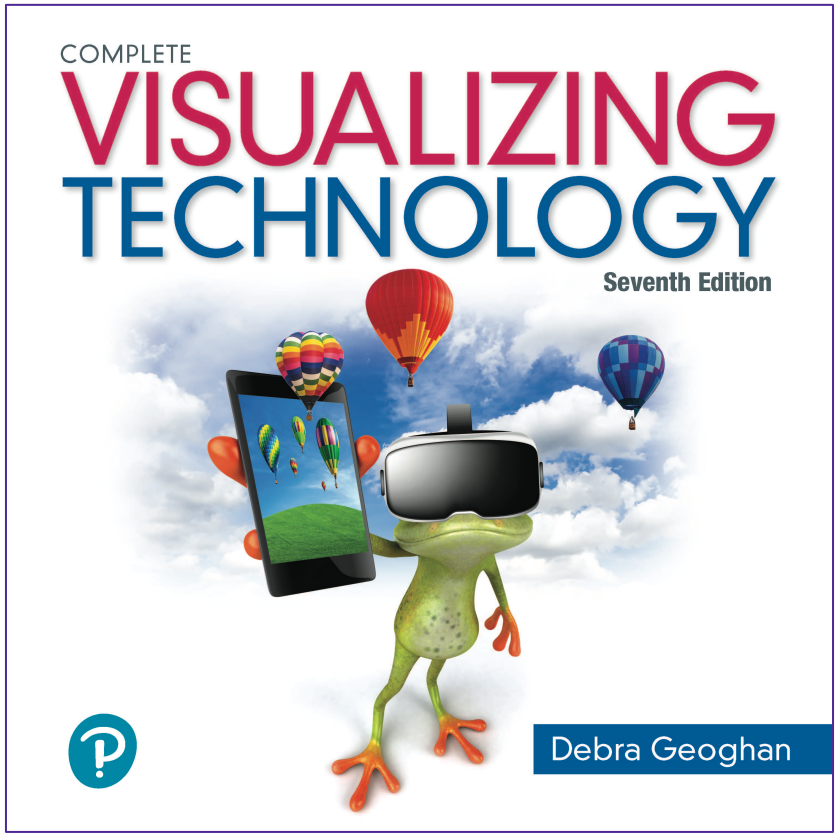
Introductory Visualizing Technology

Seventh Edition



Chapter 10

Security and Privacy

Pearson

Learning Objectives

10.1 Recognize Different Types of Cybercrime

10.2 Differentiate between Various Types of Malware

10.3 Explain How to Secure a Computer

10.4 Practice Safe Computing

10.5 Discuss Laws Related to Computer Security and Privacy

Learning Objective 10.1

- Recognize Different Types of Cybercrime

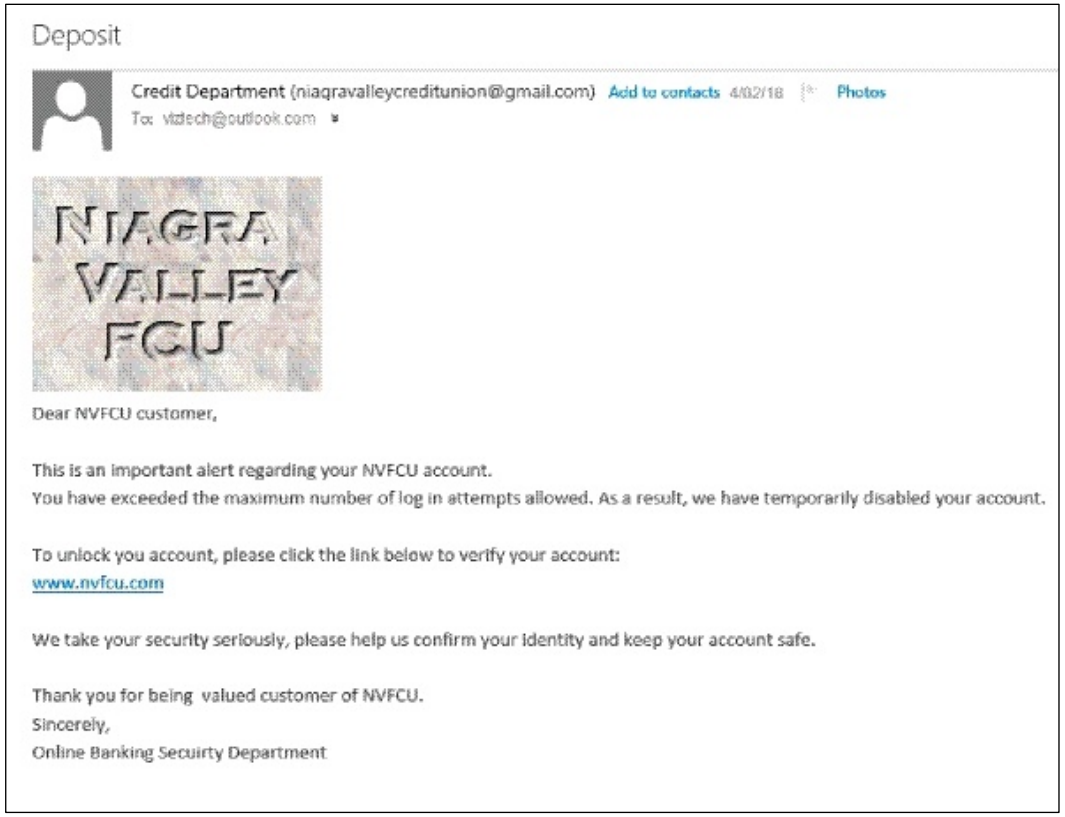
Recognize Different Types of Cybercrime

Cybercrime: They Are Out to Get You—Personal Cybercrime (1 of 2)

- Harassment
  - Cyberbullying: between two minors
  - Cyber-harassment: between adults
  - Cyber-stalking
    - More serious in nature
    - Stalker demonstrates a pattern of harassment
    - Stalker poses a credible threat of harm

Cybercrime: They Are Out to Get You—Personal Cybercrime (2 of 2)

- Phishing
  - Email messages and IMs
  - Appear to be from someone with whom you do business
  - Designed to trick you into providing usernames and passwords
- Pharming
  - Redirects you to a phony website even if you type the URL
  - Hijacks a company's domain name


Deposit

Credit Department (niagravalleycreditunion@gmail.com) Add to contacts 4/02/18 Photos
To: vizitech@outlook.com

NIAGRA VALLEY FCU

Dear NVFCU customer,

This is an important alert regarding your NVFCU account.
You have exceeded the maximum number of log in attempts allowed. As a result, we have temporarily disabled your account.

