Principles of Cybersecurity

Unit 3

Learning Objectives

- **Cybersecurity Principles:** Understand information security's goals and basic tools
- **Threats and Vulnerabilities:** Understand the differences between the two terms and learn preventative countermeasures.
- **Basic Cybersecurity Techniques:** Apply secure user processes to protect information/networks from unauthorized users.

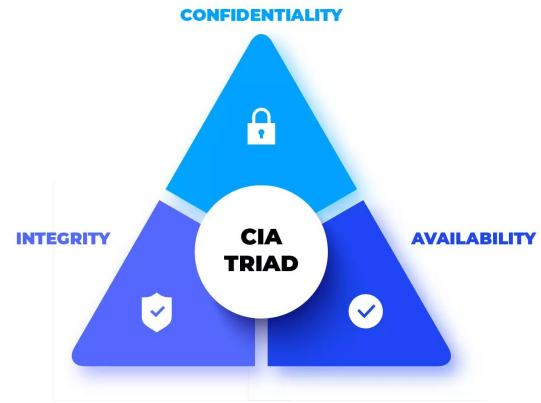
Cybersecurity Principles

Section 1

Goals of Information Security:

The CIA Triad:

- **Confidentiality**
  - Ensure only approved users have access to data
- **Integrity**
  - Data Integrity: assurance that information has not been tampered with or corrupted between the source and the end user
  - Source Integrity: assurance that the sender of the informatior is who it is supposed to be
- **Availability**
  - Ensuring data is accessible by approved users when needed

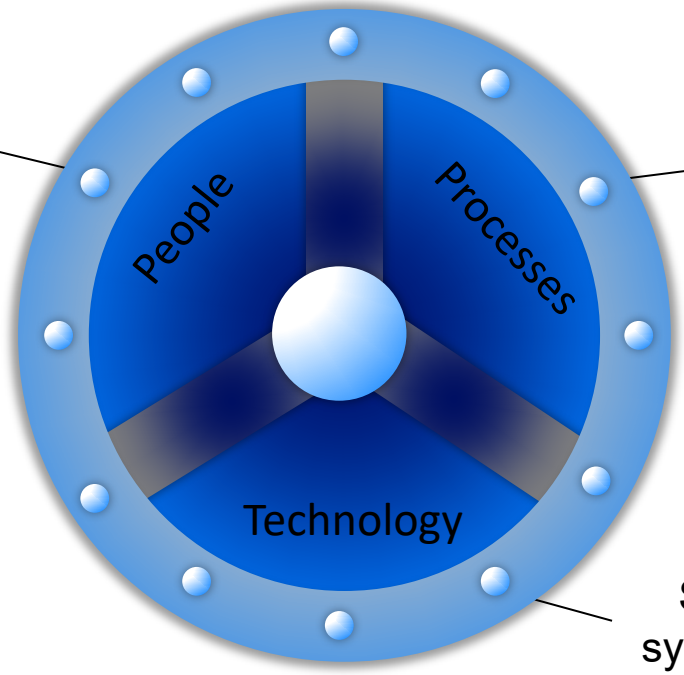


Source: http://www.techrepublic.com/blog/it-security/the-cia-triad/

People, Processes, and Technology

- Protecting the CIA Triad is about more than technology
- PPT is a holistic approach to securing an organization's information

Training for end users and resources to help IT professionals stay aware of emerging threats and industry trends



Policies, rules, and procedures for maintaining security

Security tools and system administration

Source: http://www.techrepublic.com/blog/it-security/the-cia-triad/

Tech Tools of the Trade

Measures to maintain Confidentiality, Integrity and Availability:

- Encryption
  - Passwords, encryption keys
- User access control
  - Which users have access to networks and what level of access they have
- File permissions
  - Customizable settings that only allow certain users to view and edit specific files
- Version control systems/backups
- Offsite data storage/backups
- Redundant architecture (hardware and software)

Threats and Vulnerabilities

Section 2

Important Cybersecurity Definitions

- **Threat:** An attacker or piece of malware that desires and/or is able to cause harm to a target
- **Vulnerability:** Flaw in an environment that an attacker can use to harm the target
- **Exploit:** The method by which an attacker can use a vulnerability
- **Risk:** The potential that a threat will exploit a vulnerability

Risks: Probability and Impact

The risk of a cybersecurity attack depends on two factors:

- **Probability**
  - How much motivation does an attacker have to try to exploit my system?
  - How securely have I protected my system?
- **Impact**
  - How damaging is a potential attack on my system?
  - Types of impact: Financial, Health and Safety, Personal, Service Interruption

