AIR FORCE ASSOCIATION’S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

UNIT FOUR

Principles of Cybersecurity

www.uscyberpatriot.org

AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

SECTION ONE

Cybersecurity Goals and Tools

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

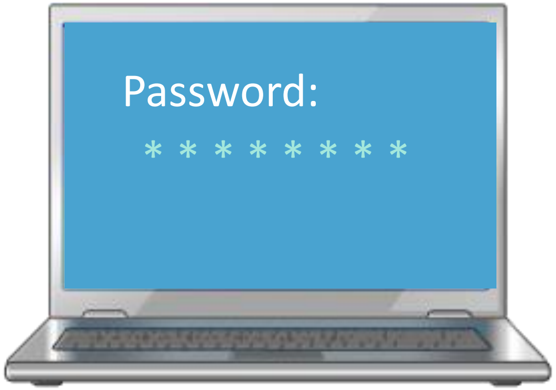
Source: http://www.techrepublic.com/blog/it-security/the-cia-triad/

The CIA Triad: 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)

Authentication/Encryption

- Process of verifying the identity of a user
- Used to control access to a resource
- 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



AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

SECTION TWO

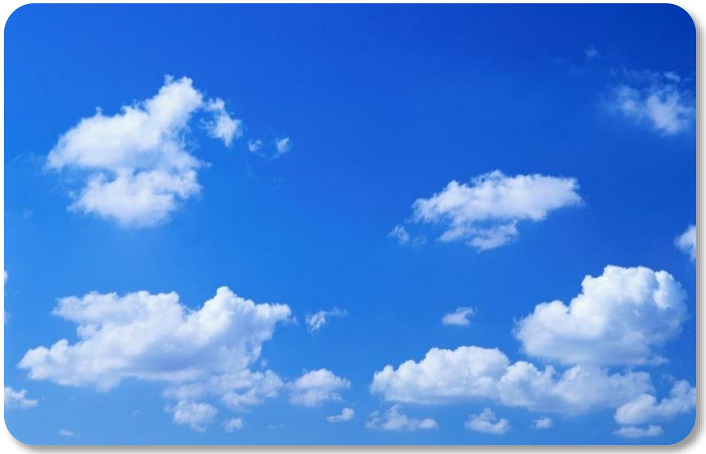
Building Strong Passwords

www.uscyberpatriot.org

Building Strong Passwords

Remember…….

NOT…



Source: tamutimes.tamu.edu

C ______________________

L ______________________

O ______________________

U ______________________

D ______________________

S ______________________

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 in < one second
~~+ Lower case: 2.8 trillion~~	Cracked in eleven minutes
~~+ Upper case: 210 trillion~~	Cracked in fifteen hours
+ Symbols: 7.2 quadrillion	Cracked in 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 in three minutes
~~Seven characters~~	Cracked in five hours
~~Eight characters~~	Cracked in three weeks
Nine characters	Cracked in five years
Ten characters	Cracked in 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
  - 123456
  - 12345678
  - abc123
  - qwerty
  - monkey
  - letmein
  - dragon
  - 111111
  - baseball
  - iloveyou
  - trustno1
  - 1234567
  - sunshine
  - master
  - 123123
  - welcome
  - 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

