

# Security Awareness



Protect Your Information

# Poor Security Knowledge

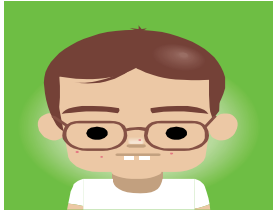
- Risks caused by poor security knowledge and practice:
- Identity Theft
- Monetary Theft
- Legal Ramifications (for yourself and your organization)
- Sanctions or termination if policies are not followed



# Cyber-Guys

## Script Kiddies:

Unsophisticated computer users who know how to execute programs



**Criminals:** Create & sell bots -> generate spam  
Sell credit card numbers, etc...



Ex. Malware package earns \$1K-2K

## System Administrators

Some scripts appear useful to manage networks...

## Hacker Bulletin Board

SQL Injection

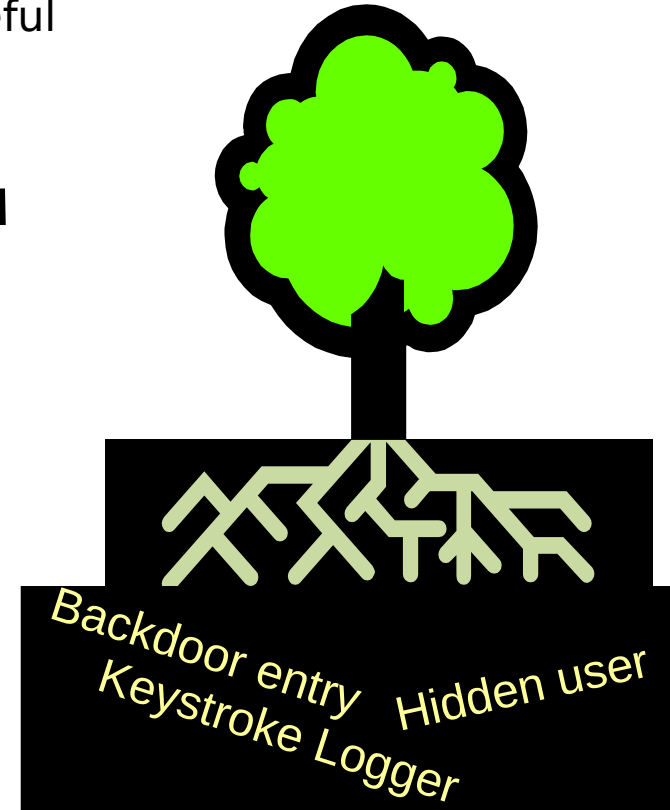
Buffer overflow

Password Crackers

Malware

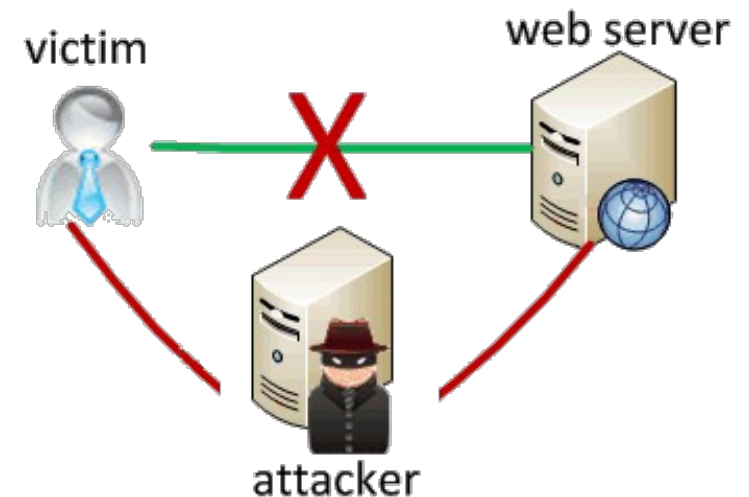