To unlock you account, please click the link below to verify your account:
www.nvfcu.com

We take your security seriously, please help us confirm your identity and keep your account safe.

Thank you for being valued customer of NVFCU.
Sincerely,
Online Banking Secuirty Department

Cybercrime: They Are Out to Get You—Social Network Attacks (1 of 4)

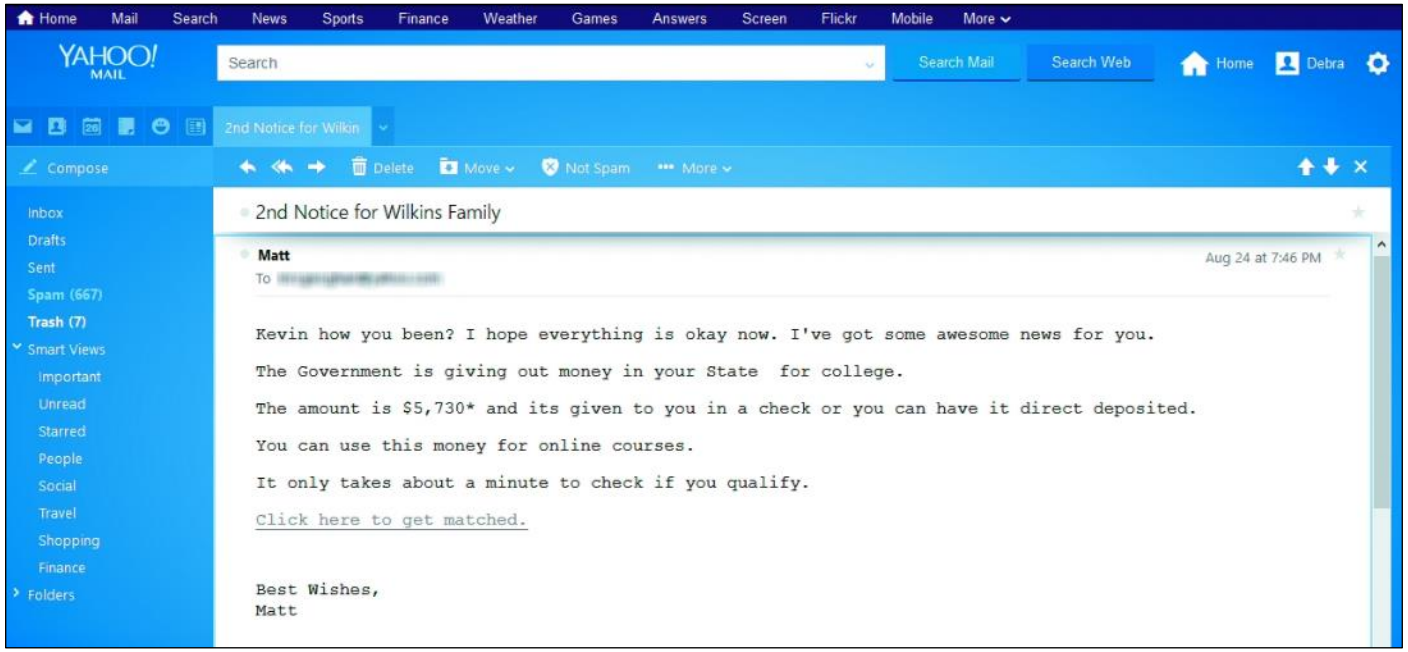
- Adware and other malware
- Suspicious emails and notifications
  - Appear to be from a site administrator
    - Asking for your password
    - Threatening to suspend your account
- Phishing and "Please send money" scams

Cybercrime: They Are Out to Get You—Social Network Attacks (2 of 4)

- Clickjacking
  - Clicking on a link allows this malware to post unwanted links on your page
- Clickbaiting
  - Gets you to click a link, driving traffic to a webpage
- Sharebaiting
  - Sharing unverified posts

Cybercrime: They Are Out to Get You—Social Network Attacks (3 of 4)

- Fraud
  - Schemes that convince you to give money or property to a person
  - Shill bidding is fake bidding to drive up the price of an item



Cybercrime: They Are Out to Get You—Social Network Attacks (4 of 4)

- Identity theft
  - The use of your name, Social Security number, or bank or credit cards for financial gain
  - Keyloggers
    - Programs or devices that capture what is typed

Cybercrime: They Are Out to Get You—Cybercrime Against Organizations (1 of 2)

- Hacking
  - White-hat or “sneakers”
    - Attempt to find security holes in a system to prevent future hacking
  - Black-hat or “crackers”
    - Malicious intent
  - Gray-hat
    - Illegal but not malicious intent

Cybercrime: They Are Out to Get You—Cybercrime Against Organizations (2 of 2)

- Hacktivism
  - Hacking to make a political statement
- Data breach
  - Sensitive data is stolen or viewed by an unauthorized person
- Cyber-terrorism