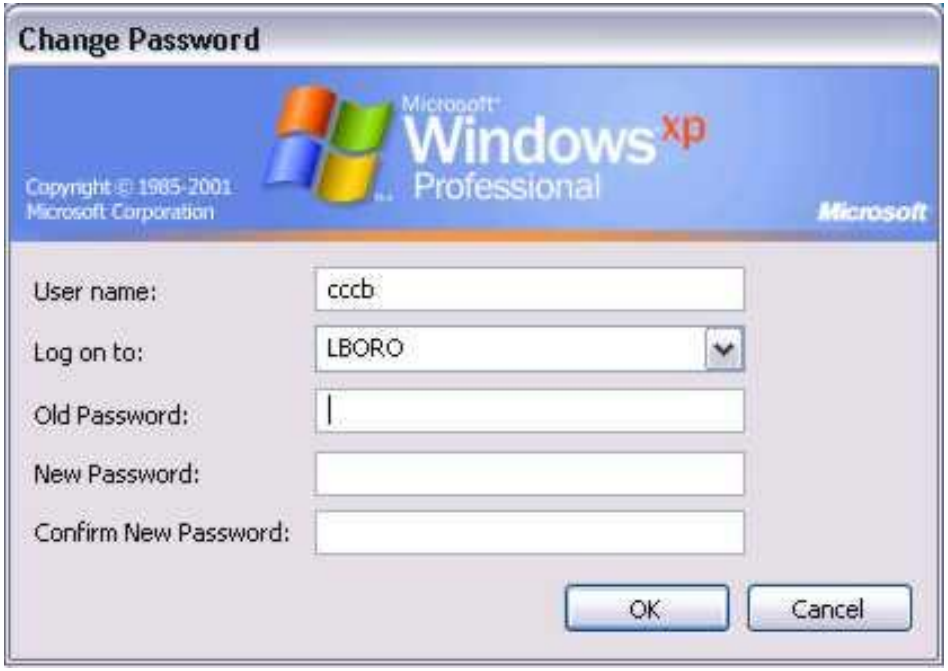
Example:	[base password]	[site]	
	↓	↓	
Gmail:	[Ronald123!]	[GMA]	= **Ronald123!GMA**
Facebook:	[Ronald123!]	[FAC]	= **Ronald123!FAC**

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



Change Password

Microsoft Windows xp Professional
Copyright © 1985-2001 Microsoft Corporation
Microsoft

User name: cccb

Log on to: LBORO

Old Password:

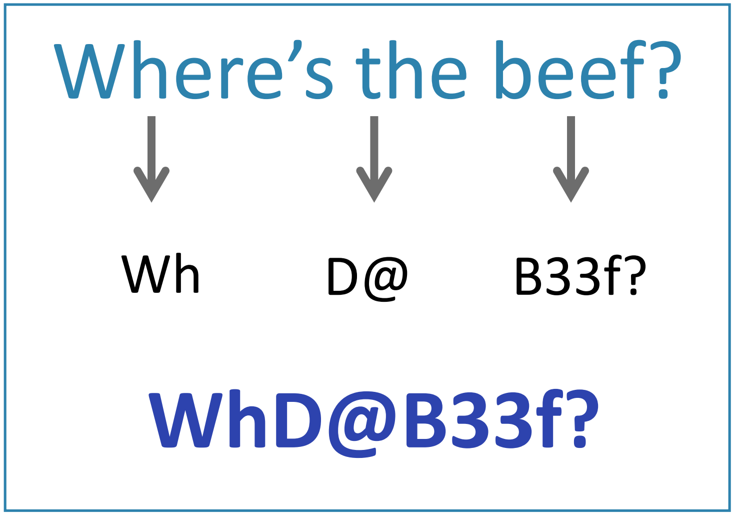
New Password:

Confirm New Password:

© Air Force Association

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

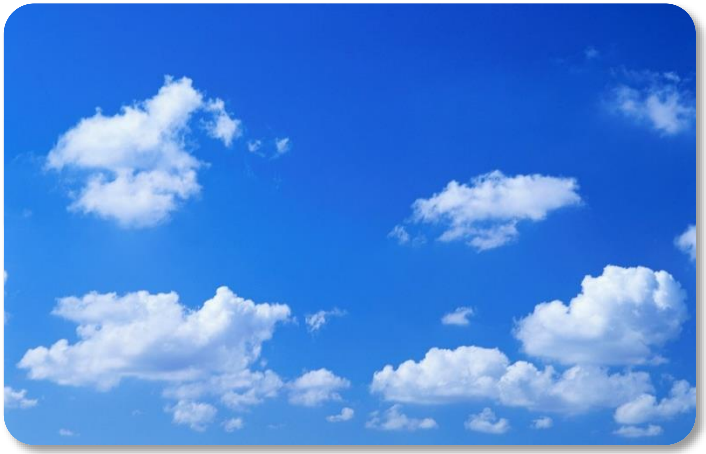
Old Gmail Password: Ronald123!GMA
New Password: WhD@B33f?GMA

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

Building Strong Passwords

Remember…….

