

# Cybersecurity Primer

Defense in Depth Approach



# Importance of Cybersecurity

- ◎ The internet allows an attacker to work from anywhere on the planet.
- ◎ Risks caused by poor security knowledge and practice:
  - Identity Theft
  - Monetary Theft
  - Legal Ramifications (for yourself and your organization)
  - Sanctions or termination if policies are not followed
- ◎ According to the SANS Institute, the top vectors for vulnerabilities available to a cyber criminal are:
  - Web Browser
  - IM Clients
  - Web Applications
  - Excessive User Rights



# Cybersecurity is Safety

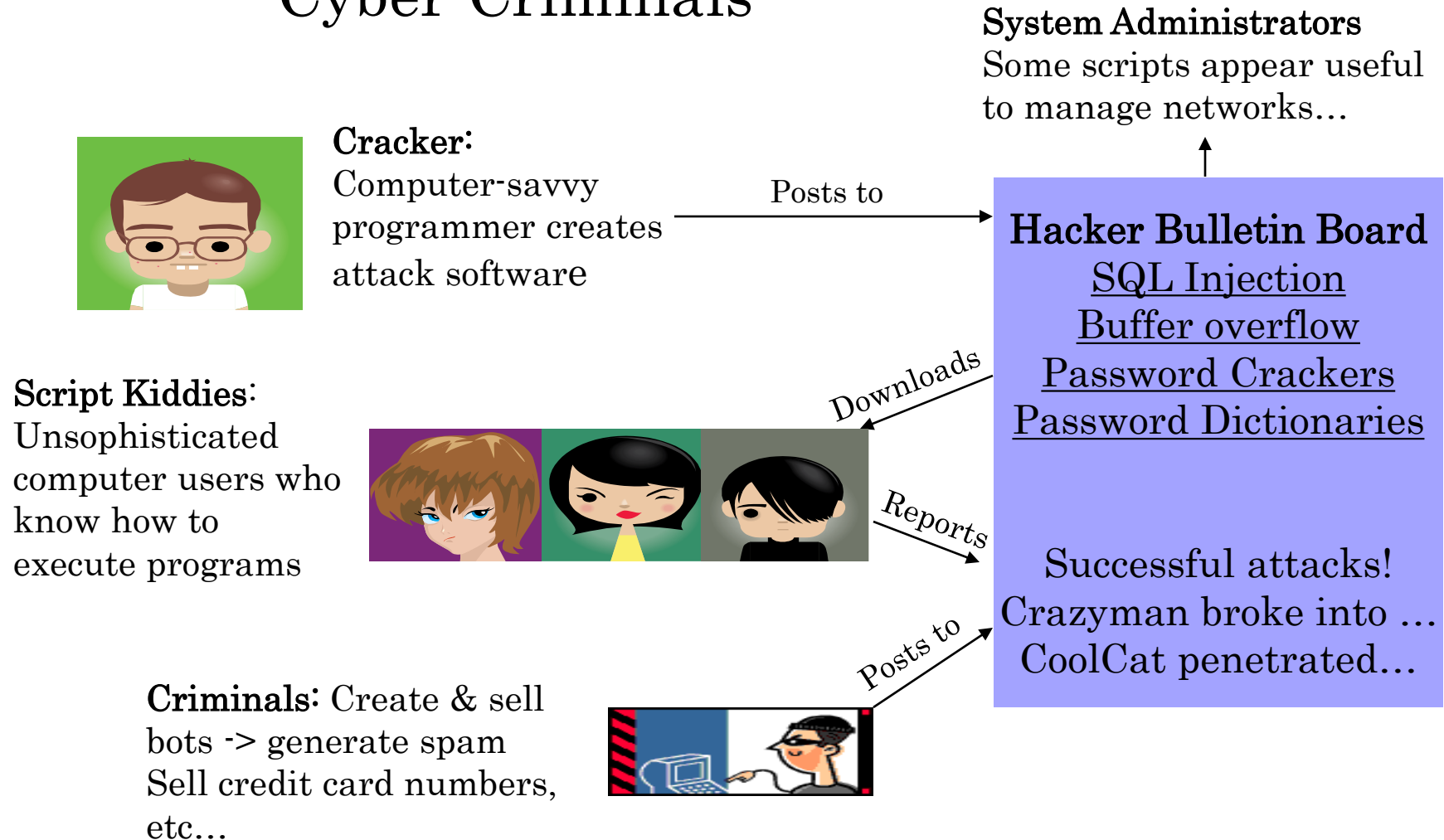
**Security:** We must protect our computers and data in the same way that we secure the doors to our homes.

**Safety:** We must behave in ways that protect us against risks and threats that come with technology.



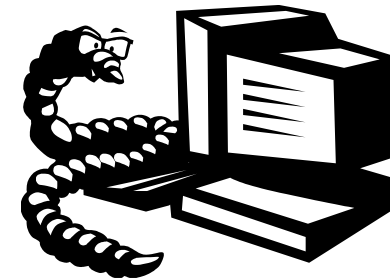
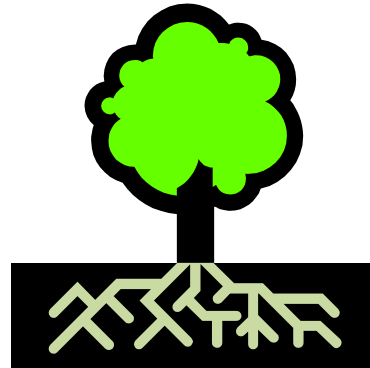
# User Awareness

