow hackers to remotely access data stored on a device
- Allow hackers to take remote control of a device and turn it into a zombie
- Link a device to others in a botnet that can send millions of spam emails or wage denial-of-service attacks against Web sites
- Cause network traffic jams

Computer Viruses

- A ***computer virus*** is a set of self-replicating program instructions that surreptitiously attaches itself to a legitimate executable file on a host device.
- Today, viruses are a mild threat; they do not spread rapidly, and they are easily filtered out by antivirus software.

Computer Viruses

- Viruses reveal the basic techniques that are still used to inject third-party code into legitimate data streams.
- ***Code injection*** is the process of modifying an executable file or data stream by adding additional commands.

Computer Worms

- A ***computer worm*** is a self-replicating, self-distributing program designed to carry out unauthorized activity on a victim's device.
- A ***mass-mailing worm*** spreads by sending itself to every address in the address book of an infected device.

Computer Worms

- An ***internet worm*** looks for vulnerabilities in operating systems, open communication ports, and JavaScripts on Web pages.
- A ***file-sharing worm*** copies itself into a shared folder under an innocuous name.

Antivirus Software

- ***Antivirus software*** is a type of utility software that looks for and eliminates viruses, trojans, worms, and other malware.
- A ***virus signature*** is a section of program code that contains a unique series of instructions known to be part of a malware exploit; they are discovered by security experts who examine the bit sequences contained in malware program code.

Antivirus Software

- Antivirus software can use techniques called ***heuristic analysis*** to detect malware by analyzing the characteristics and behavior of suspicious files.
- Heuristics may produce ***false positives*** that mistakenly identify a legitimate file as malware.

Antivirus Software

- **Repair.** Antivirus software can sometimes remove the malware code from infected files.
  - This strategy is beneficial for files containing important documents that have become infected.
  - Many of today's malware exploits are embedded in executable files and are difficult to remove.
  - When malware cannot be removed, the file should not be used.

Antivirus Software

- **Quarantine.** In the context of antivirus software, a **quarantined file** contains code that is suspected of being part of a virus.
  - For your protection, most antivirus software encrypts the file's contents and isolates it in a quarantine folder so it can't be inadvertently opened or accessed by a hacker.
- Quarantined files cannot be run, but they can be moved out of quarantine if they are later found to have been falsely identified as malware.

Antivirus Software

- **Delete.** Quarantined files should eventually be deleted.
  - Most antivirus software allows users to specify how long an infected file should remain in quarantine before it is deleted.
  - Most users rarely retrieve files from quarantine because it is risky to work with files that are suspected of harboring malicious code.
  - There is no need, therefore, to delay deletion for more than a few days.