NOT…



Source: tamutimes.tamu.edu

Complex
Lengthy
Only Yours
Unique
Different
Short Term

Simple
User ID
Name

SECTION THREE

Cyber Threats

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

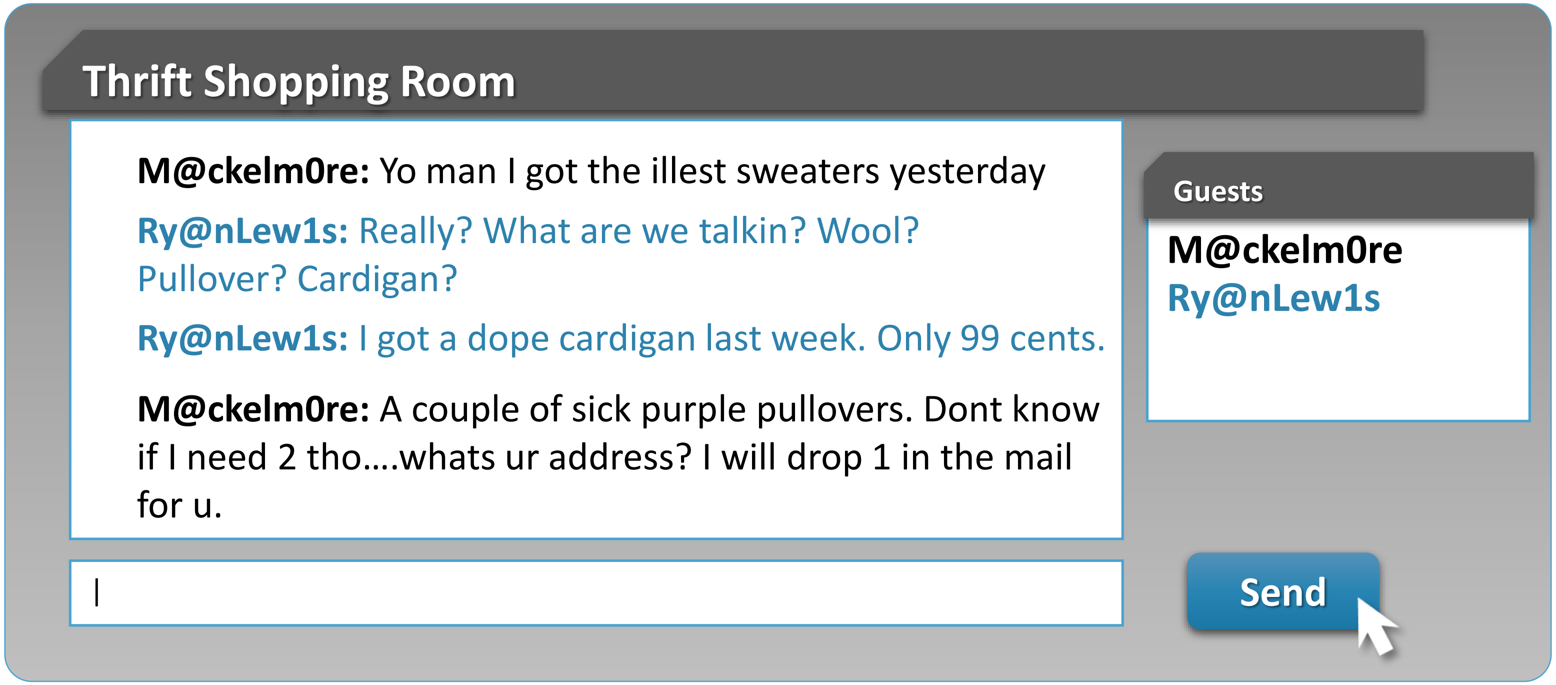
3. Use anti-malware and updates

4. Avoid using open networks

5. Customize security settings

Online Threats

SOCIAL ENGINEERING



M@ckelm0re: Yo man I got the illest sweaters yesterday

Ry@nLew1s: Really? What are we talkin? Wool? Pullover? Cardigan?