## Cyber-Criminals



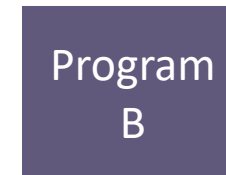
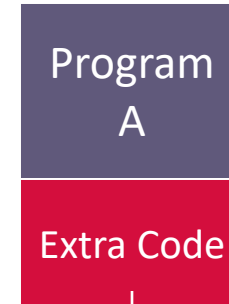
# Leading Threats

- Viruses
- Worms
- Trojan Horses / Logic Bombs
- Social Engineering
- Rootkits
- Phishing



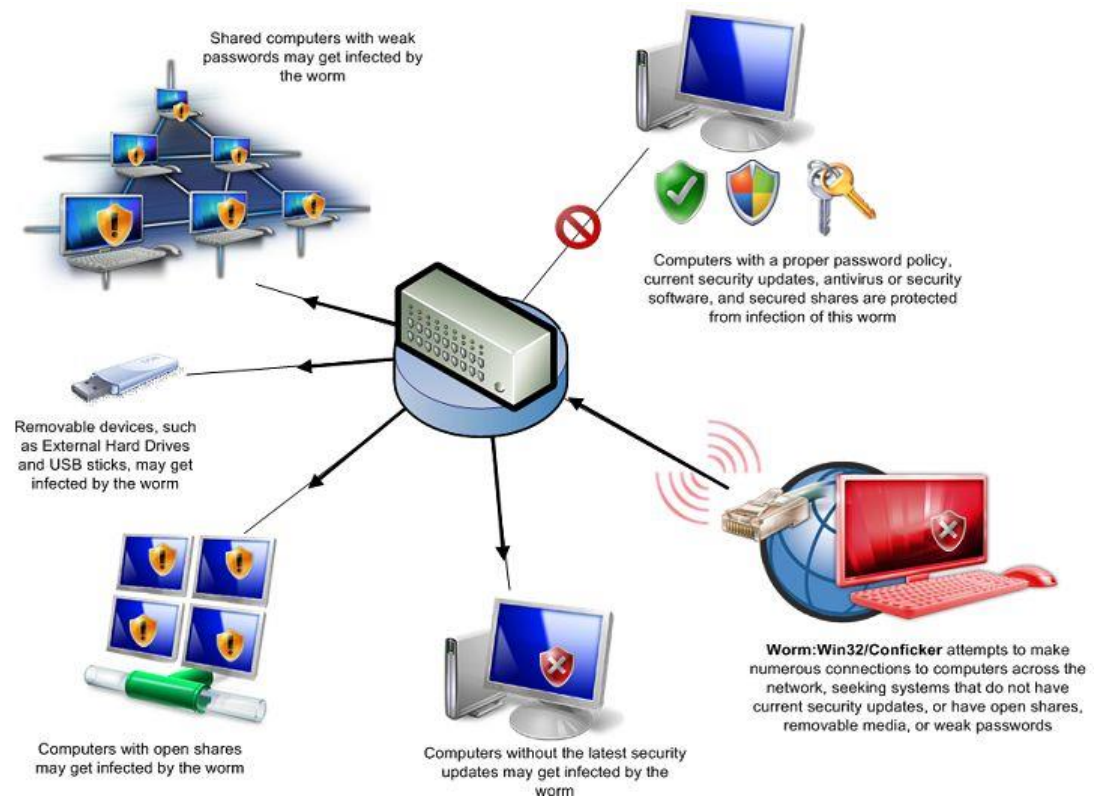
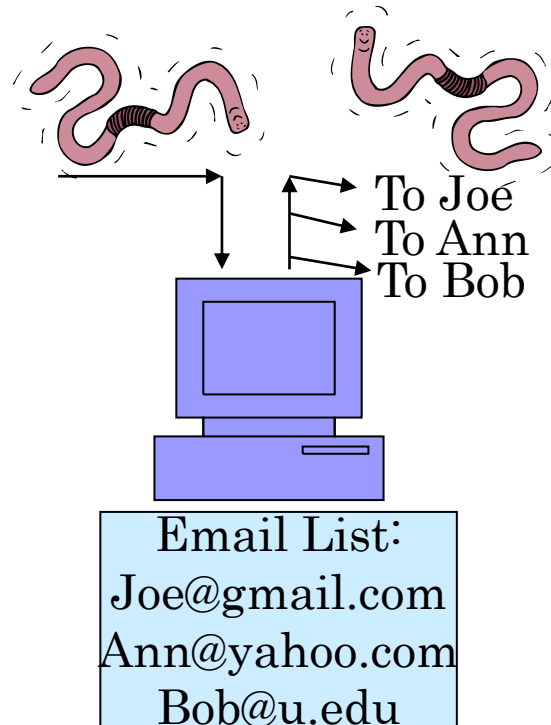
# Viruses

- ⦿ A virus attaches itself to a program, file, or disk.
- ⦿ When the program is executed, the virus activates and replicates itself.
- ⦿ The virus may be benign or malignant but executes its payload at some point (often upon contact).
  - Viruses can cause computer crashes and loss of data.
- ⦿ In order to recover or prevent virus attacks:
  - Avoid potentially unreliable websites/emails.
  - System Restore.
  - Re-install operating system.
  - Use and maintain anti-virus software.



# Worms

- Independent program that replicates itself and sends copies from computer to computer across network connections.
- Upon arrival, the worm may be activated to replicate.



# Logic Bombs and Trojan Horses

- Logic Bomb: Malware logic executes upon certain conditions. The program is often used for otherwise legitimate reasons.
  - Examples:
    - Software which malfunctions if maintenance fee is not paid.
    - Employee triggers a database erase when he is fired.
- Trojan Horse: Masquerades as a benign program while quietly destroying data or damaging your system.
  - Download a game: It may be fun but contains hidden code that gathers personal information without your knowledge.