Learning Objective 10.2

- Differentiate between Various Types of Malware

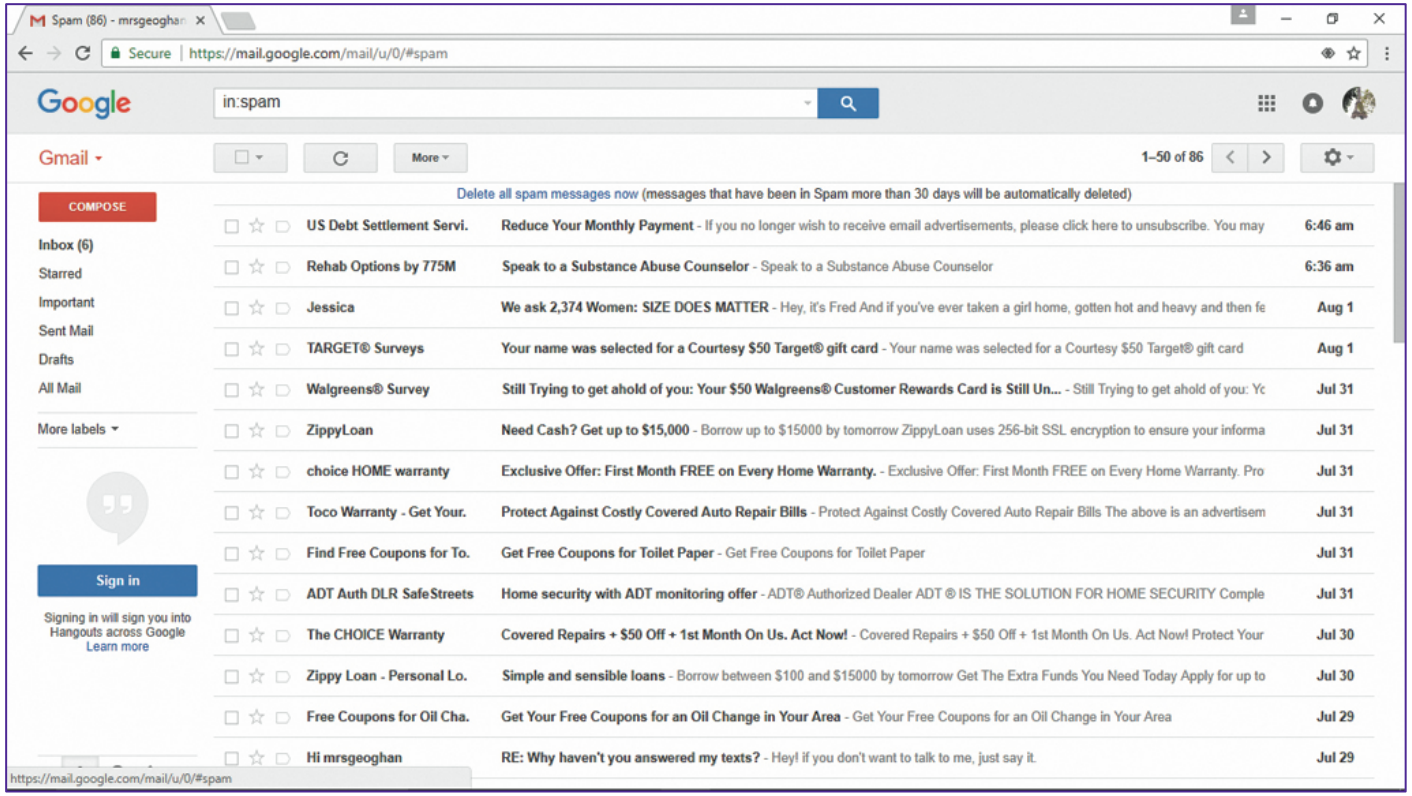
Differentiate between Various Types of Malware

Malware: Pick Your Poison

- Different types of programs designed to be harmful or malicious
  - Spam
  - Adware and spyware
  - Viruses
  - Worms
  - Trojan horses
  - Rootkits

Malware: Pick Your Poison—Spam and Cookies (1 of 2)

- Spam
  - Spamming is sending mass unsolicited emails
  - Messages are called spam
  - Other forms
    - Fax spam
    - IM spam
    - Text spam



Malware: Pick Your Poison—Spam and Cookies (2 of 2)

- Cookies
  - Installed without your permission
  - Help websites identify you when you return
    - Track websites and pages you visit to better target ads
    - May collect information you don't want to share

Malware: Pick Your Poison—Adware and Spyware (1 of 2)

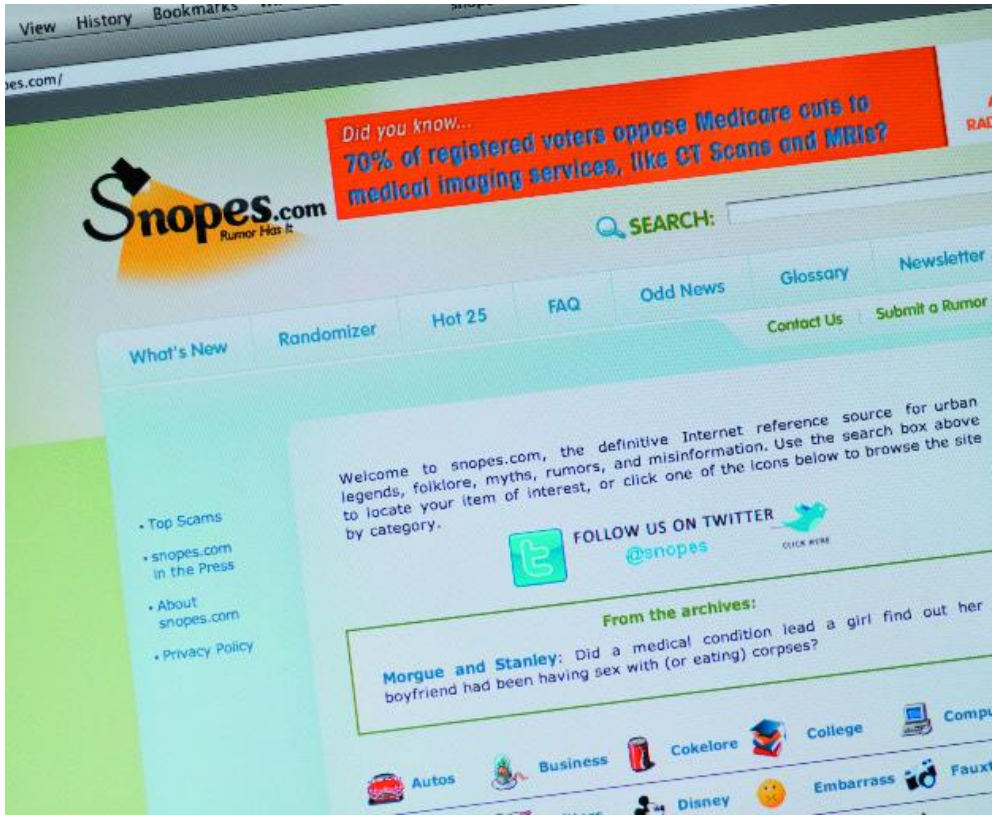
- Adware
  - Pop-ups or banner ads
  - Generate income
  - Use CPU cycles and Internet bandwidth
  - Reduce PC performance