		Impact				
		Trivial	Minor	Moderate	Major	Extreme
Probability	Rare	Low	Low	Low	Medium	Medium
	Unlikely	Low	Low	Medium	Medium	Medium
	Moderate	Low	Medium	Medium	Medium	High
	Likely	Medium	Medium	Medium	High	High
	Very likely	Medium	Medium	High	High	High

Risk Assessment: Target Breach

Case: Attackers breached Target's network through a heating and air conditioning (HVAC) company and point-of-sale systems to steal 40 million credit card numbers

Likelihood: Likely

- Attackers knew that Target has a massive network with many potential holes and that they could gain a wealth of information
- Network was not fully secured; HVAC company had open access to it

Impact: Major

- Loss of financial information could have major impact on Target's customers
- Breach was a huge embarrassment to Target and could have led to decrease in future sales

		Impact				
		Trivial	Minor	Moderate	Major	Extreme
Probability	Rare	Low	Low	Low	Medium	Medium
	Unlikely	Low	Low	Medium	Medium	Medium
	Moderate	Low	Medium	Medium	Medium	High
	Likely	Medium	Medium	Medium	High	High
	Very likely	Medium	Medium	High	High	High

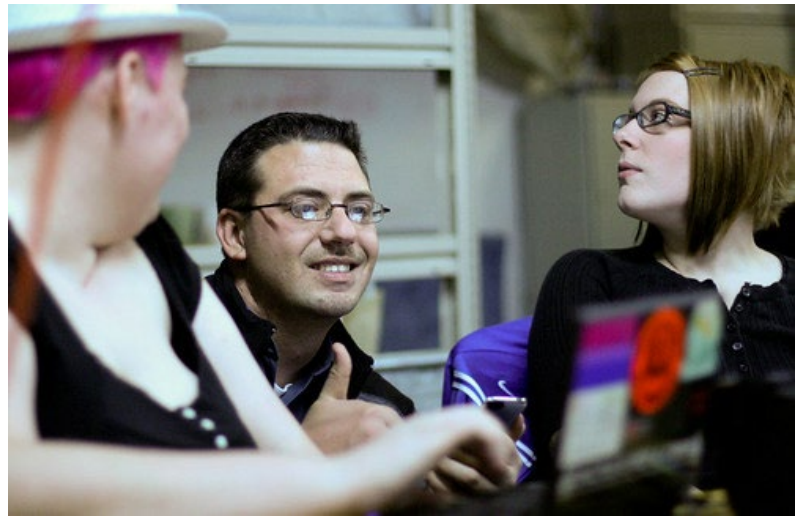
Physical Threats

Dumpster Diving:

Thieves sift through garbage for receipts with credit card information, medical forms with social security numbers, or other documents with PII

Shoulder Surfing:

By looking over your shoulder as you type, thieves can glean your passwords, account information, and other sensitive information



These are simple, but often overlooked threats.

Cyber Hygiene

Basic personal practices that keep computers and data safe:

- Lock your computer when in public areas
- Shield your keyboard when you type passwords
- Do not let strangers use your computer
- Keep sensitive information in secure places
- Use a secure network and reputable browser.
- Back up data regularly
- Be mindful of the information you share

Additional practices will be presented throughout the Unit.

Securing Mobile Devices

- Guard your devices- They can be easily stolen and lost
- Lock your device
  - Set a strong passcode or use biometrics to secure each device
- Use anti-malware and updates when available
- Avoid using open networks
- Customize security settings
  - Be sure to limit information collected from apps and visited sites.

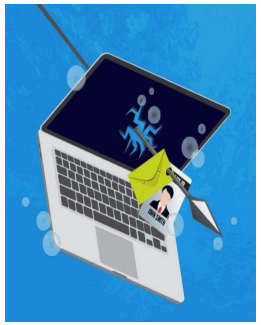
Online Threats: Social Engineering Methods

Social Engineering:

Manipulating people into sharing personal information

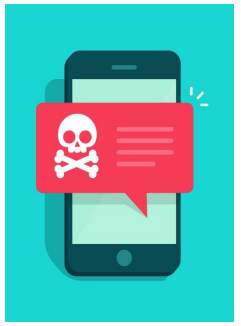
- Phishing: fraud attempts perpetrated by random attackers against a wide number of users
- Spear-phishing: fraud attempts targeted at specific people based on their membership or affiliation with a spoofed group
  - e.g. emails sent to Microsoft employees aiming to steal Microsoft secrets
- Vishing: Attempts to manipulate people into giving PII over the phone
- Smishing: Attempts to manipulate people into giving PII via text message