# Social Engineering

manipulates people into performing actions or divulging confidential information. Similar to a confidence trick or simple fraud, the term applies to the use of deception to gain information, commit fraud, or access computer systems.

**Phone Call:**  
This is John,  
the System  
Administrator.  
What is your  
password?



**In Person:**  
What ethnicity  
are you? Your  
mother's  
maiden name?



**Email:**  
ABC Bank has  
noticed a  
problem with  
your account...

and have  
some  
lovely  
software  
patches!

I have come  
to repair  
your  
machine...



# Phishing: Counterfeit Email

A seemingly trustworthy entity asks for sensitive information such as SSN, credit card numbers, login IDs or passwords via e-mail.



# Pharming: Counterfeit Web Pages



Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: \$135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

<http://www.trustedbank.com/general/custverifyinfo.asp>

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,  
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Misspelled

Copyright  
date is old

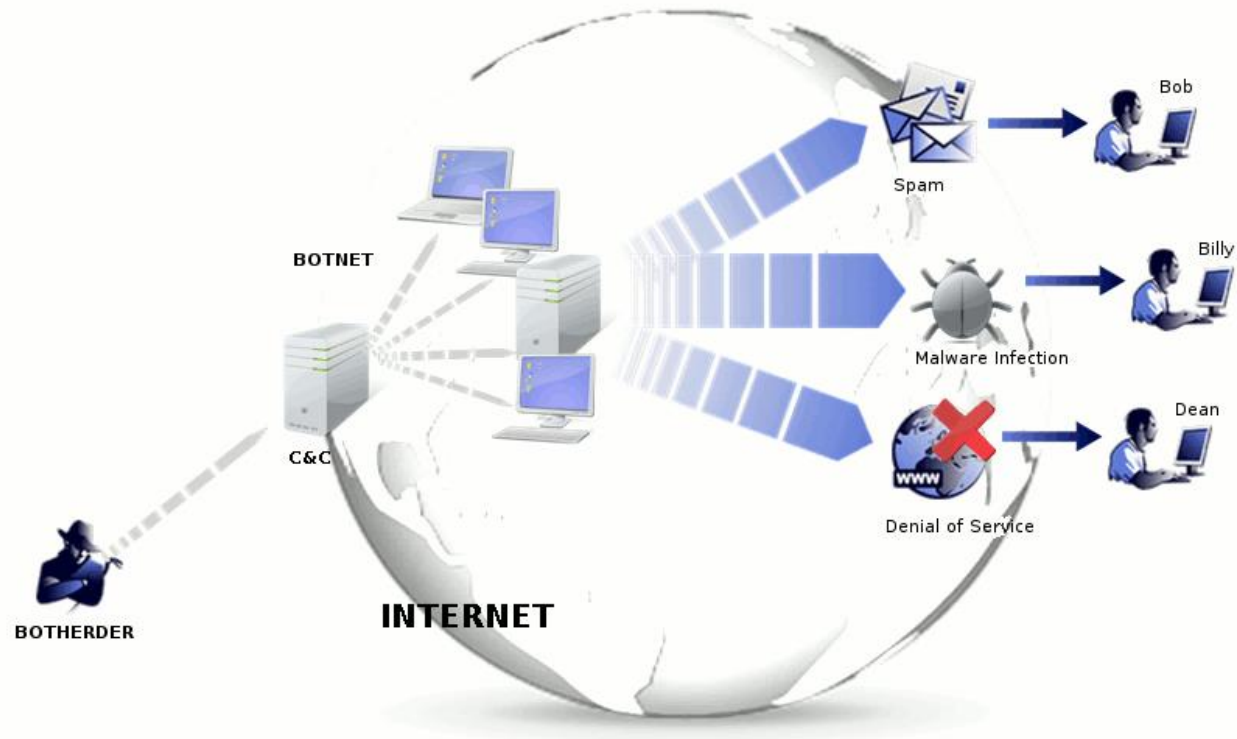
Wiping  
over, but  
not clicking  
the link  
may reveal  
a different  
address.

With whom?

- The link provided in the e-mail leads to a counterfeit webpage which collects important information and submits it to the owner.
- The counterfeit web page looks like the real thing
  - Extracts account information

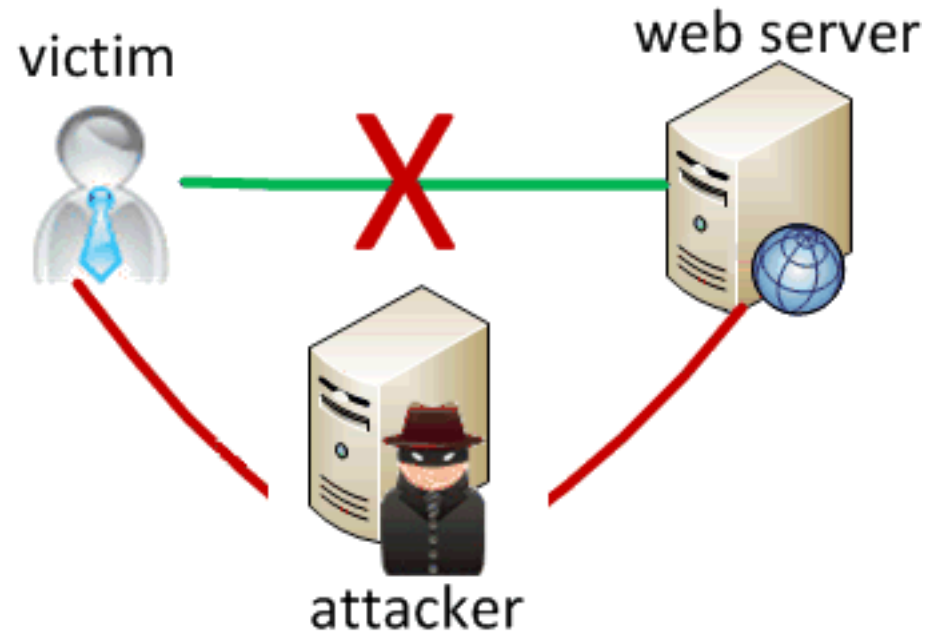
# Botnet

- ⦿ A botnet is a number of compromised computers used to create and send spam or viruses or flood a network with messages as a denial-of-service attack.
- ⦿ The compromised computers are called zombies.