Rootkits

## Rootkit



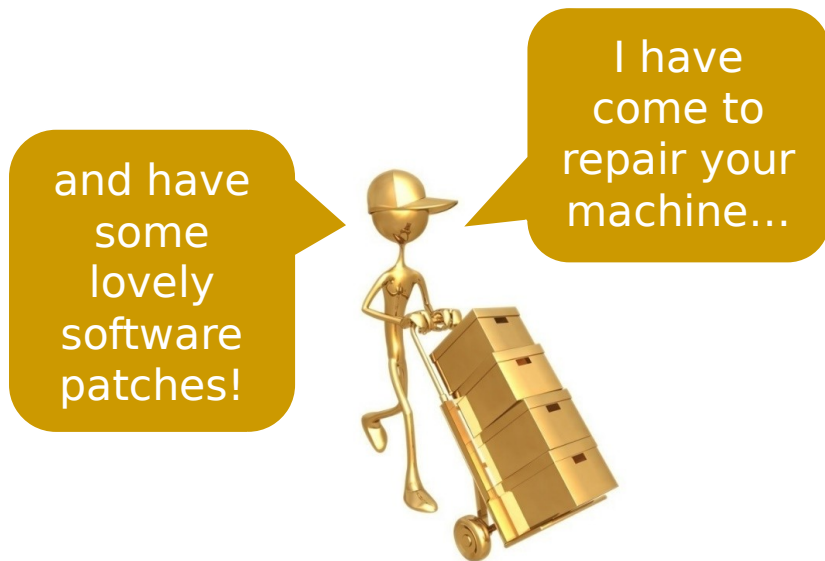
# Man In The Middle Attack

- 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.



# 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?

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

# Phishing: Counterfeit Email

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

From: GlobalPay <VT@globalpay.com>   
Subject: Restore your account  
Date: February 7, 2014 3:47:02 AM MST  
To: David

[Hide](#)

1 Attachment, 7 KB [Save](#) [Quick Look](#)

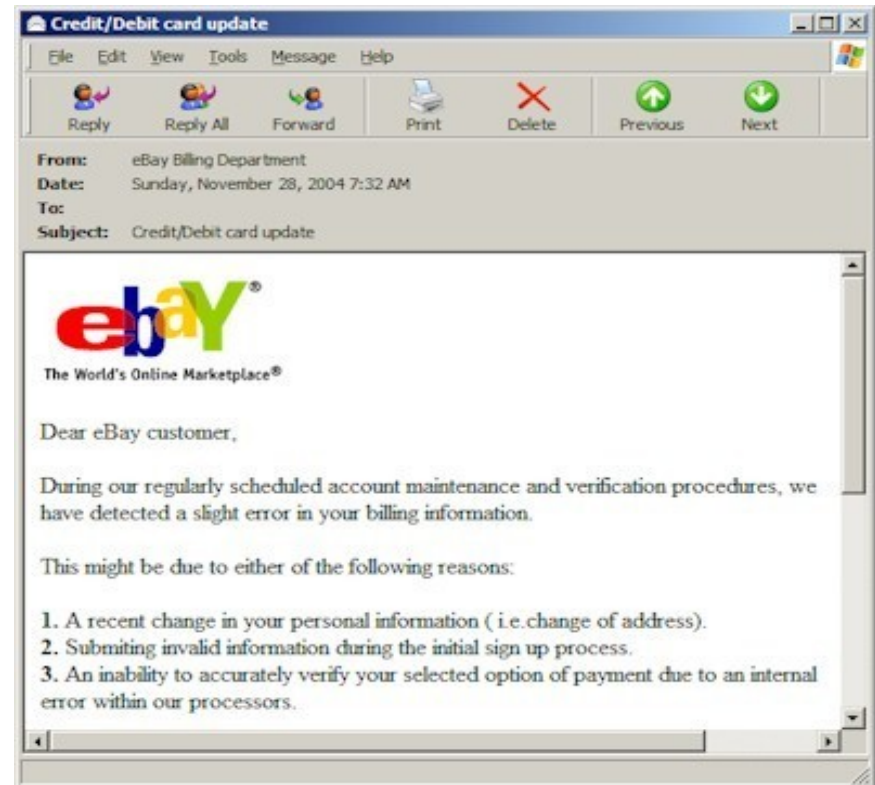
Dear customer,

We regret to inform you that your account has been restricted.  
To continue using our services please download the file attached to this e-mail and update your login information.