PHISHING



SPEAR-PHISHING

VISHING



SMISHING

How to Spot Phishing Emails

*Phishing attempts are rarely this obvious, but these are useful errors to look for

Spoofed email address

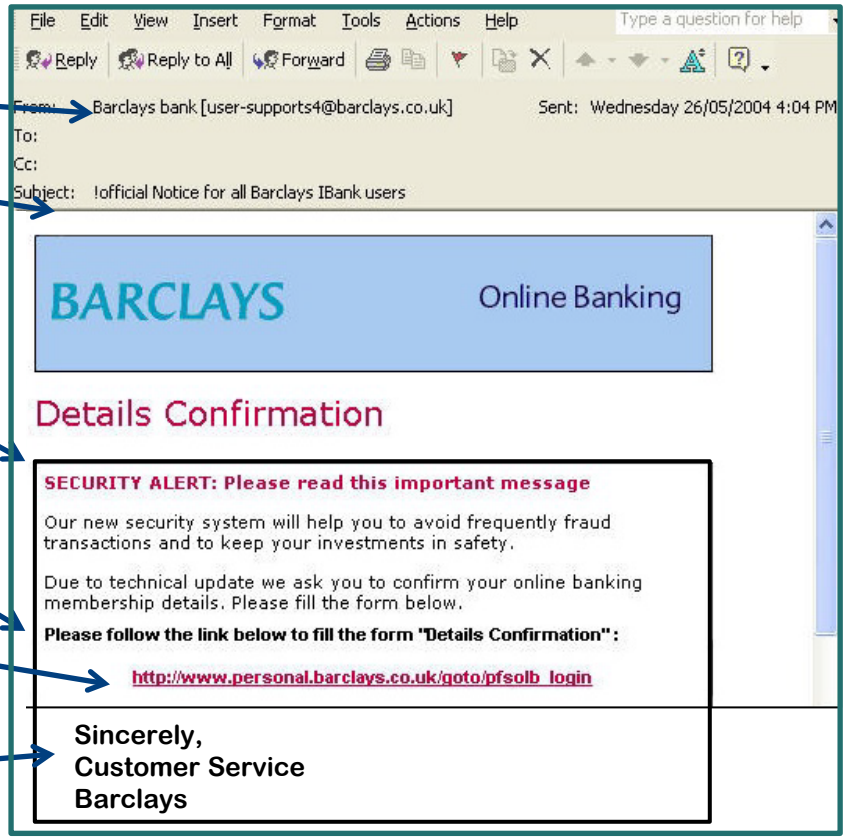
Spelling Errors/Typos

ALL CAPS

Asks for Personally Identifying Information

Executable attachment or link to a Website

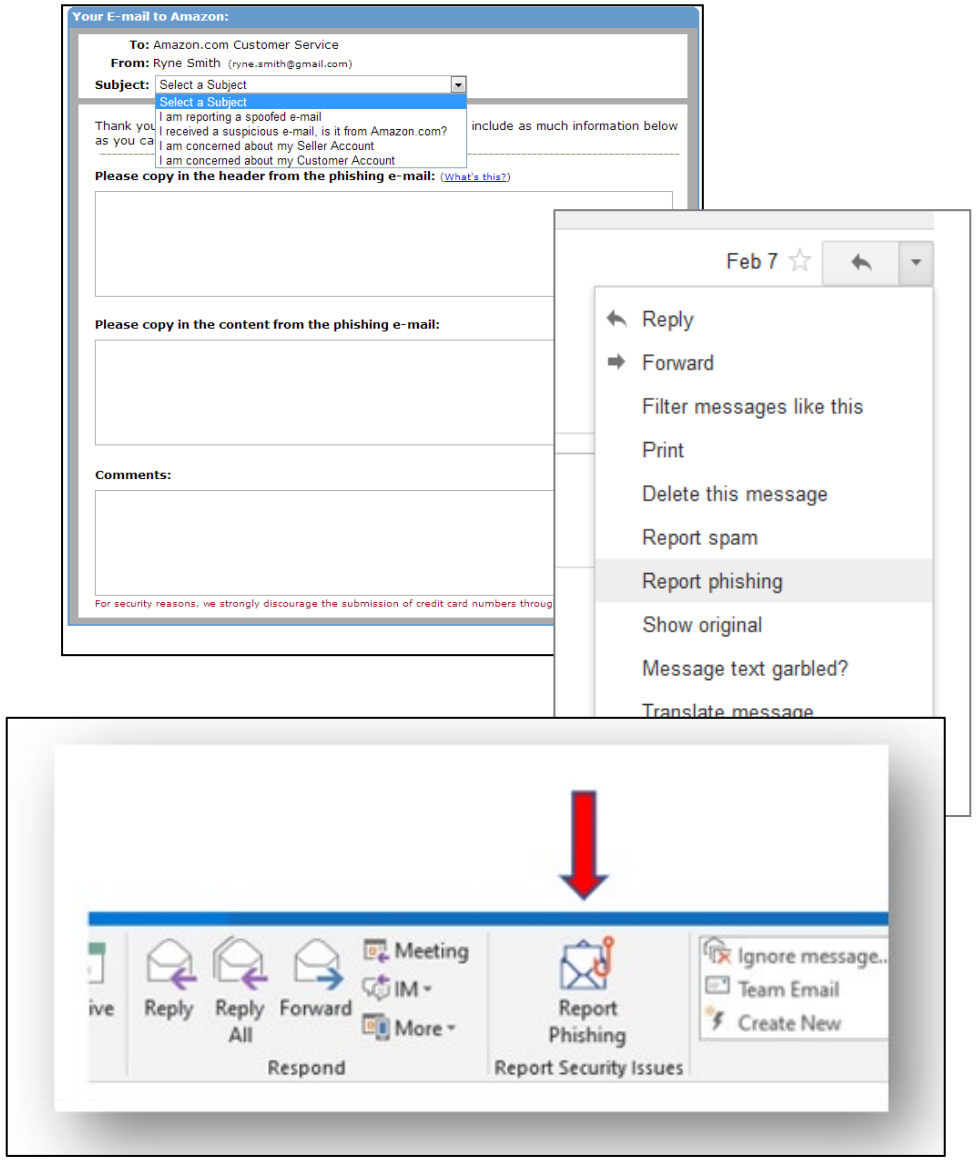
Signed by a department, not an individual



Source: www.Vanish.org

Reporting Email Scams

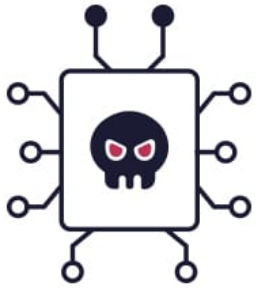
- Report phishing attempts so other people aren't victimized
- Go to the legitimate website of the spoofed organization (not through a link in the email)
- Follow the site's procedure for reporting
- Report the spoof to your email provider



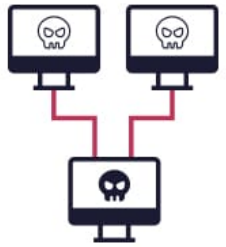
Malware

- Malicious Software = Malware
- Software designed and written to:
  - Steal information
  - Spy on users
  - Gain control of computers
- Categorized by
  - How it spreads
  - What it does

Malware: What is it?