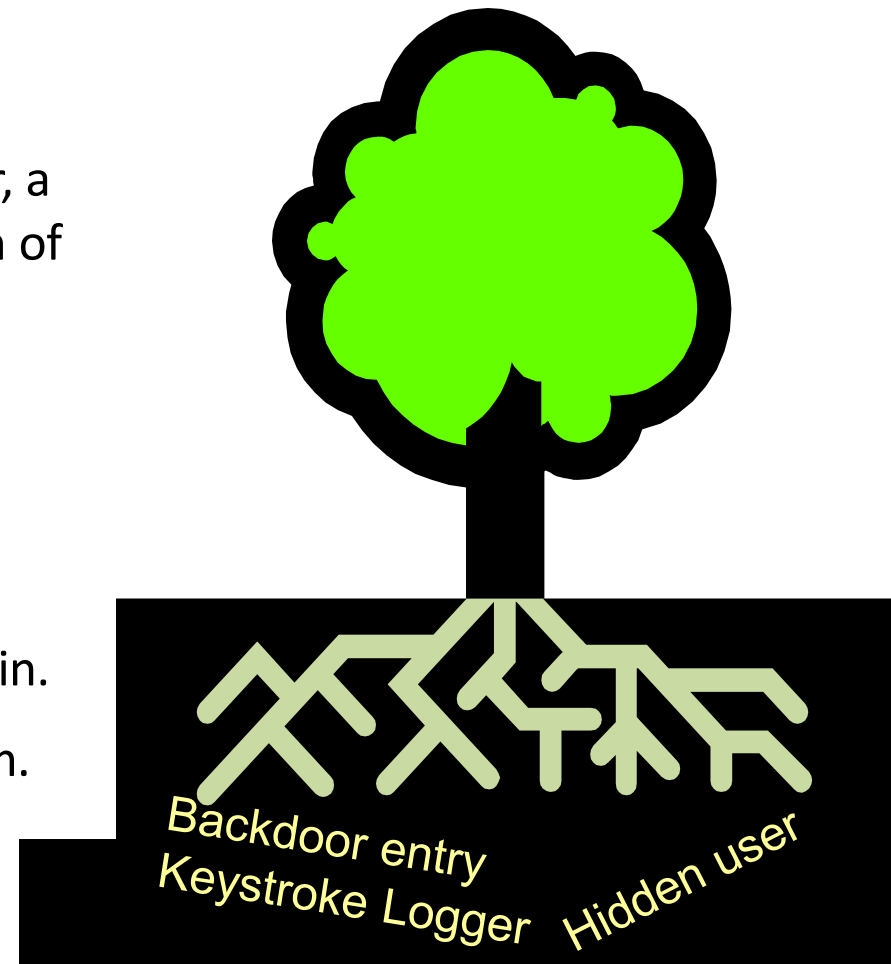
# Man In The Middle Attack

- An attacker pretends to be your final destination on the network. When a person tries to connect to a specific destination, an attacker can mislead him to a different service and pretend to be that network access point or server.



# Rootkit

- ◎ Upon penetrating a computer, a hacker may install a collection of programs, called a rootkit.
- ◎ May enable:
  - Easy access for the hacker (and others) into the enterprise
  - Keystroke logger
- ◎ Eliminates evidence of break-in.
- ◎ Modifies the operating system.



# Password Cracking

## Dictionary Attack and Brute Force: How Much Time It Will Take To Crack

Pattern	Calculation	Result	Time to Guess ( $2.6 \times 10^{18}$ tries/month)
Personal Info: interests, relatives		20	Manual 5 minutes
Social Engineering		1	Manual 2 minutes
American Dictionary		80,000	< 1 second
4 chars: lower case alpha	$26^4$	$5 \times 10^5$	
8 chars: lower case alpha	$26^8$	$2 \times 10^{11}$	
8 chars: alpha	$52^8$	$5 \times 10^{13}$	
8 chars: alphanumeric	$62^8$	$2 \times 10^{14}$	3.4 min.
8 chars alphanumeric +10	$72^8$	$7 \times 10^{14}$	12 min.
8 chars: all keyboard	$95^8$	$7 \times 10^{15}$	2 hours
12 chars: alphanumeric	$62^{12}$	$3 \times 10^{21}$	96 years
12 chars: alphanumeric + 10	$72^{12}$	$2 \times 10^{22}$	500 years
12 chars: all keyboard	$95^{12}$	$5 \times 10^{23}$	
16 chars: alphanumeric	$62^{16}$	$5 \times 10^{28}$	

