AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

UNIT FOUR

Principles of Cybersecurity

Learning Objectives

- Participants will gain an understanding of basic cybersecurity concepts
  - The CIA triad
  - People, processes, and technologies that relate to CIA
- Participants will understand the differences between a threat and a vulnerability
  - Threats, Vulnerabilities, and Exploits
  - Risk and vulnerability severity
- Participants will become familiar with basic threat types and countermeasures
  - Overview of major threat categories
  - How attackers exploit infected computers
  - Best practices for threat prevention
- Participants will understand fundamental user security processes
  - Identification, Authentication, Authorization, and Accounting
  - Proper password configuration

SECTION ONE

The CIA Triad

The CIA Triad

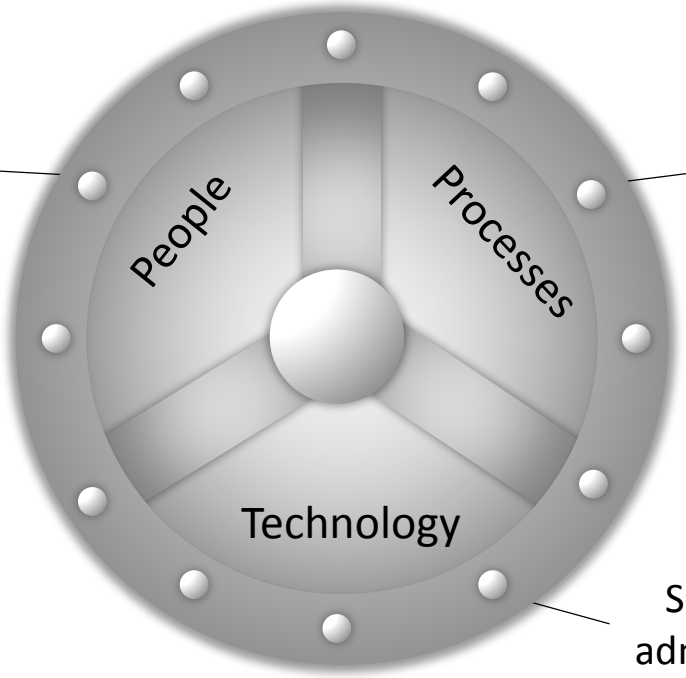
- 3 Goals of information security:
  - Maintain information **confidentiality**
    - Making sure only approved users have access to data
  - Maintain information **integrity**
    - Data Integrity: assurance that information has not been tampered with or corrupted between the source and the end user
    - Source Integrity: assurance that the sender of the information is who it is supposed to be
  - Maintain information **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 best practices

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

The CIA Triad: Tech Tools of the Trade

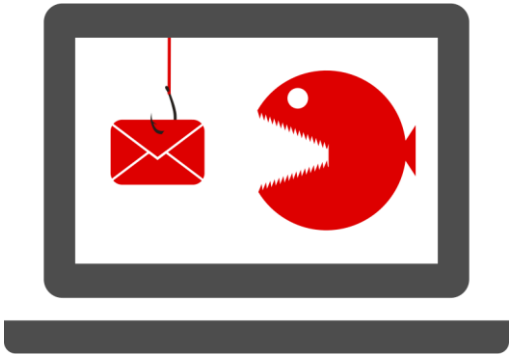
- Confidentiality
  - Encryption
    - Passwords, encryption keys
  - User access control
    - Controlling which users have access to networks and what level of access each user has
- Integrity
  - Encryption
  - User access control
  - File permissions
    - Customizable settings that only allow certain users to view and edit files
  - Version control systems/backups
- Availability
  - Offsite data storage/backups
  - Redundant architecture (hardware and software)

SECTION TWO

Threats and Vulnerabilities

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



Source: http://www.pen-tests.com/difference-between-threat-vulnerability-and-risk.html

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

Risk Matrix

Probability	Impact: Trivial	Minor	Moderate	Major	Extreme
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

Source: http://2.bp.blogspot.com/-xSHY5tsTvvY/Tzqi_kSorfI/AAAAAAAABDo/cR71Da7qCQY/s1600/ProbabilityAndImpactMatrix.png

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

SECTION THREE

Cyber Threats and Countermeasures

Physical Threats

DUMPSTER DIVING

SHOULDER SURFING

- 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
- 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

What are mobile devices?