VIRUS
Spreads between computers



WORM
Spreads between computers in one company or location

TROJAN
Sneaks malware onto your computer

SPYWARE
Steals your data

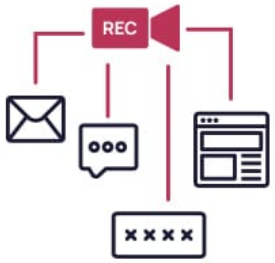
ADWARE
Spams you with ads

RANSOMWARE
Encrypts files and blackmails you

FILELESS MALWARE
Operates in your system's memory

ROOTKIT
Gives remote access to your device

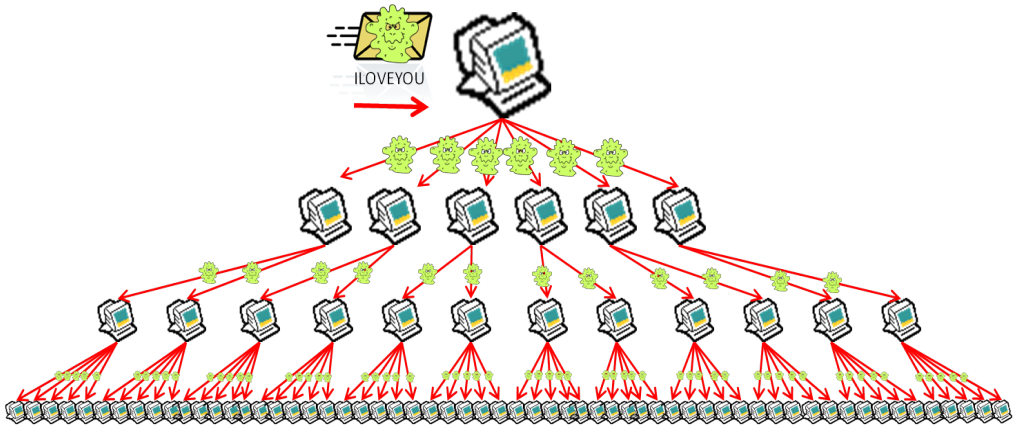
BOTNET
Turns your PC into a puppet



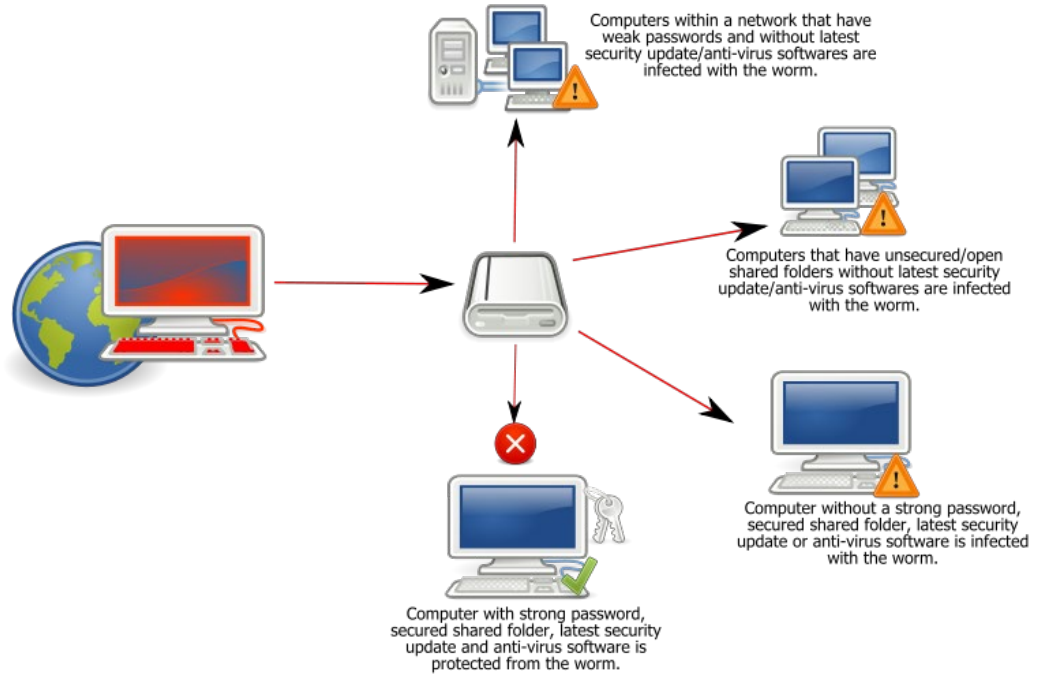
KEYLOGGER
Records user activity

Malware: Viruses/Worms

- **Viruses:** Can infect and spread, but need human assistance
  - People download infected email attachments, shared files, spoof links, etc.
  - Example: ILOVEYOU virus

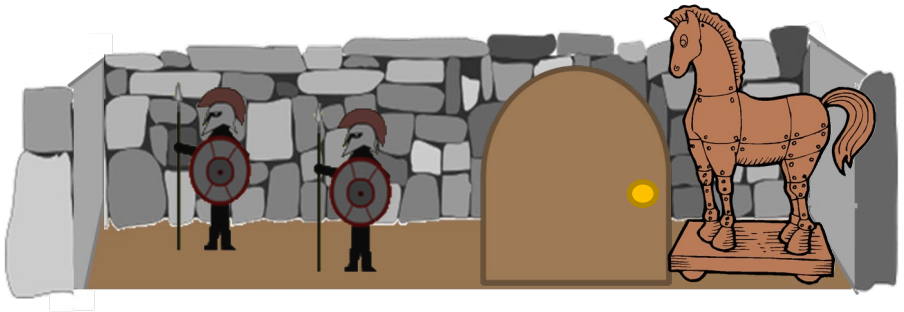


- **Worms:** Can infect and spread *without* human assistance
  - Example: Sasser worm