# Identifying Security Compromises

## © Indicators:

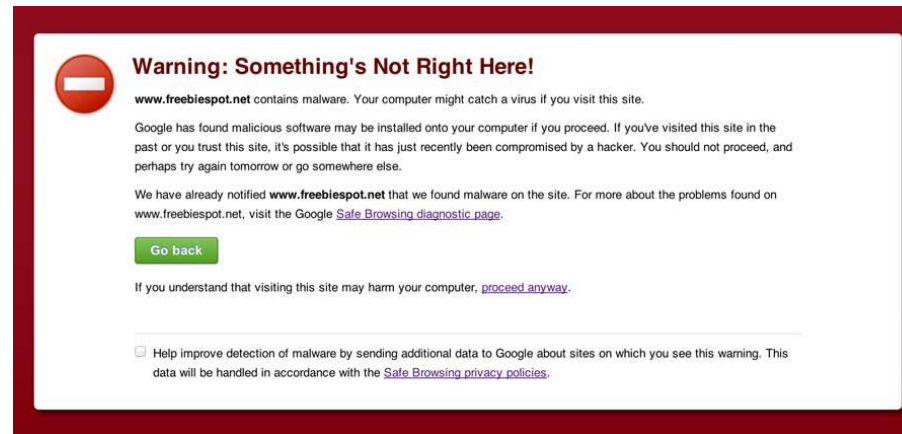
- Antivirus software detects a problem.
- Disk space disappears unexpectedly.
- Pop-ups suddenly appear, sometimes selling security software.
- Files or transactions appear that should not be there.
- The computer slows down to a crawl.
- Unusual messages, sounds, or displays on your monitor.
- Stolen laptop: 1 stolen every 53 seconds; 97% never recovered.
- The mouse pointer moves by itself.
- The computer spontaneously shuts down or reboots.
- Often unrecognized or ignored problems.





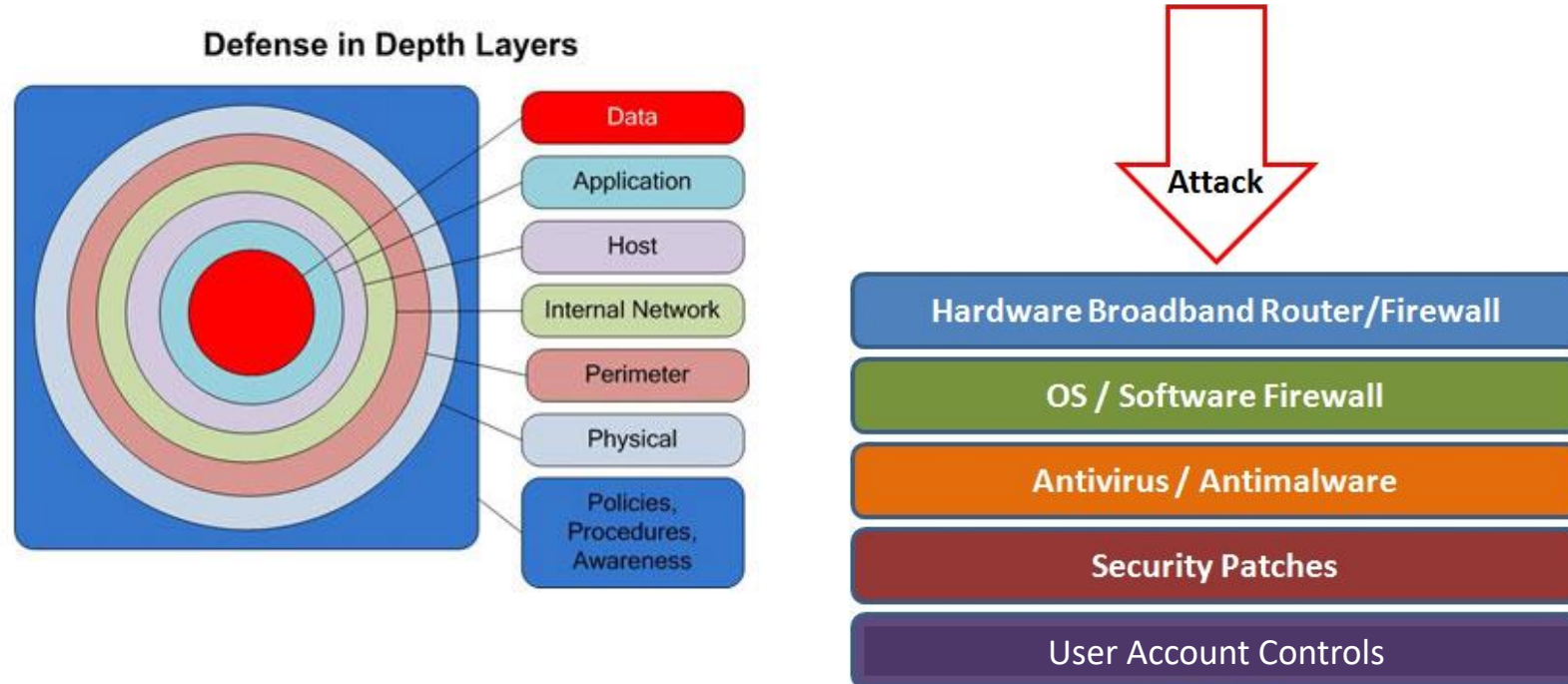
# Malware detection

- Spyware Indicators:
  - Changes to your browser homepage/start page.
  - Ending up on a strange site when conducting a search.
  - System-based firewall is turned off automatically.
  - Lots of network activity while not particularly active.
  - Excessive pop-up windows.
  - New icons, programs, favorites which you did not add.
  - Frequent firewall alerts about unknown programs when trying to access the Internet.
  - Poor system performance.



# Best Practices to avoid these threats

**Defense in depth** uses multiple layers of defense to address technical, personnel and operational issues.



# Anti-virus and Anti-spyware Software

- Anti-virus software detects certain types of malware and can destroy it before any damage is done.
- Install and maintain anti-virus and anti-spyware software.
- Be sure to keep anti-virus software updated.
- Many free and commercial options exist.
- Contact your Technology Support Professional for assistance.