Portable or handheld devices that have data or can connect to another device that has data




Securing Mobile Devices

Risk

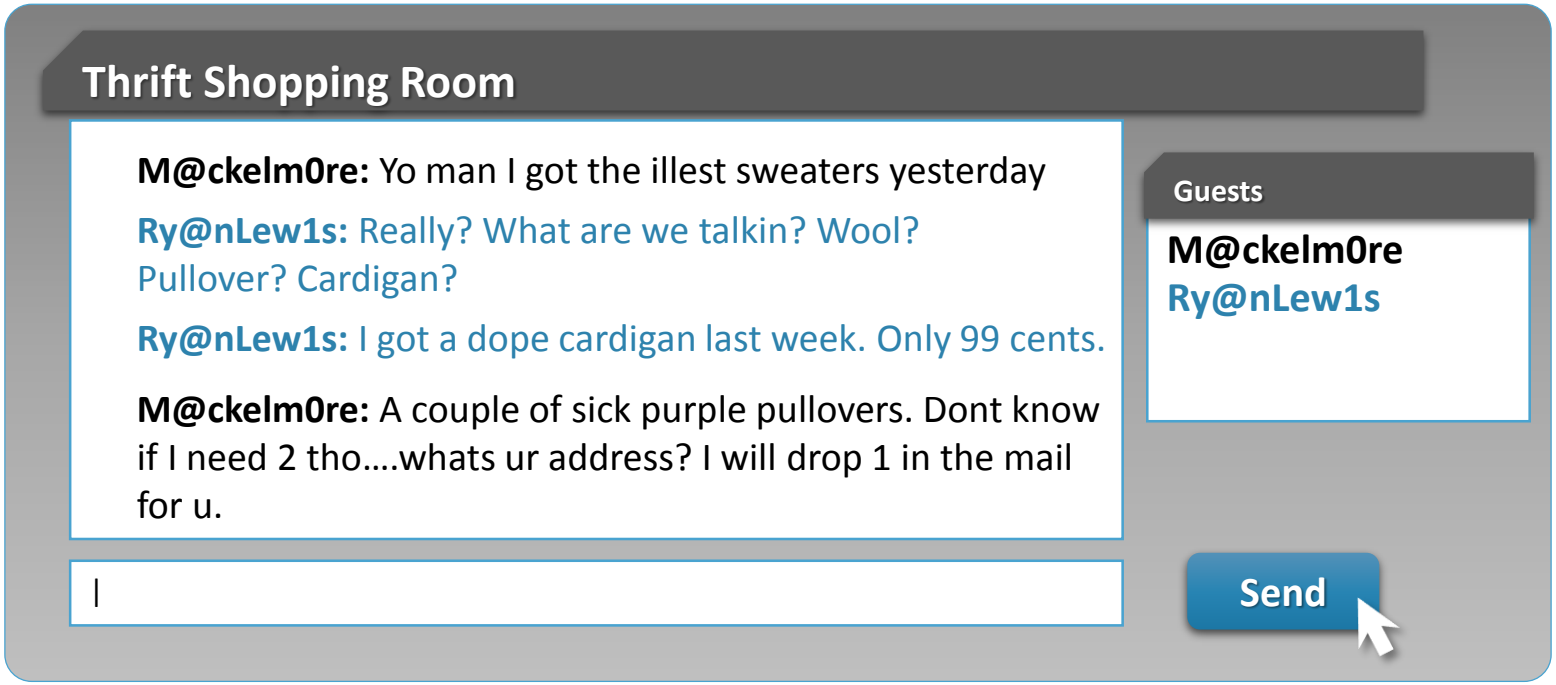
1. Easily stolen and lost
2. Often not encrypted
3. Targets of malware, tools for attackers
4. Can be compromised via wireless
5. Applications collect information