Malware: Trojan Horses

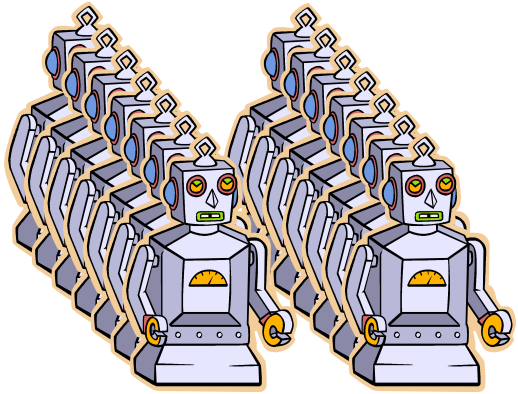
- **Trojan horse:** Program with a hidden malicious function
  - It looks like something you want
  - It does something you do not want
- Can cause computer crashes and be used by attackers to gain remote access to your system or steal information



Malware: Zombies and Botnets

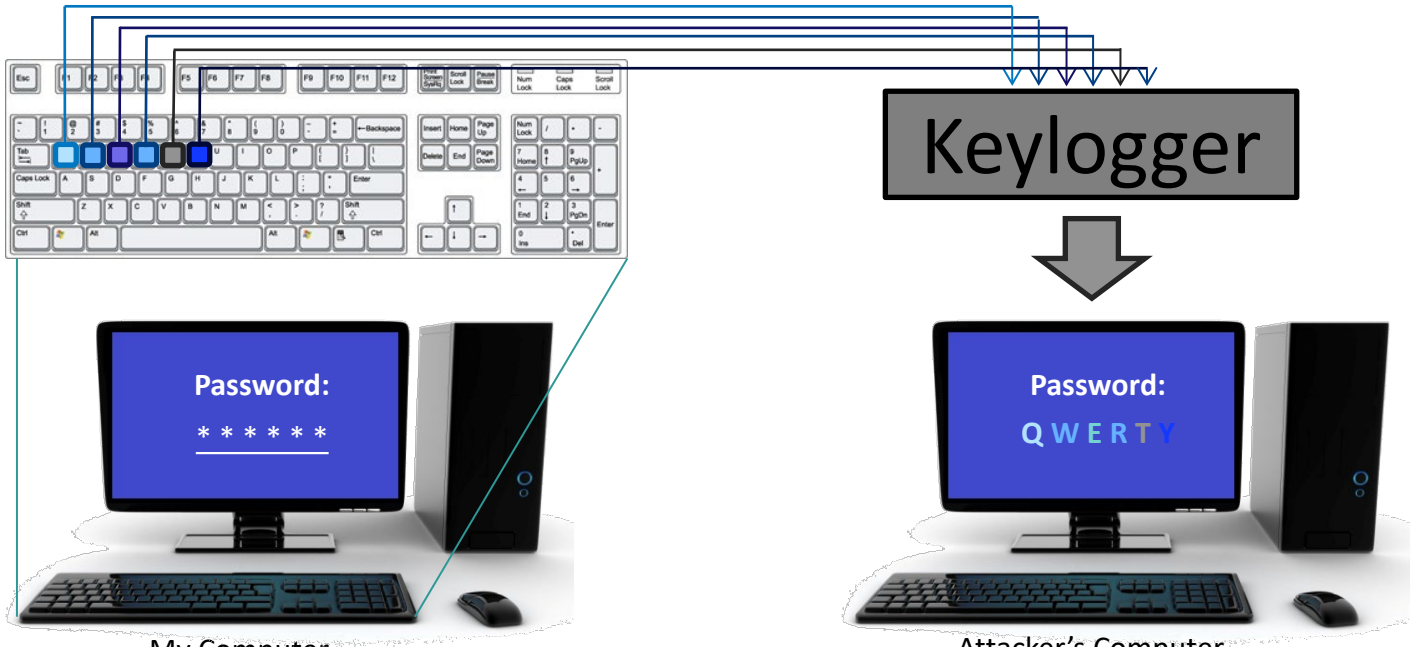
- **Zombies (a.k.a. bots):** compromised computers under the control of an attacker
  - Make it possible for someone else to control your computer from anywhere in the world

- **Botnet:** a collection of compromised computers (zombies) under the control of an attacker
  - Attackers pool the computing power of all of the zombie machines to launch huge spam attacks or to bring down websites through Distributed Denial of Service (DDoS) attacks
  - DDoS attacks direct massive amounts of communication requests and traffic to websites in attempt to overwhelm their servers