Malware: Pick Your Poison—Adware and Spyware (2 of 2)

- Spyware
  - Malware
  - Secretly gathers personal information
  - Usually installed by accident
  - Browser hijacker

Malware: Pick Your Poison—Viruses, Worms, Trojans, and Rootkits (1 of 7)

- Virus - program that replicates itself and infects computers
  - Needs a host file
  - May use an email program to infect other computers
  - The attack is called the payload
  - Check to see if message is a hoax



Malware: Pick Your Poison—Viruses, Worms, Trojans, and Rootkits (2 of 7)

- Logic or time bomb
  - Behaves like a virus
  - Performs malicious act
  - Does not replicate
  - Attacks when certain conditions are met
    - An employee name is removed
    - April Fool's Day

Malware: Pick Your Poison—Viruses, Worms, Trojans, and Rootkits (3 of 7)

- Worms
  - Self-replicating
  - Do not need a host to travel
  - Travel over networks to infect other machines
  - Conficker worm
    - First released in 2008
    - Reemerged in 2010 with new behaviors

Malware: Pick Your Poison—Viruses, Worms, Trojans, and Rootkits (4 of 7)

- Botnet
  - Network of computer bots controlled by a master
  - Fake security notifications
  - Denial-of-service attacks
    - Use excessive traffic to cripple a server or network

Malware: Pick Your Poison—Viruses, Worms, Trojans, and Rootkits (5 of 7)

- Trojan horse
  - Appears to be legitimate program
  - Actually malicious
  - Might install adware, a toolbar, or a keylogger, or open a backdoor

Malware: Pick Your Poison—Viruses, Worms, Trojans, and Rootkits (6 of 7)

- Ransomware
  - Malware that prevents computer use until a fine or fees paid
  - Bitcoin is an anonymous, digital, encrypted currency

Malware: Pick Your Poison—Viruses, Worms, Trojans, and Rootkits (7 of 7)

- Rootkit
  - Set of programs
  - Allows someone to gain control over system
  - Hides the fact that the computer has been compromised
  - Nearly impossible to detect
  - Masks behavior of other malware

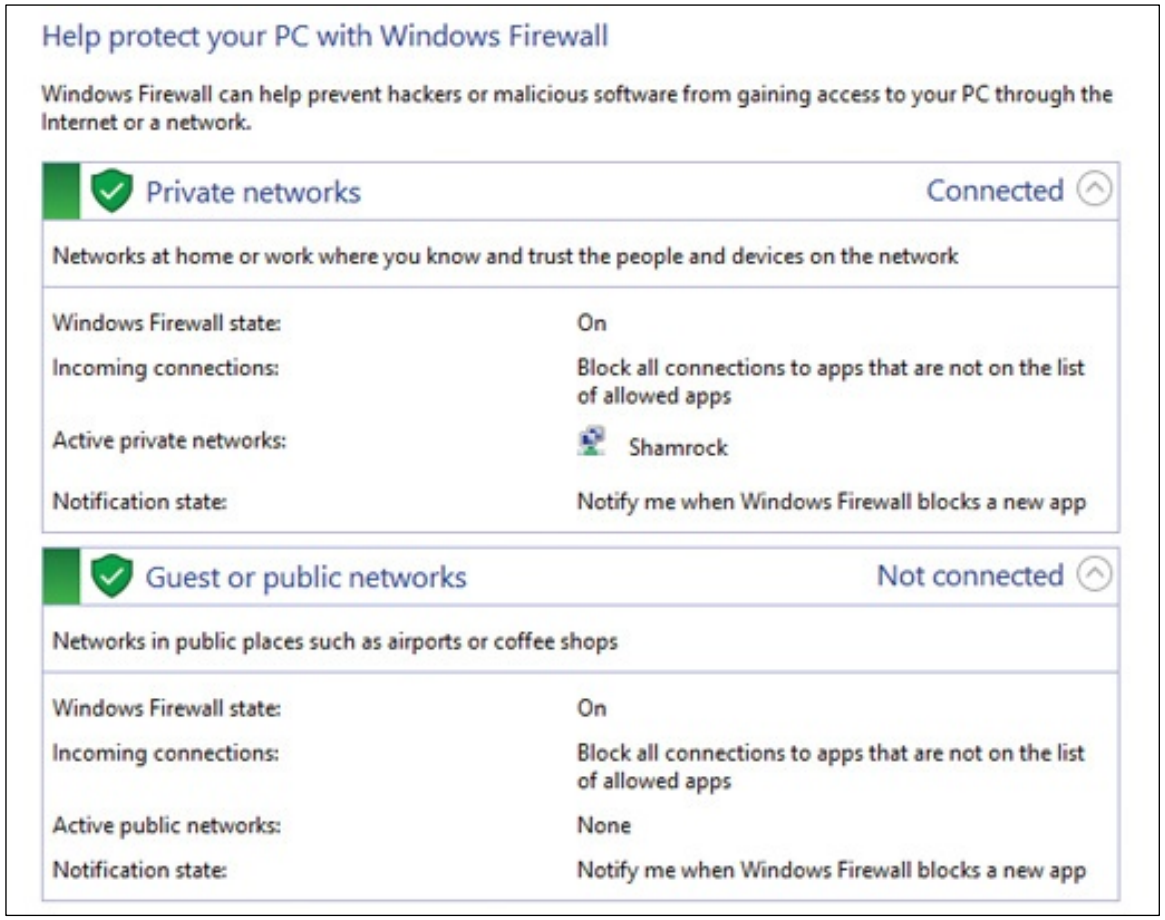
Learning Objective 10.3

- Explain How to Secure a Computer

Explain How to Secure a Computer

Shield's Up – Software (1 of 2)