Fix

1. Guard your devices
2. Set a strong passcode
3. Use anti-malware and updates
4. Avoid using open networks
5. Customize security settings

Online Threats

SOCIAL ENGINEERING



- Social Engineering: Manipulating people into giving up personal information

Social Engineering Methods

- 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 the spoofed group
  - e.g. fraudulent emails sent to Microsoft employees aiming to steal Microsoft secrets
- Vishing: Attempts to manipulate people into giving up PII over the phone
- Smishing: Attempts to manipulate people into giving up PII by text message (SMS)

How to Spot Phishing Emails

Spoofed email address

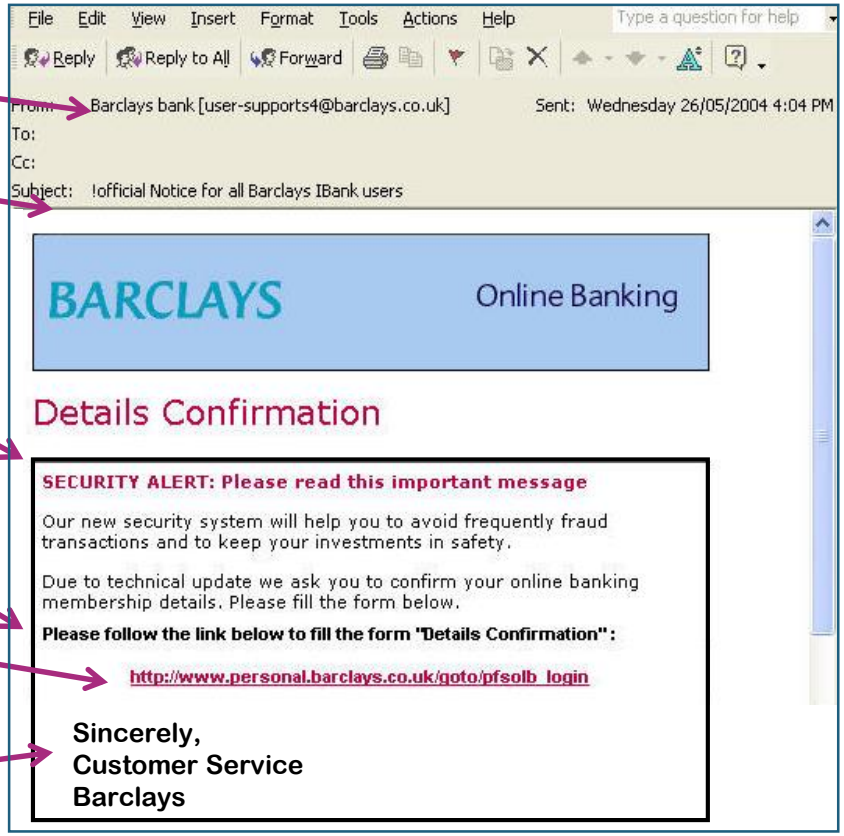
Spelling Errors/Typos

ALL CAPS

Asks for Personally Identifying Information