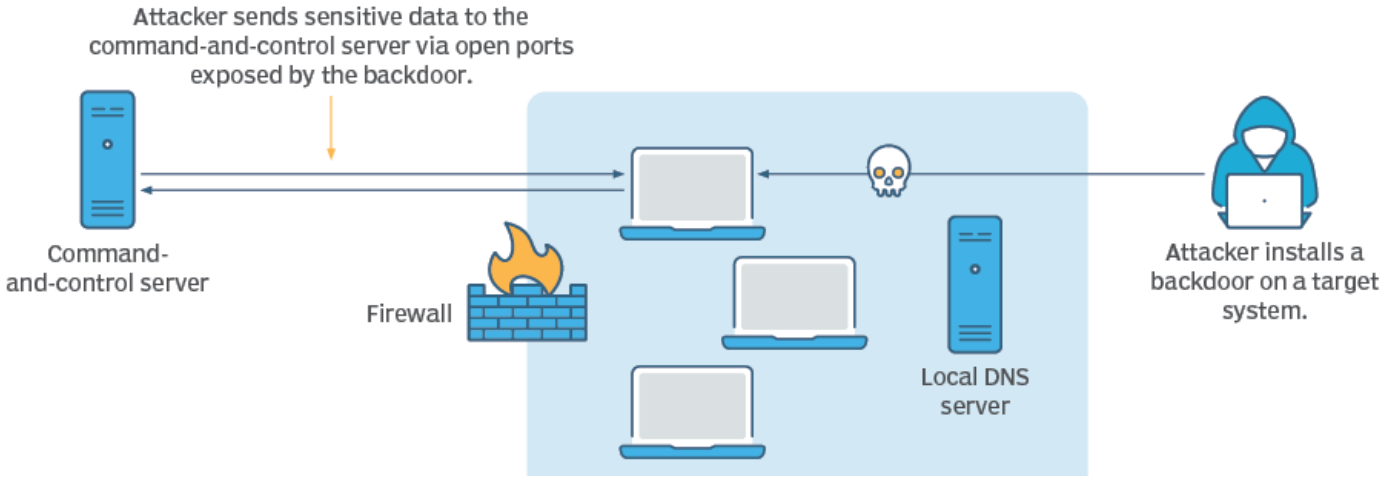
Malware: Keyloggers

- **Keylogger:** Tracks users' keystrokes, obtains passwords and other personal information
- Especially dangerous because they track everything a user does, not just what they do on an unprotected Internet browser



Malware: Backdoors

- **Backdoor:** An entry point into a program without all the normal, built-in security checks
- Programmers sometimes install backdoors when they develop programs so that they can manipulate a program's code more easily during troubleshooting and testing.
  - Sometimes they forget to close them
- Attackers use malware like viruses, worms, and Trojan Horses to install backdoors on the computers they infect



Malware: Logic/Time Bombs

- **Logic/time bomb:** Malware designed to lie dormant until a specific logical condition is met:
  - A particular person logs in
  - A specific date or time
  - A message is received

Malware: Spyware

- **Spyware:** Collects information about you, without your knowledge or consent
  - Keyloggers are a type of Spyware

Anti-malware Software

Scans files for matches in databases of known malware

Alerts you when a match is identified or when a suspect program attempts to run

Quarantines and removes infected files

Basic Cybersecurity Techniques

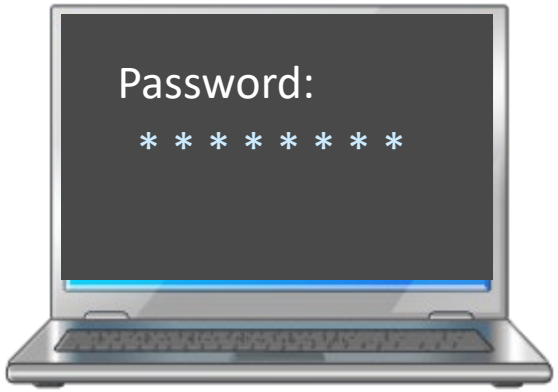
Section 3

Basic Cybersecurity Techniques

- **Identification:** Providing user identity to a system
- **Authentication:** Verifying the user identity
- **Authorization:** Determining whether a user is allowed to access certain resources
- **Accountability:** Holding users responsible for their actions on a system

Identification and Authentication

- Uses encryption to ensure that a user is who they say they are
- **Methods:**
  - Passwords
  - Physical “keys” (key chains, swipe cards)
  - Biometrics (fingerprints, retina scanning)



- **Threats:**
  - Brute force cracking
    - Test every possible combination of letters, numbers, and characters until the password is found
  - Dictionary cracking
    - Test words and combinations of words found in the dictionary or from a slightly shorter list of words known to be commonly used in passwords

Authorization

Uses tools to control access to a resource

- **Methods:**
  - File permissions
  - Account management
  - Sharing settings
- **Threats:**
  - Insider Threats: Disgruntled or inexperienced employees that have high-level access may cause intentional or accidental harm to a system.
  - Elevation of privilege: Attacker successfully enters the system as a low-level user but is able to attain a high-level access.