- Drive-by download
  - Visited website installs a program without your knowledge
- Firewall
  - Hardware device that blocks access to your network
  - Software that blocks access to an individual machine



Shield's Up – Software (2 of 2)

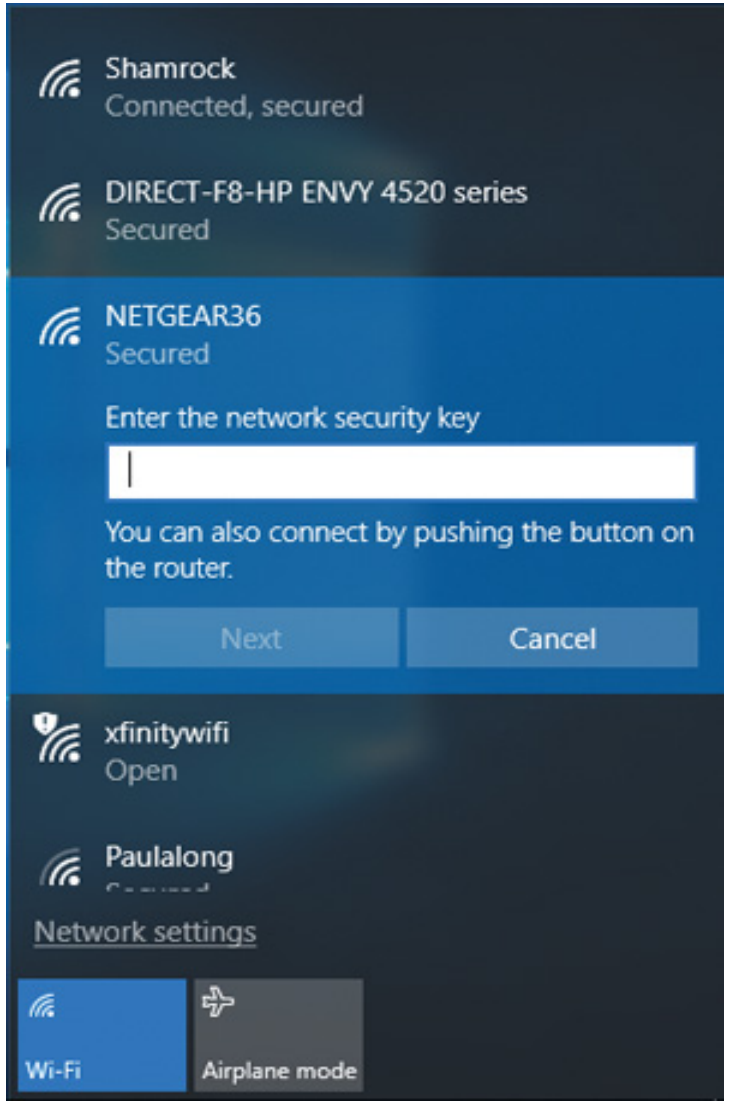
- Antivirus program
  - Protects against viruses, Trojans, worms, spyware
- Antispyware software
  - Prevents adware and spyware from installing
- Security suite
  - Package of security software
  - Combination of features

Shield's Up – Hardware (1 of 2)

- Router
  - Connects two or more networks together
  - Home router acts like firewall
- Network address translation
  - Router security feature
  - Shields devices on private network from the public network

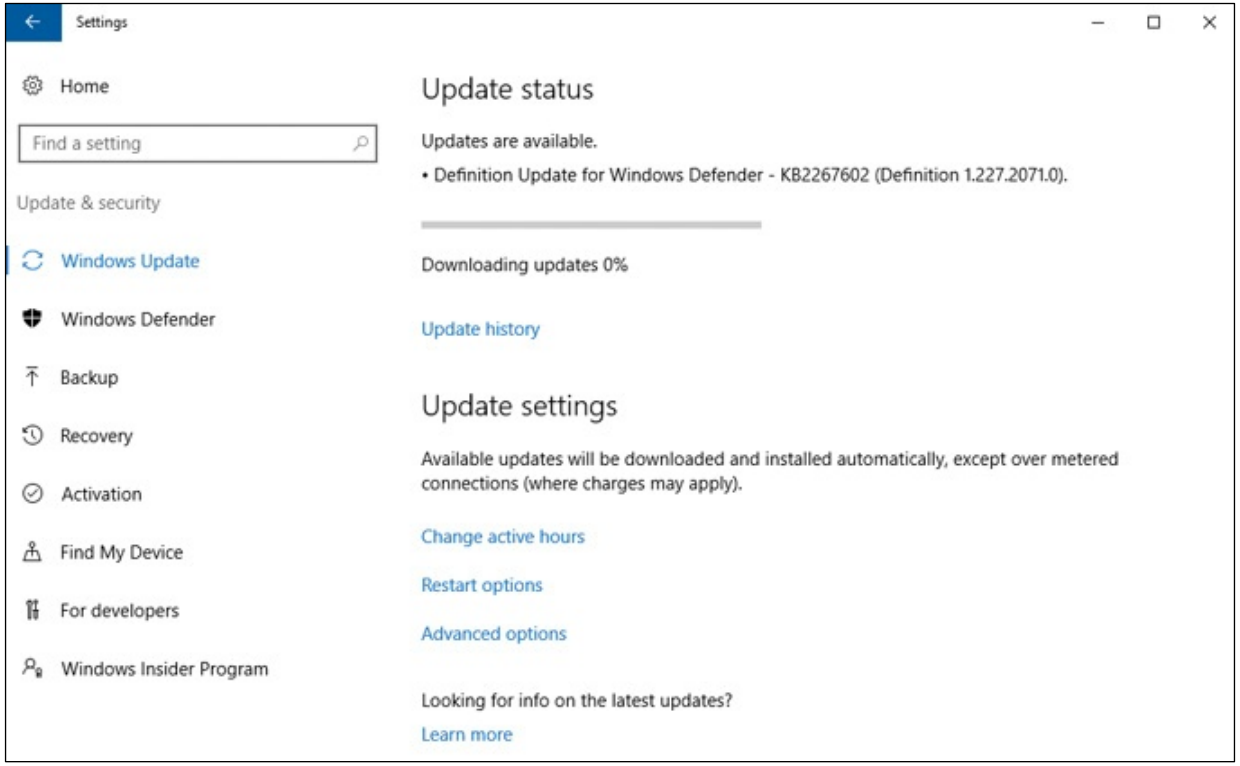
Shield's Up – Hardware (2 of 2)