Executable attachment or link to a Website

Signed by a department, not an individual

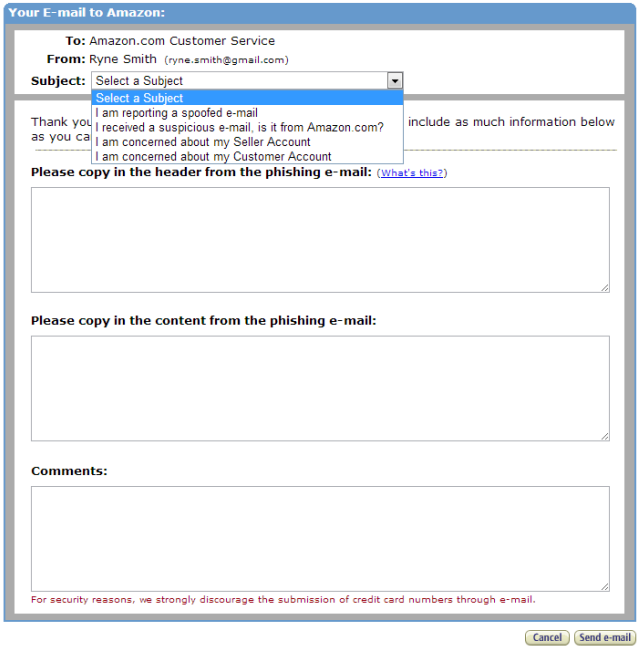


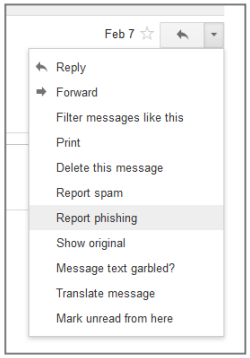
*Phishing attempts are rarely this obvious, but these are useful errors to look for

Source: www.Vanish.org

Reporting Email Scams

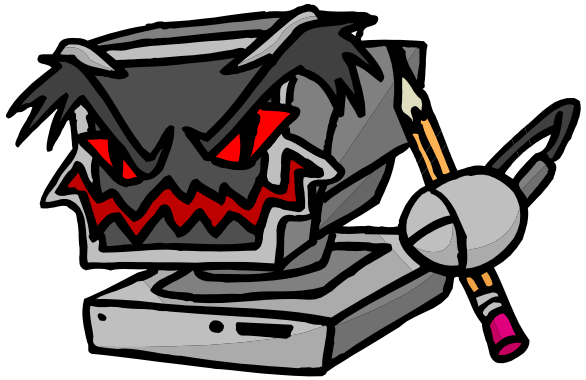
- Report phishing attempts so other people aren't victimized
- Go to the legitimate website of the spoofed organization (not through a link in the email)
- Follow the site's procedure for reporting
- Report the spoof to your email provider





Malware: What is it?

- 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

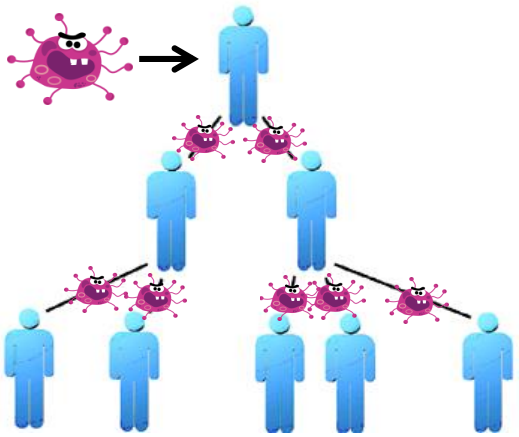


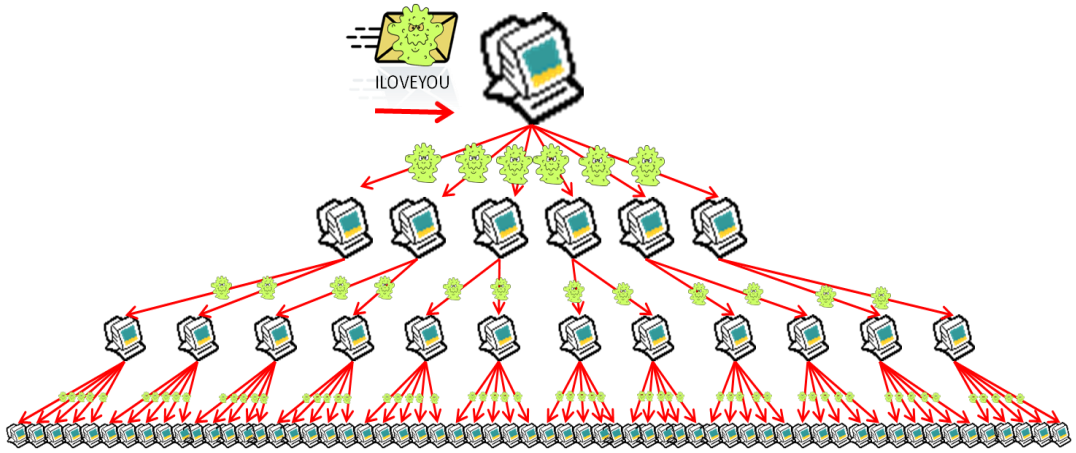
Malware: What is it?