Ry@nLew1s: I got a dope cardigan last week. Only 99 cents.

M@ckelm0re: A couple of sick purple pullovers. Dont know if I need 2 tho....whats ur address? I will drop 1 in the mail for u.

- Social Engineering: Manipulating people into giving up personal information

Social Engineering Methods

SPEAR-PHISHING

- 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

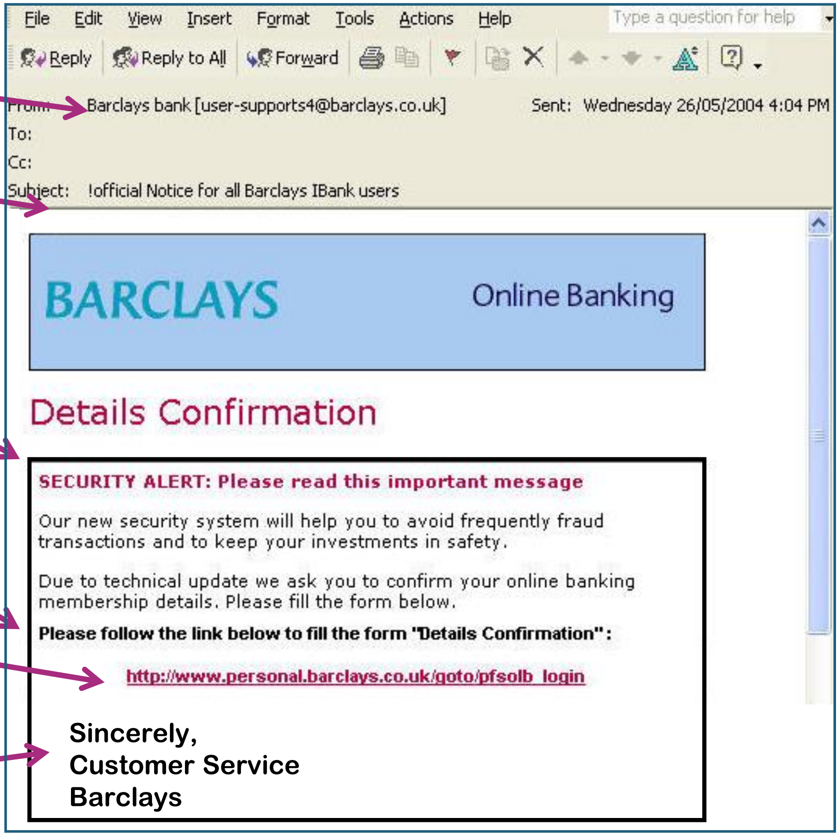
Spelling Errors/Typos

ALL CAPS

Asks for Personally Identifying Information

Executable attachment or link to a Website

Signed by a department, not an individual



From: Barclays bank [user-supports4@barclays.co.uk] Sent: Wednesday 26/05/2004 4:04 PM
To:
Cc:
Subject: !official Notice for all Barclays IBank users

BARCLAYS Online Banking

Details Confirmation

SECURITY ALERT: Please read this important message

Our new security system will help you to avoid frequently fraud transactions and to keep your investments in safety.

Due to technical update we ask you to confirm your online banking membership details. Please fill the form below.