- SSID (service set identifier)
  - Wireless network name
- Wireless encryption
  - Adds security by encrypting transmitted data
  - Wi-Fi Protected Setup (WPS) is one option



Shield's Up – Operating System

- Most important piece of security software
- Keep patched and up-to-date



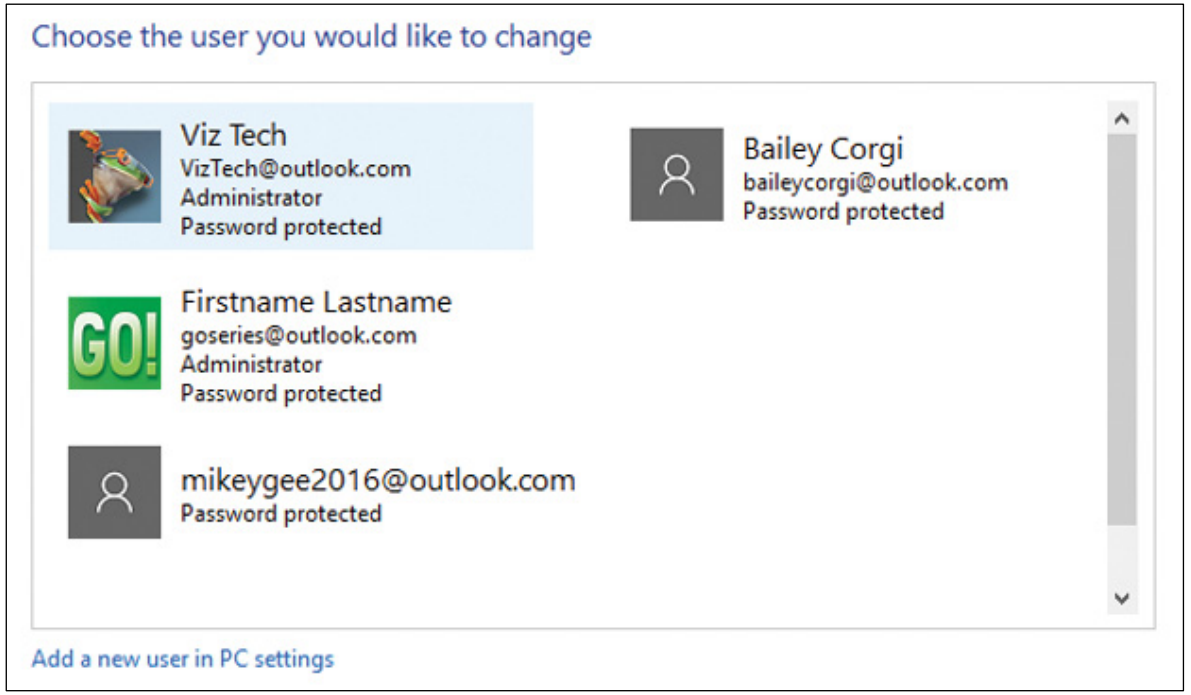
Learning Objective 10.4

- Practice Safe Computing

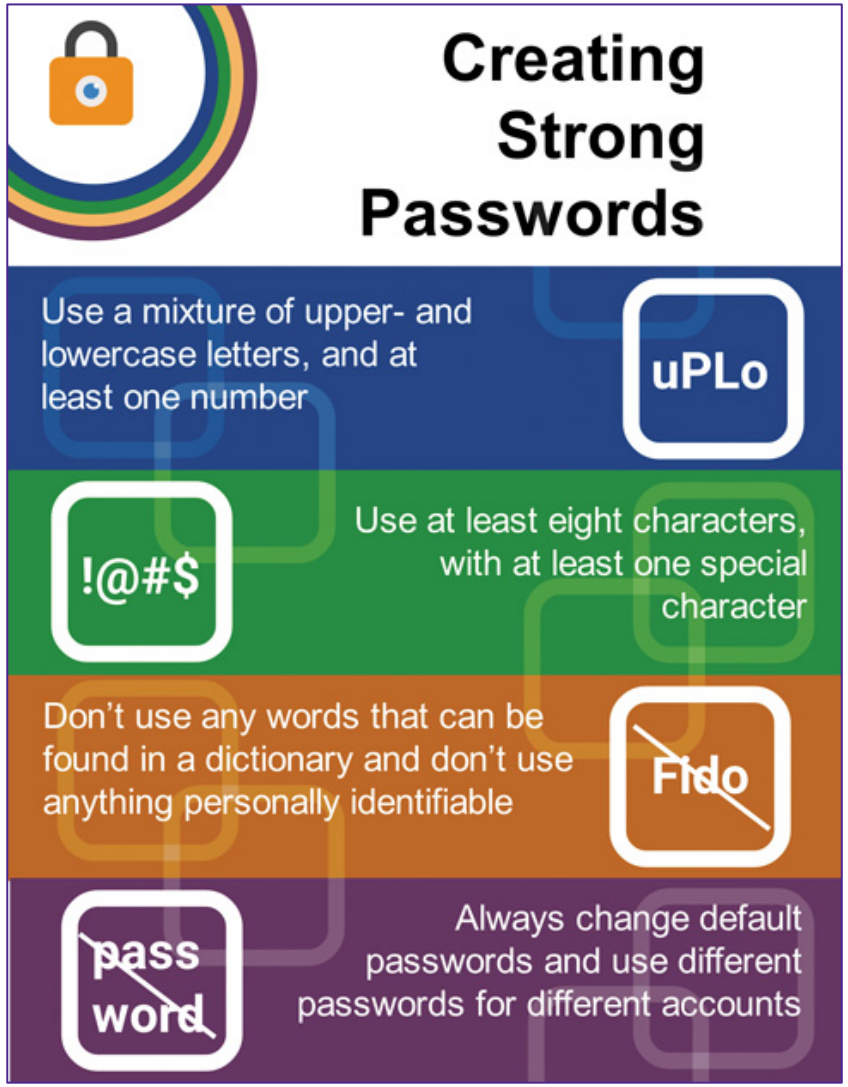
Practice Safe Computing