- **V**iruses/Worms
- **T**rojan Horses
- **Z**ombies and Botnets
- **K**eyloggers
- **B**ackdoors
- **L**ogic/Time Bombs
- **S**pyware

Malware: Viruses/Worms

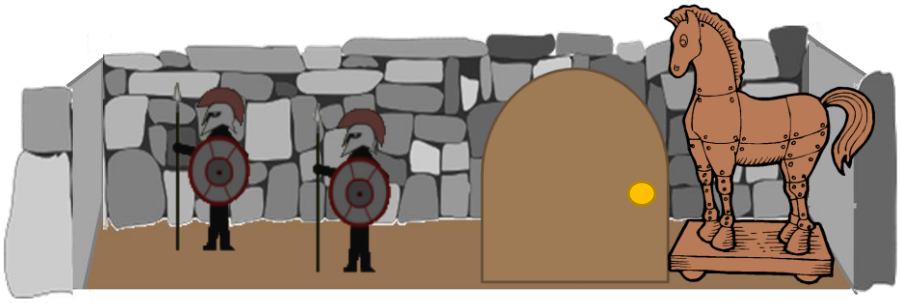
- Viruses: Can infect and spread, but need human assistance
  - People download infected email attachments, shared files, spoof links, etc.
  - Example: ILOVEYOU virus
- Worms: Can infect and spread *without* human assistance
  - Example: Sasser worm