**Norton**  
from symantec

**McAfee**

**KASPERSKY**

**AVG**  
Anti-Virus

**avast!**  
be free

**AVIRA**

**NOD32**  
antivirus

**bitdefender**  
secure your every bit

**TREND**  
MICRO

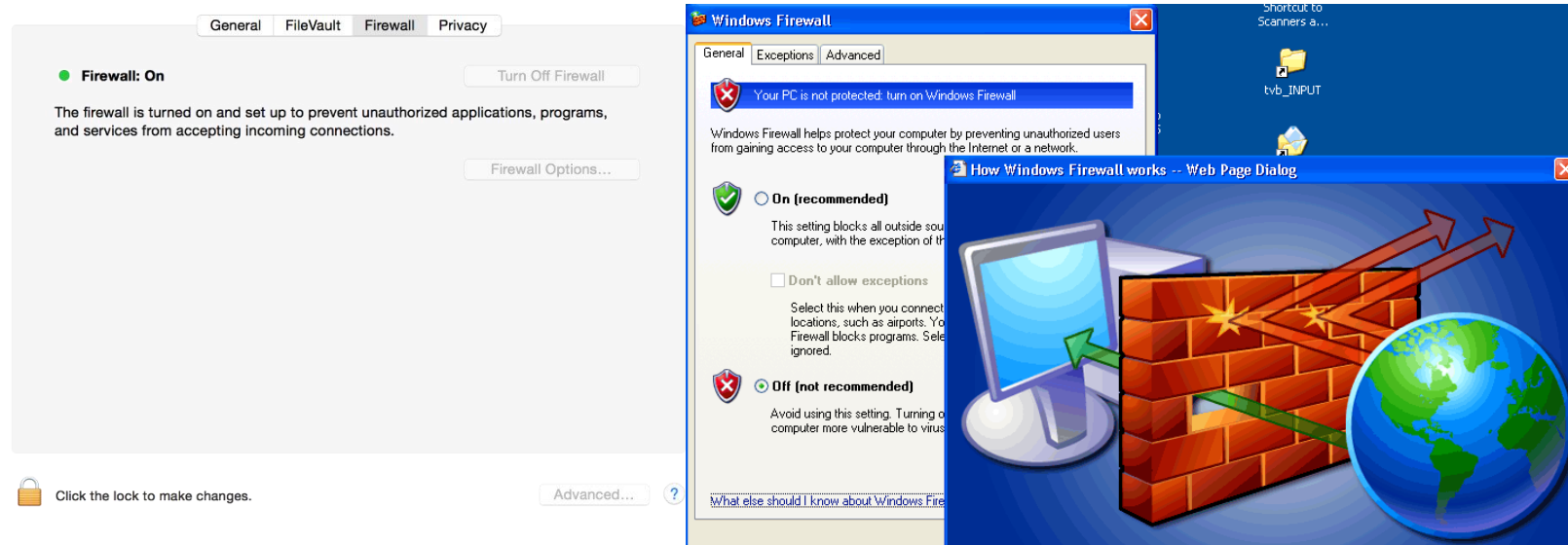
**F-Secure**

**eset**

**GDATA**

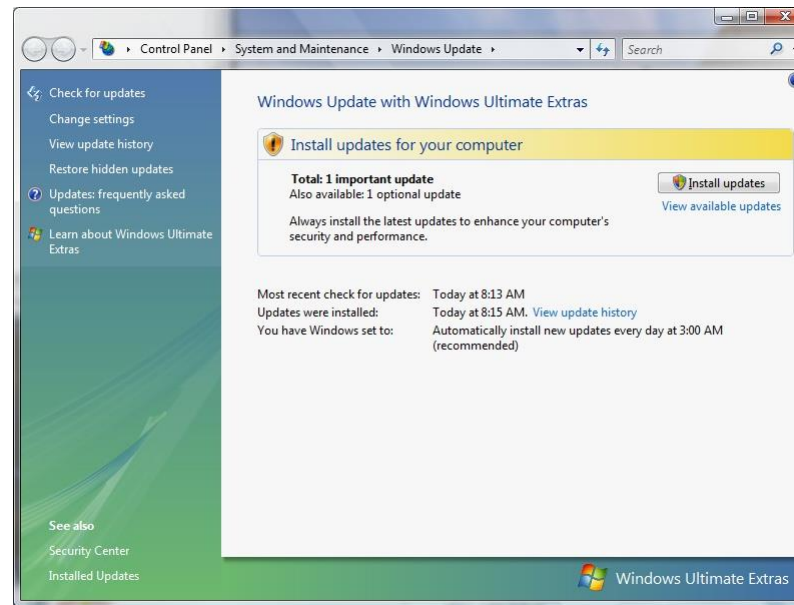
# Host-based Firewalls

- A firewall acts as a barrier between your computer/private network and the internet. Hackers may use the internet to find, use, and install applications on your computer. A firewall prevents many hacker connections to your computer.
- Firewalls filter network packets that enter or leave your computer



# Protect your Operating System

- Microsoft regularly issues patches or updates to solve security problems in their software. If these are not applied, it leaves your computer vulnerable to hackers.
- The Windows Update feature built into Windows can be set up to automatically download and install updates.
- Avoid logging in as administrator
- Apple provides regular updates to its operating system and software applications.
- Apply Apple updates using the App Store application.