An Ounce of Prevention is Worth a Pound of Cure—User Accounts

- Three user account types
  - Standard
  - Administrator
  - Guest
- User Account Control notifies you before changes made to your computer
  - Do not turn this feature off
- Malware tricks users into clicking fake Windows notifications

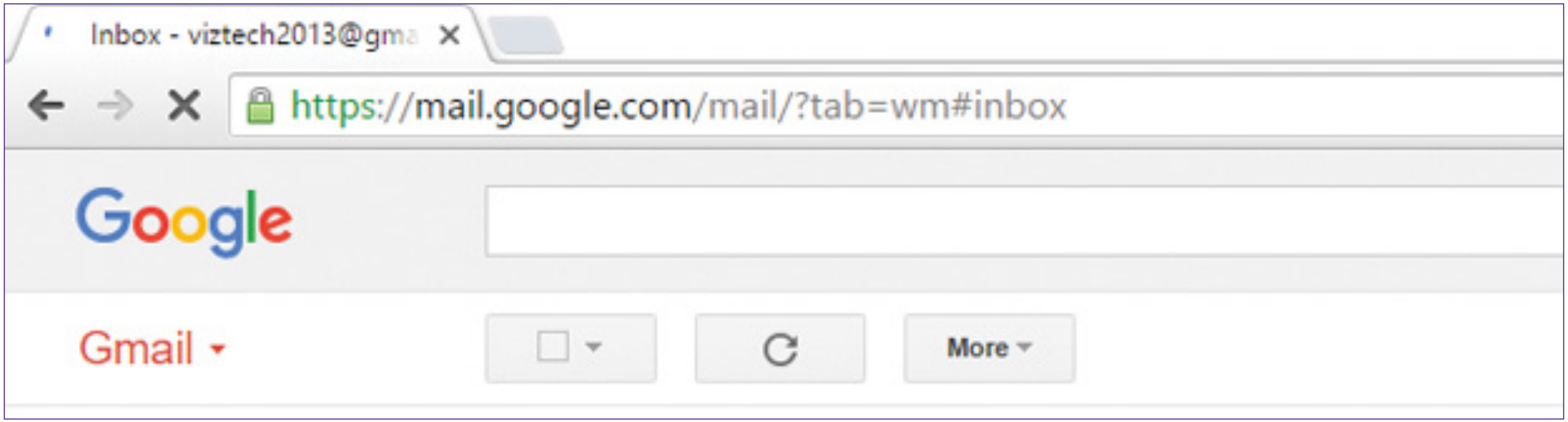


An Ounce of Prevention is Worth a Pound of Cure—— Passwords



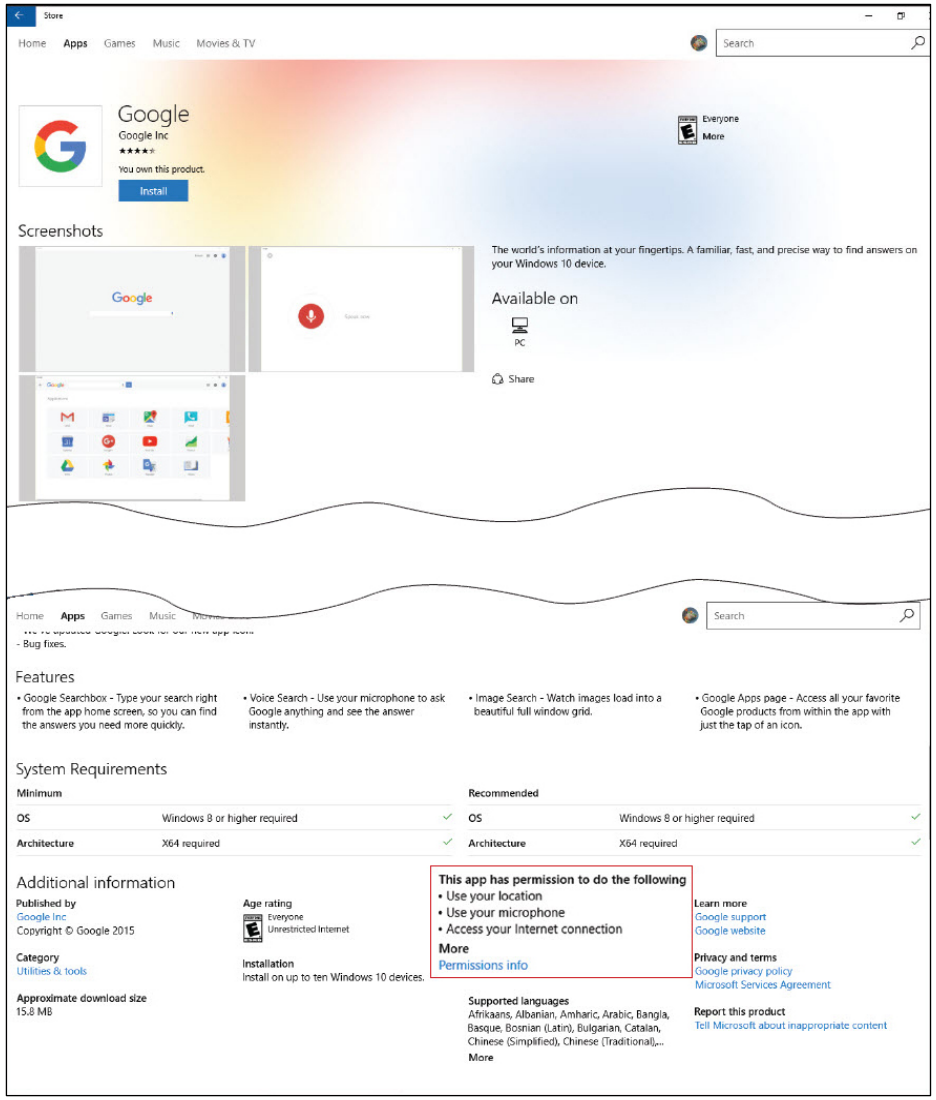
An Ounce of Prevention is Worth a Pound of Cure—Encryption