Additional information provided in later training units.

Authentication: Building Strong Passwords

- **Use at least 3 of the following:**
  - Numbers
  - Lower case letters
  - Upper case letters
  - Symbols (% # * & ! : { “ > |)
- Experts recommend changing passwords no more than 90 days
- Always use at least 10 characters
  - 12-16 characters is best!

Original Password: Pa123

New Password: Pa$Sw0rd!23

Did you know:

A brute force attack can run 4 billion calculations per second!

Authentication: Building Strong Passwords

- Passwords should be UNIQUE to you!
  - Do not use commonly known passwords.
  - Do not use the same password for each account
    - More than 42% of Americans use the same password for all their accounts.
- Use different passwords for each login by **adding a unique code to a base password that distinguishes between different accounts/sites**

Example:

[Base Password]	**[Site]**	
[Cyb3r!23$]	[Gmail]	**= Cyb3r!23$GMA**
[Cyb3r!23$]	[Facebook]	**= Cyb3r!23$FAC**

Authentication: Building Strong Passwords

- Use a **passphrase**
  - A passphrase is a password composed of a sentence or a combination of words.
- Add complex characters to make it more secure.
- Use a phrase that has some significance or meaning to you.

[Phrase]

CyberPatriot is fun!

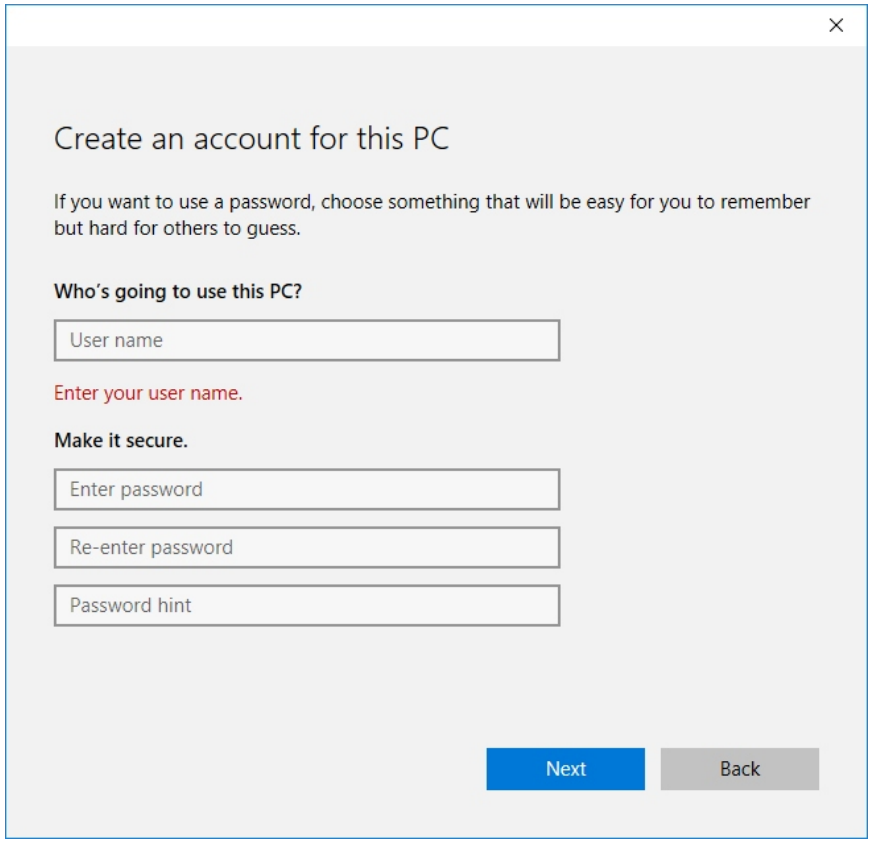
[Passphrase]

Cyb3rP@tr!0t_!s_Fun!

Passwords should be changed if there is any evidence of your account being compromised.

Authentication: Building Strong Passwords

- The longer you keep a password the longer attackers have to crack it.
- Changing your passwords regularly can help foil cracking attempts as they happen.
- It's best to change your passwords at least every few months.



Password Management System

Password Management Systems store your login information for all the websites you use and help you log into them automatically.

NordPass

bitwarden

DASHLANE

1Password

KEEPER
Cybersecurity Starts Here