© GlobalPaymentsInc



[update2816.html \(7 KB\)](#)



# Identifying Security Compromises

- Symptoms:
- 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.
- The mouse pointer moves by itself.
- The computer spontaneously shuts down or reboots.
- Often unrecognized or ignored problems.



# 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.





# Use Strong Passwords

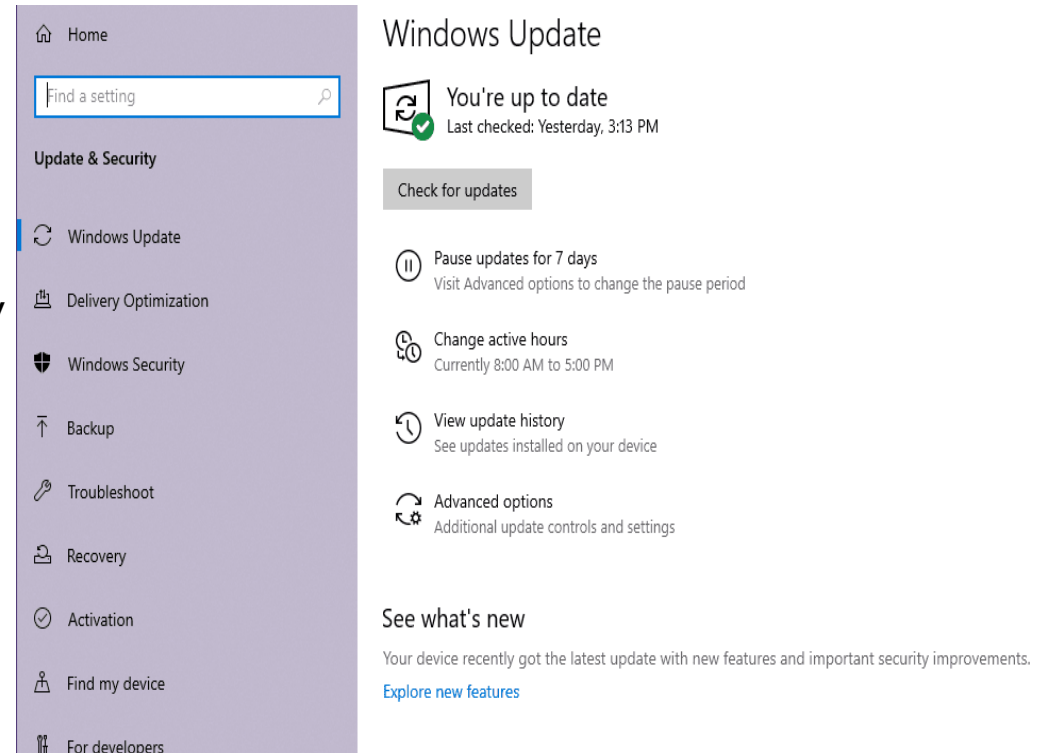
Make passwords easy to remember but hard to guess

- 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.



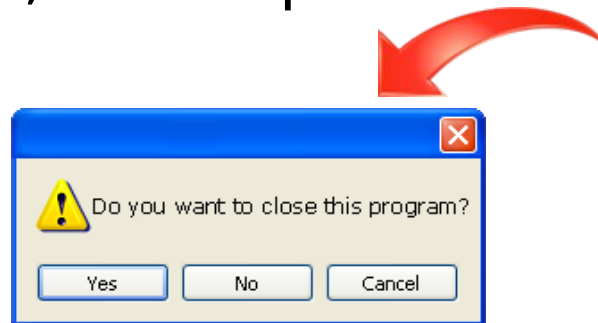
# Keep your Operating System Updated

- 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.



# 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.”



# 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?