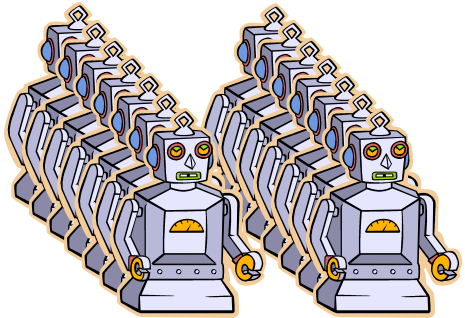
Malware: Trojan Horses

- 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



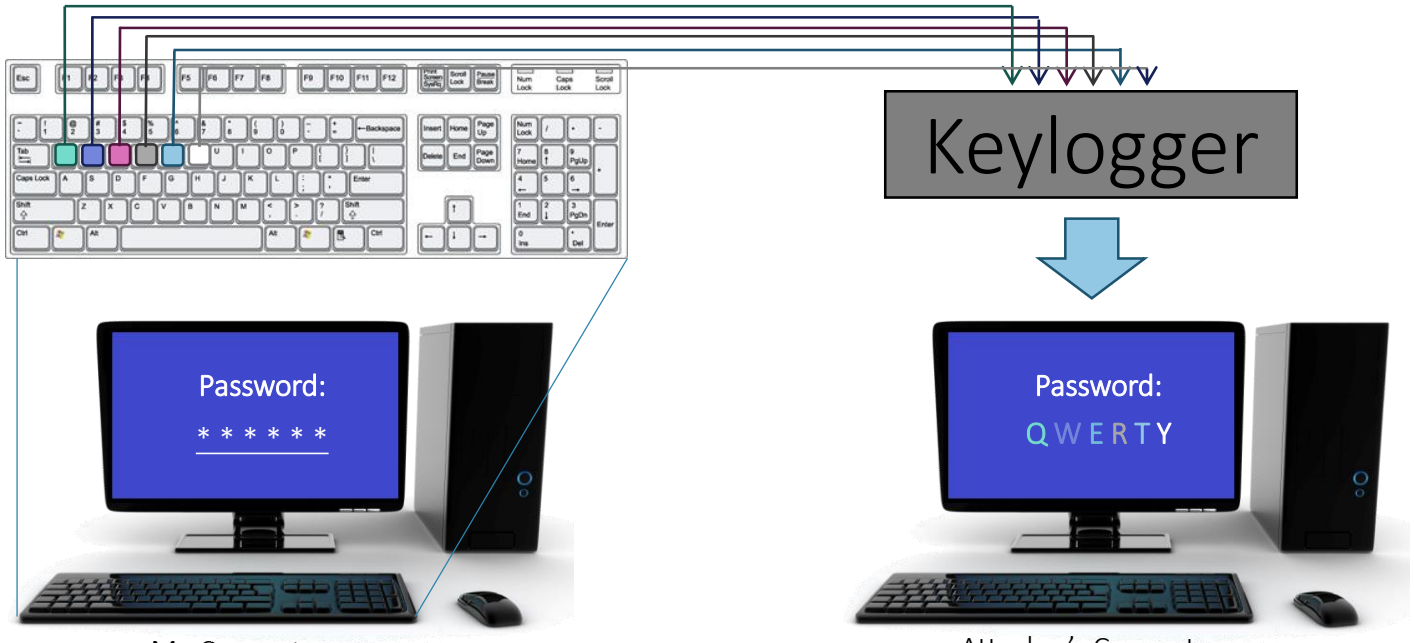
Malware: Zombies and Botnets

- 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 a suspect program attempts to run

Quarantines and removes infected files

Symantec

McAfee

Source: www.pcworld.com

AVG Anti-Virus

Source: www.royalpccare.com

digital defender
Digital Security Made Simple

Source: www.digital-defender.com

Microsoft Security Essentials

Source: www.zdnet.com

AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

SECTION FOUR

Basic Cybersecurity Techniques

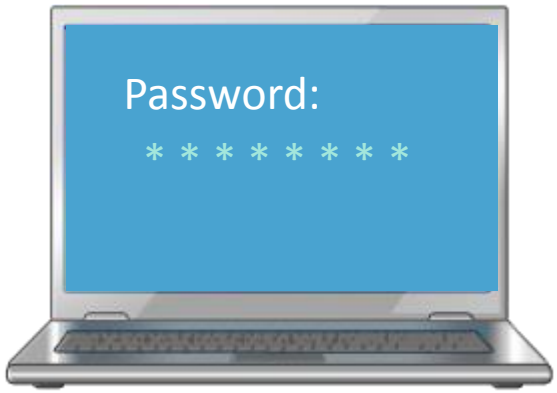
Basic Cybersecurity Techniques

- 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

Source: http://www.infosectoday.com/Articles/Authentication.htm

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



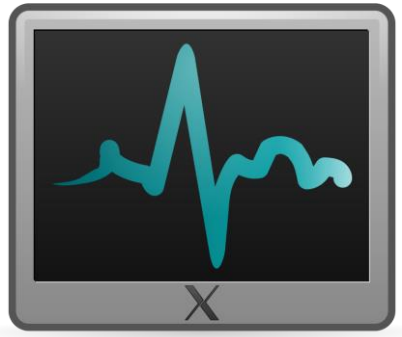
Authorization

- 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 is able to enter the system as a low-level user, but is able to attain high-level access
- Methods covered in detail in Units 7 and 8

Accountability

- Holds users responsible for their actions on a system
- Methods:
  - System monitoring
  - Audit logs



- Threats:
  - Denial of Service
    - Attack overwhelms audit logs with excessive or very large log entries, causing the system to run slowly or not at all
  - Disclosure of confidential information
    - Attacker is able to gather confidential or personally identifiable information from log files
- Methods covered in detail in Unit 8

Source: http://www.infosectoday.com/Articles/Authentication.htm

Authentication: Building Strong Passwords

Remember…….