Please follow the link below to fill the form "Details Confirmation":

http://www.personal.barclays.co.uk/goto/pfsolb_login

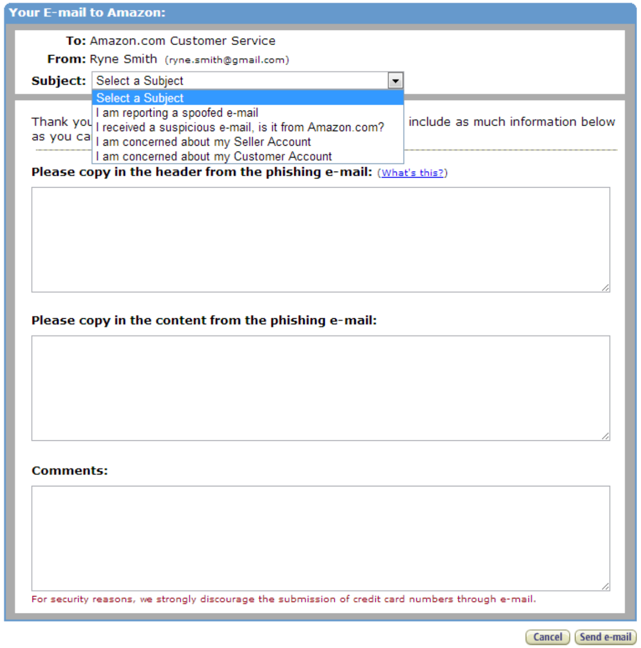
Sincerely,
Customer Service
Barclays

*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



Your E-mail to Amazon:

To: Amazon.com Customer Service

From: Ryne Smith (ryne.smith@gmail.com)

Subject: Select a Subject

Select a Subject
I am reporting a spoofed e-mail
I received a suspicious e-mail, is it from Amazon.com?
I am concerned about my Seller Account
I am concerned about my Customer Account

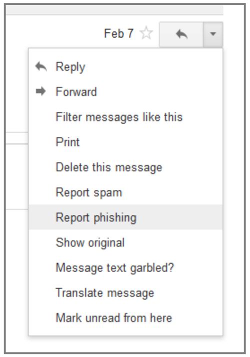
Thank you include as much information below as you ca

Please copy in the header from the phishing e-mail: (What's this?)

Please copy in the content from the phishing e-mail:

Comments:

For security reasons, we strongly discourage the submission of credit card numbers through e-mail.



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

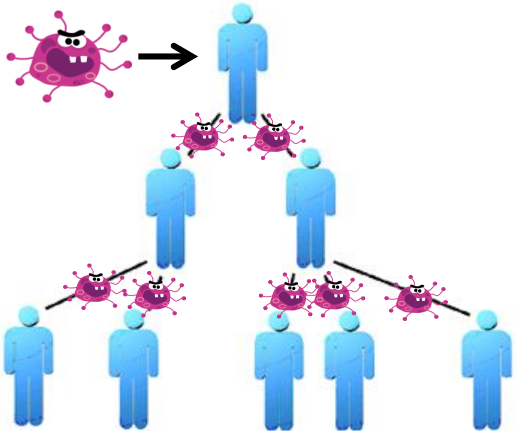
Malware: What is it?

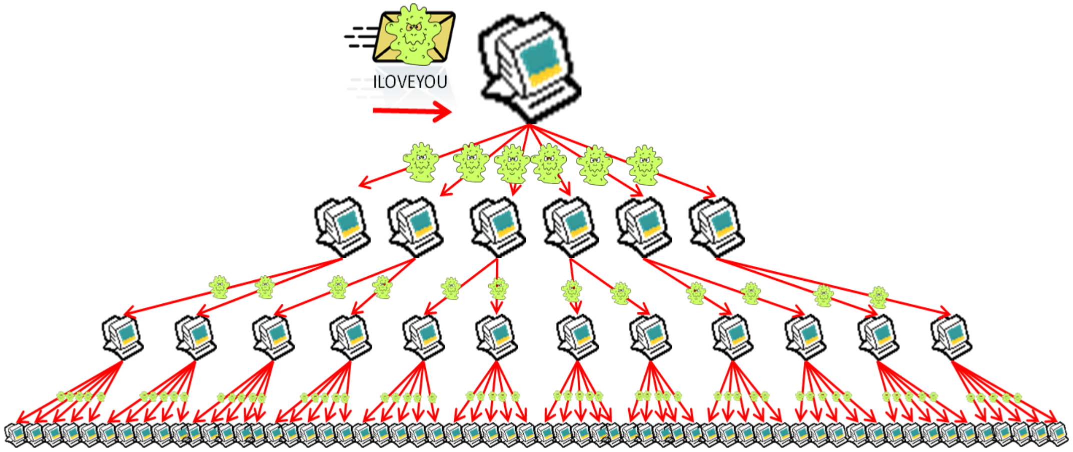
- **V**iruses/Worms
- **T**rojan Horses
- **Z**ombies and Botnets
- **K**eyloggers
- **B**ackdoors
- **L**ogic/Time Bombs
- **S**pyware