- Converts plain text into ciphertext
- Must have a key to decrypt it



An Ounce of Prevention is Worth a Pound of Cure—Safely Installing Software

- Copies files to the computer
- Alters settings

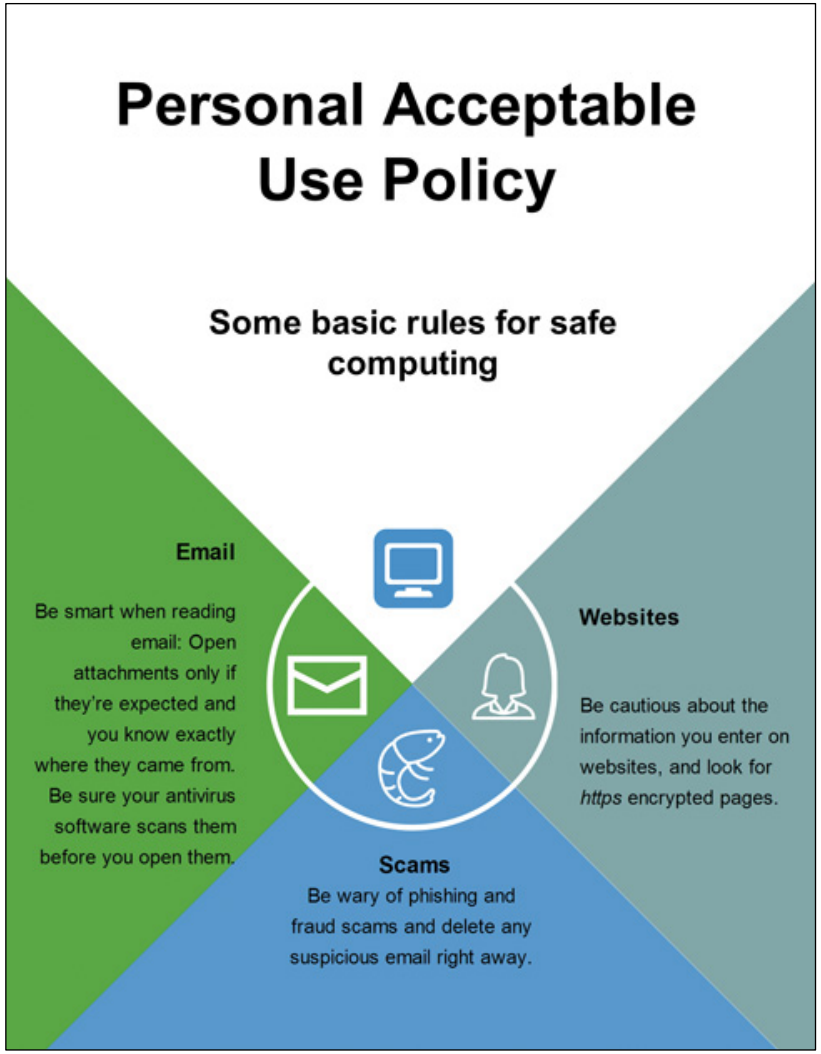


An Ounce of Prevention is Worth a Pound of Cure—Updating and Installing Software

- Protect yourself from downloading problems
  - Only download from reliable sources
- Zero-day exploit
  - Attack that occurs on the day an exploit is discovered, before the publisher can fix it
- Bugs are flaws in the programming of software and are fixed by:
  - Patch or hotfix
  - Service pack

An Ounce of Prevention is Worth a Pound of Cure—Acceptable Use Policies (AUP)

- Common in businesses and schools
- Rules for computer and network users
- Depend on:
  - Type of business
  - Type of information
- Force users to practice safe computing



Learning Objective 10.5

- Discuss Laws Related to Computer Security and Privacy

Discuss Laws Related to Computer Security and Privacy

The Law Is on Your Side—The Enforcers

- No single authority responsible for investigating cybercrime
- Internet Crime Complaint Center (IC3)
  - Place for victims to report cybercrimes
  - ic3.gov
  - Reports processed and forwarded to appropriate agency

The Law Is on Your Side—Current Laws (1 of 2)

- Computer Fraud and Abuse Act
  - Makes it a crime to access classified information
  - Passed in 1986; amendments between 1988 and 2002 which included additional cybercrimes
- USA PATRIOT Act antiterrorism legislation (2001)

The Law Is on Your Side—Current Laws (2 of 2)

- Cyber Security Enhancement Act (2002)
  - Provisions for fighting cybercrime
- Convention on Cybercrime Treaty
  - Drafted by Council of Europe
  - Signed by more than 40 countries

Questions

Copyright