C _____
L _____
O _____
U _____
D _____
S _____

NOT…

Source: tamutimes.tamu.edu

S _____
U _____
N _____

Passwords

This is Ronald Donald's Password:

NOT GOOD!

~~1234~~

Passwords - Complex

- Passwords of 8 characters consisting of
  - ~~Numbers only: 100 million~~ **Cracked under one second**
  - ~~+ Lower case: 2.8 trillion~~ **Cracked under eleven minutes**
  - ~~+ Upper case: 210 trillion~~ **Cracked under fifteen hours**
  - + Symbols: 7.2 quadrillion **Cracked under three weeks**

- Always use at least 3 of the following:
  - ✓ Numbers
  - ✓ Lower case letters
  - ✓ Upper case letters
  - ✓ Symbols (% # * & ! : { " > |)

Ronald's Old Password: 1234 New Password: Pa123!

Source: www.howsecureismypassword.net

Passwords - Lengthy

- Brute force attacks can run 4 billion calculations per second
  - ~~Six or fewer characters~~ — Cracked within three minutes
  - ~~Seven characters~~ — Cracked within five hours
  - ~~Eight characters~~ — Cracked within three weeks
  - Nine characters — Cracked within five years
  - Ten characters — Cracked within 526 years
- Always use at least 8 characters

Ronald's Old Password: Pa123!

New Password: Password123!

Passwords - Only Yours

Do not Share Your Password with ANYONE

Passwords - Unique

- Any of the top 10,000 passwords will be broken immediately
- 91% of people have one of the 1,000 most popular passwords
- Almost half of all people use one of the 100 most popular

– password	– letmein	– 1234567
– 123456	– dragon	– sunshine
– 12345678	– 111111	– master
– abc123	– baseball	– 123123
– qwerty	– iloveyou	– welcome
– monkey	– trustno1	– shadow

Ronald's Old Password: Password123!

New Password: Ronald123!

Passwords - Different

- Use different passwords for each login (e.g. Gmail and Facebook)
  - 73% of people do not

Example: [base password] [site]

Gmail: [Ronald123!] [GMA] = **Ronald123!GMA**

Facebook: [Ronald123!] [FAC] = **Ronald123!FAC**

Ronald's Old Password: Ronald123!

New Passwords: Ronald123!FAC and Ronald123!GMA

Passwords - Short Term

- The longer you keep a password the longer attackers have to try and 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

Passwords NOT Simple

- Do not use dictionary words
  - Fend off dictionary cracking attacks by using passphrases

Where's the beef?

↓ ↓ ↓

Wh D@ B33f?

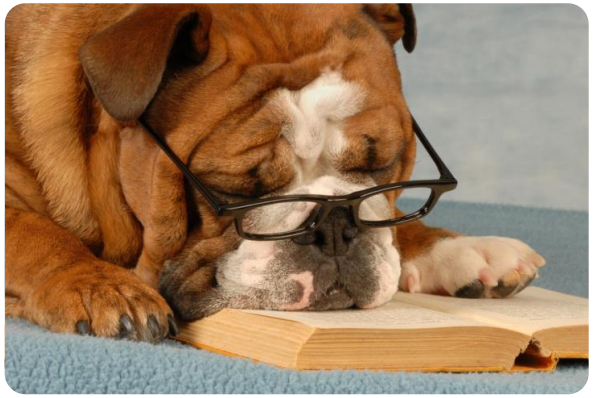
WhD@B33f?

Passwords - NOT User ID

- User ID is publicly available
- Using it as a password = Giving it away

Passwords - NOT Name

- Do not use any personal info – can be easily found by other means
  - Name
  - Birthday
  - Pet's Name
  - Mother's Maiden Name
  - Hometown



Old Gmail Password: Ronald123!GMA
New Password: WhD@B33f?GMA

Old Facebook Password: Ronald1234FAC
New Password: WhD@B33f?FAC

Building Strong Passwords

Remember…….

Complex
Lengthy
Only Yours
Unique
Different
Short Term

NOT…

Source: tamutimes.tamu.edu

Simple
User ID
Name