© Air Force Association

Malware: Viruses/Worms

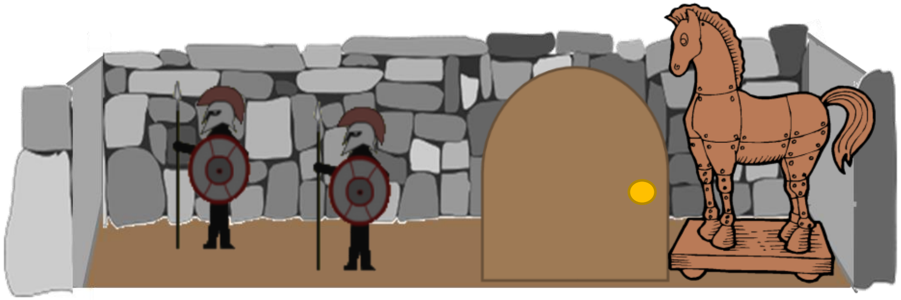
- Viruses: Can infect and spread but need human assistance
  - People download infected email attachments, shared files, spoof links, etc.
  - Example: ILOVEYOU virus
- Worms: Can infect and spread *without* human assistance
  - Example: Sasser worm





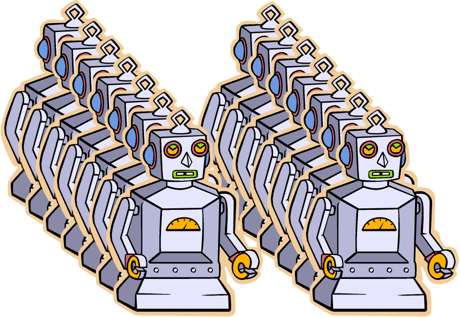
Malware: Trojan Horses