# Use Strong Passwords

Make passwords easy to remember but hard to guess

- nOps standards:
- Be at least ten characters in length
- Must contain characters from at least two of the following four types of characters:
  - English upper case (A-Z)
  - English lower case (a-z)
  - Numbers (0-9)
  - Non-alphanumeric special characters (\$, !, %, ^, ...)
- Must not contain the user's name or part of the user's name
- Must not contain easily accessible or guessable personal information about the user or user's family, such as birthdays, children's names, addresses, etc.

# Creating Strong Passwords

- A familiar quote can be a good start:

“LOVE IS A SMOKE MADE WITH THE FUME OF SIGHS”

*William Shakespeare*

- Using the organization standard as a guide, choose the first character of each word:
  - LIASMWTFOS
- Now add complexity the standard requires:
  - L1A\$mwTF0S (10 characters, 2 numerals, 1 symbol, mixed English case: password satisfies all 4 types).
- Or be more creative!

# Password Guidelines

- Never use admin, root, administrator, or a default account or password for administrative access.
- A good password is:
  - Private: Used by only one person.
  - Secret: It is not stored in clear text anywhere, including on Post-It® notes!
  - Easily Remembered: No need to write it down.
  - Contains the complexity required by your organization.
  - Not easy to guess by a person or a program in a reasonable time, such as several weeks.
  - Changed regularly: Follow organization standards.
- Avoid shoulder surfers and enter your credentials carefully! If a password is entered in the username field, those attempts usually appear in system logs.





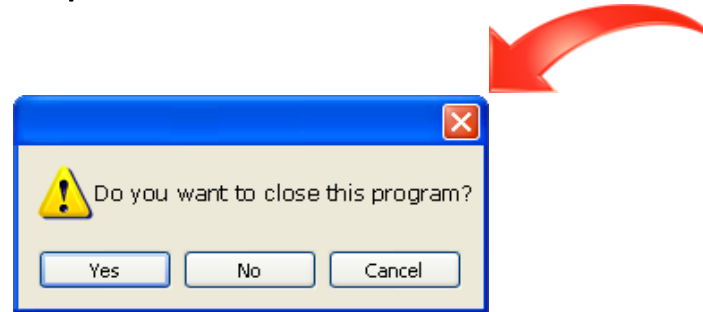
# Avoid Social Engineering and Malicious Software

- Do not open email attachments unless you are expecting the email with the attachment, and you trust the sender.
- Do not click on links in emails unless you are absolutely sure of their validity.
- Only visit and/or download software from web pages you trust.



# Avoid Stupid Hacker Tricks

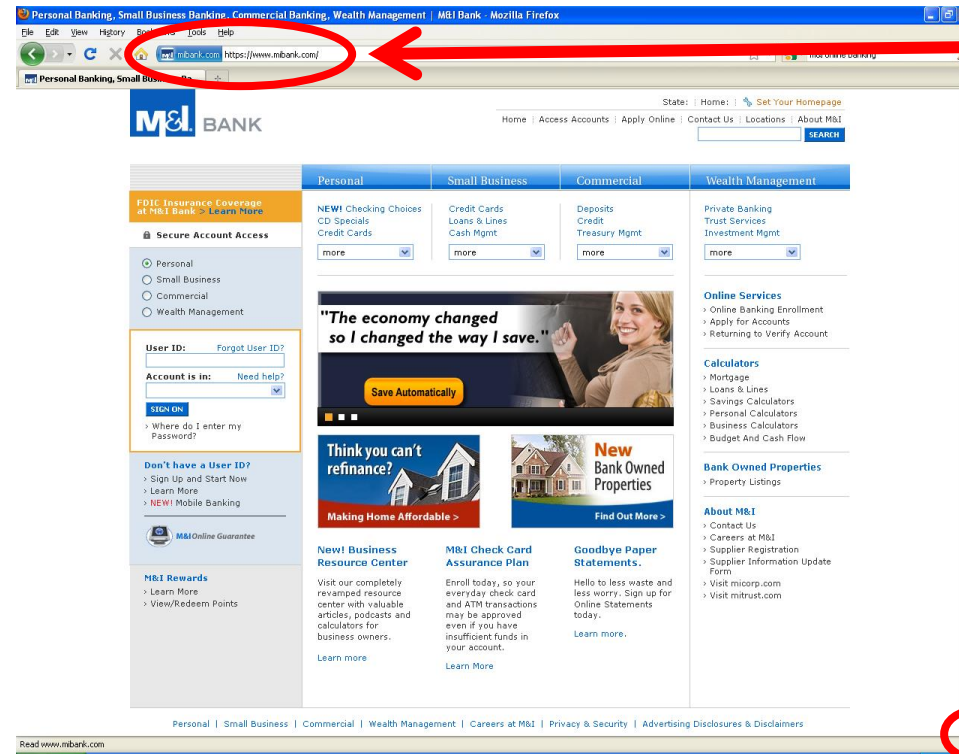
- ◎ Be sure to have a good firewall or pop-up blocker installed.
- ◎ Pop-up blockers do not always block ALL pop-ups so always close a pop-up window using the 'X' in the upper corner.
- ◎ Never click “yes,” “accept” or even “cancel.”



- ◎ Infected USB drives are often left unattended by hackers in public places.

# Secure Business Transactions

- ⑦ Always use secure browser to do online activities.
- ⑦ Frequently delete temp files, cookies, history, saved passwords etc.



https://

Symbol indicating enhanced security

# Backup Important Information

- ⦿ No security measure is 100% reliable.
- ⦿ Even the best hardware fails.
- ⦿ What information is important to you?
- ⦿ Is your backup:



Recent?  
Off-site & Secure?  
Process Documented?  
Encrypted?  
Tested?



# Cyber Incident Reporting

If you suspect a cybersecurity incident, notify your organization's help desk or the nOps help desk immediately. Be prepared to supply the details you know and contact information.

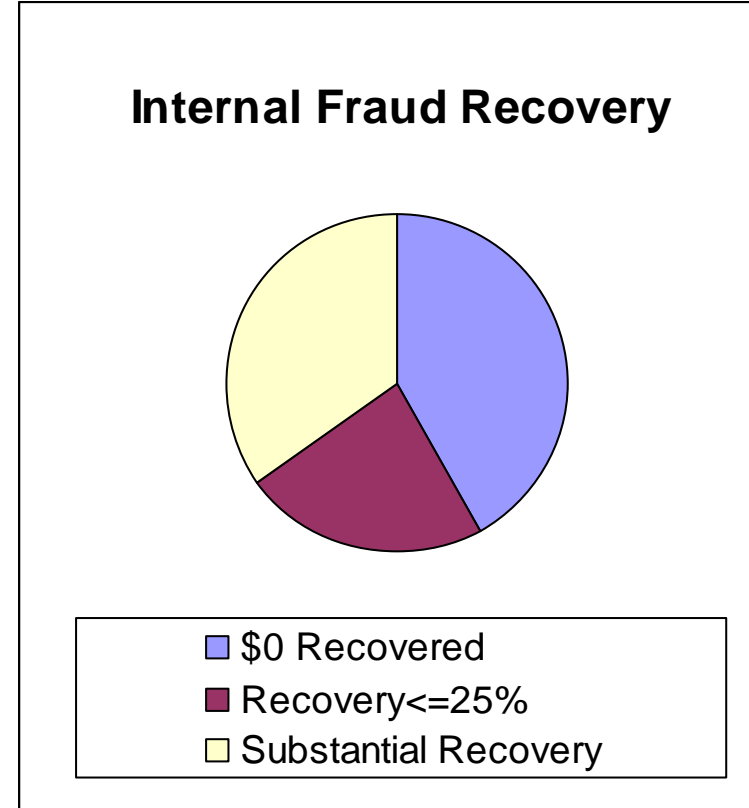
1. Do not attempt to investigate or remediate the incident on your own.
2. Inform other users of the system and instruct them to stop work immediately.
3. Unless instructed, do not power down the machine.
4. Unless instructed, do not remove the system from the network.

The cybersecurity incident response team will contact you as soon as possible to gather additional information.

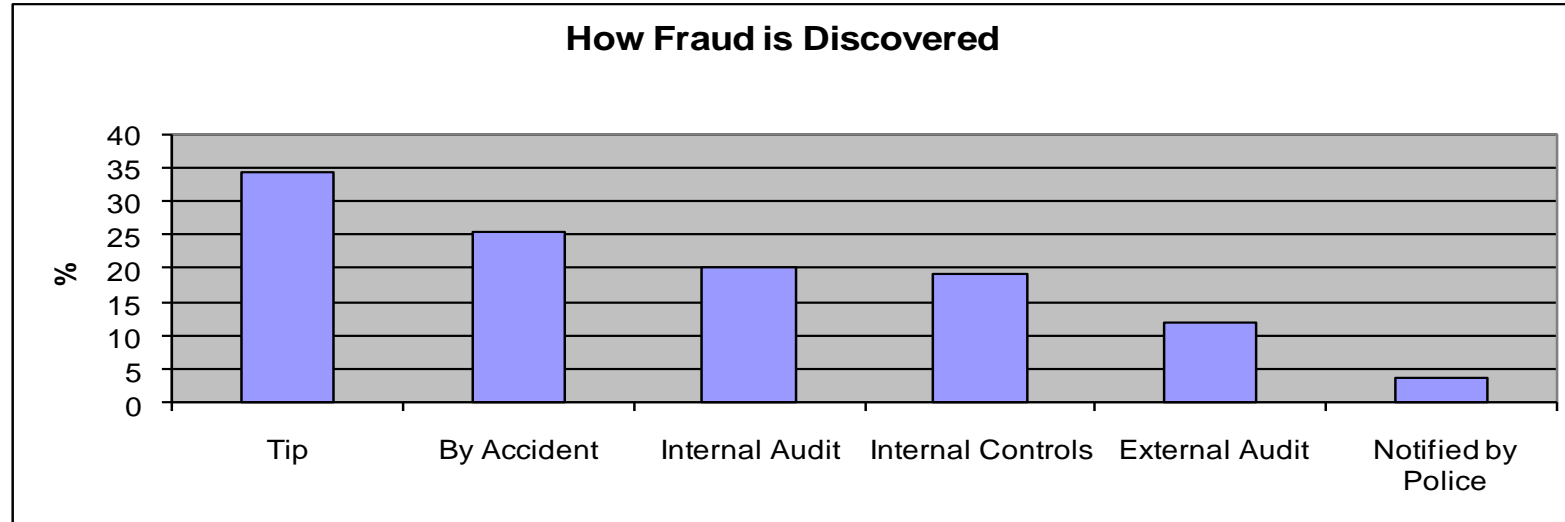
Each nOps department is required to have a specific plan to handle cybersecurity incidents. Refer to local policies, standards and guidelines for specific information.

# Fraud

- ◎ Organizations lose 5-6% of revenue annually due to internal fraud = \$652 Billion in U.S. (2006)
- ◎ Average scheme lasts 18 months, costs \$159,000
- ◎ 25% costs exceed \$1M
- ◎ Smaller companies suffer greater average dollar losses than large companies



# Fraud Discovery



Tips are the most common way fraud is discovered.

Tips come from:

- Employee/Coworkers 64%,
- Anonymous 18%,
- Customer 11%,
- Vendor 7%

# Thank you



keep  
yourself  
secure  
online