- 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



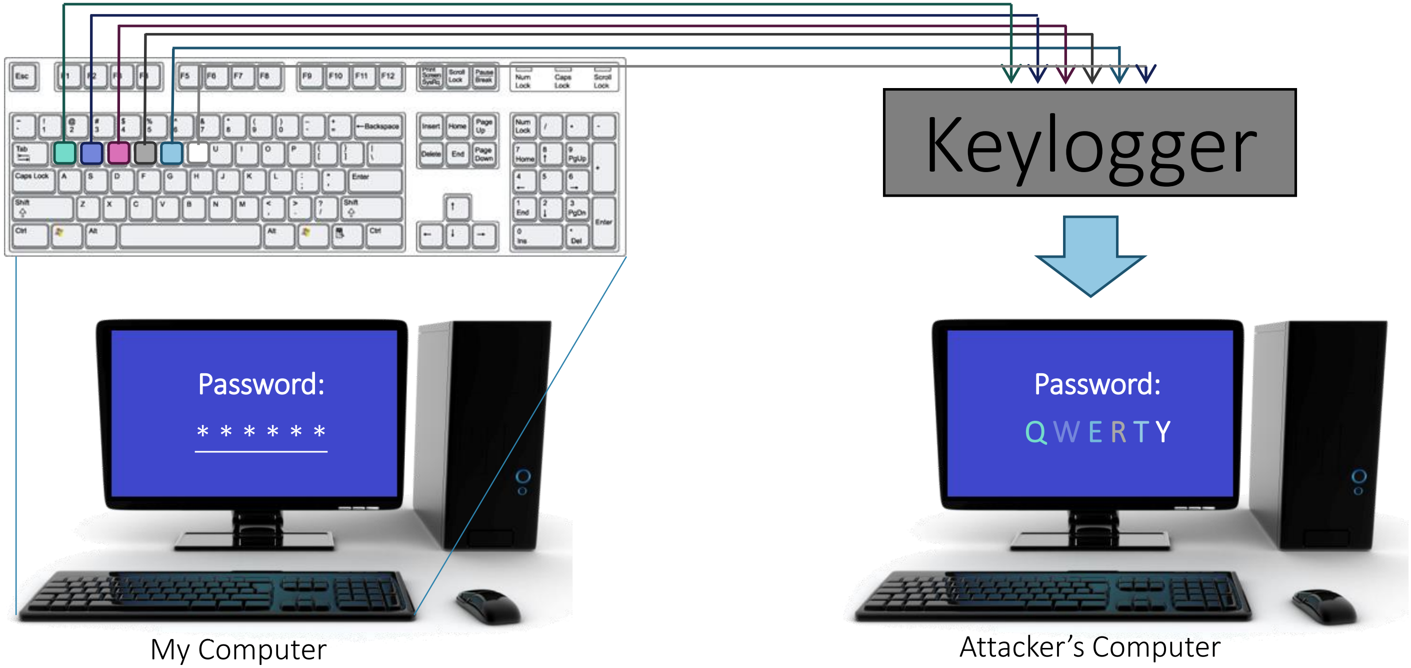
Malware: Zombies and Botnets

- 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

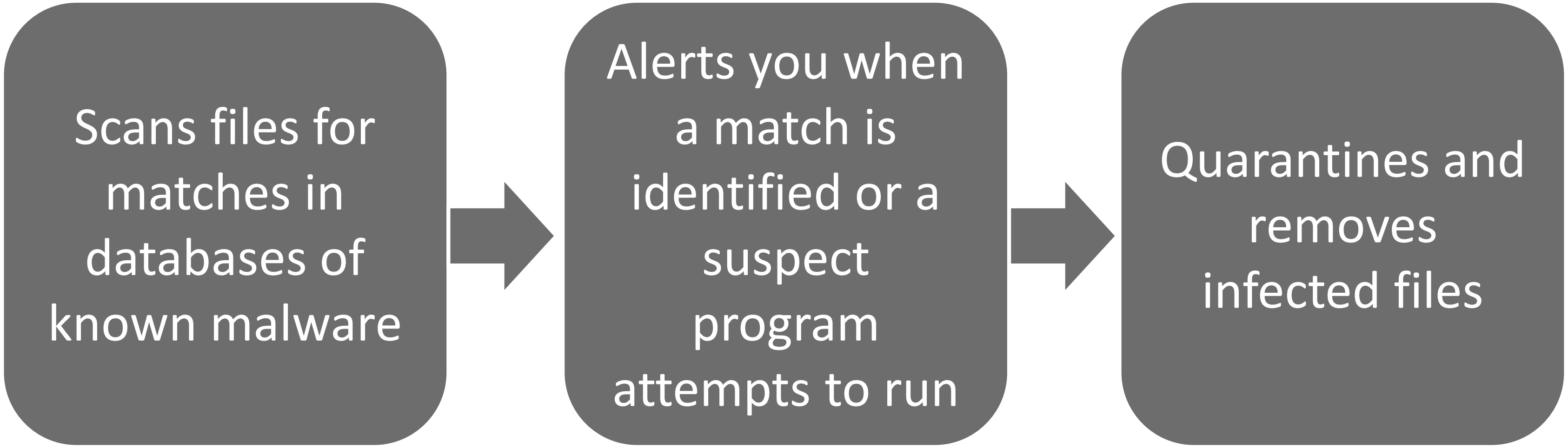
Malware: Logic/Time Bombs

- 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

Source: www.pcworld.com

Source: www.royalpccare.com

Source: www.digital-defender.com

Source: www.zdnet.com