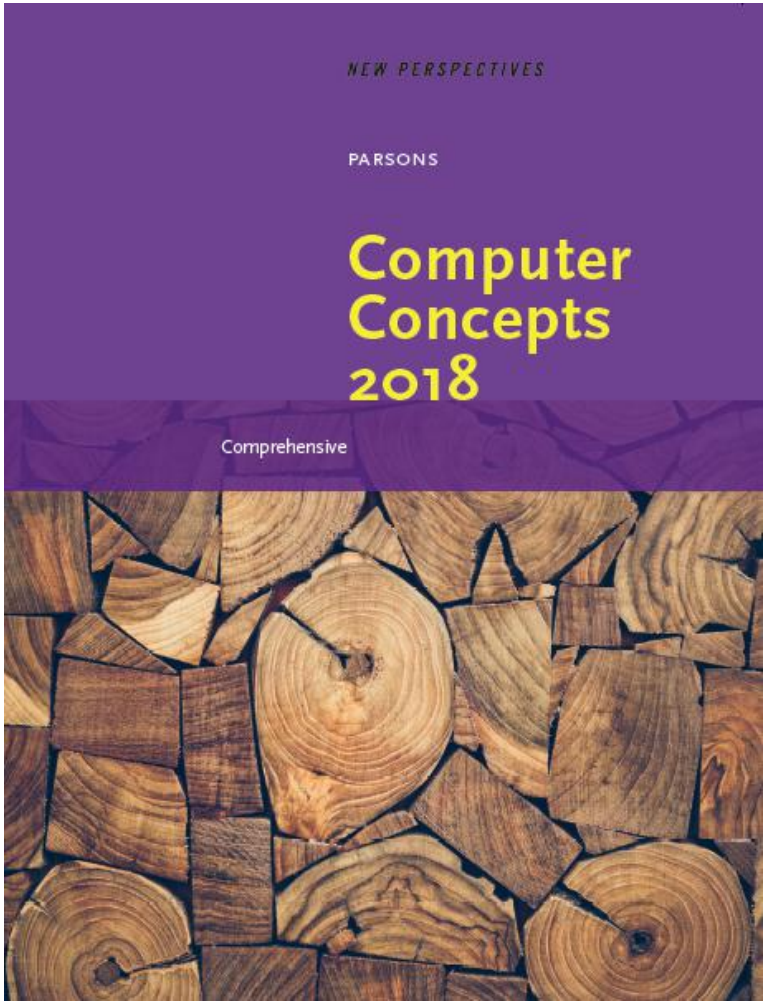
Computer Concepts 2018



Module 7
Digital Security

Module Contents

- Section A: Basic Security
- Section B: Malware
- Section C: Online Intrusions
- Section D: Interception
- Section E: Social Engineering

Section A: Unauthorized Use

- Encryption
- Authentication
- Passwords
- Password Managers

Section A: Objectives (1 of 2)

- List five examples in which digital data is encrypted for security purposes
- Describe how two-factor authentication works when you log in to a Gmail account from a device you have never used before
- Explain how encryption is linked to passcodes in some digital devices
- Describe the advantages of encrypting an entire storage volume
- Recite the basic rules for creating a strong password

Section A: Objectives (2 of 2)

- List at least five characteristics of weak passwords
- Recite the formula for calculating the number of possible passwords that can be generated using a four-digit PIN
- Explain the concept of password entropy
- Describe the advantages and disadvantages of local, cloud-based, and USB password managers

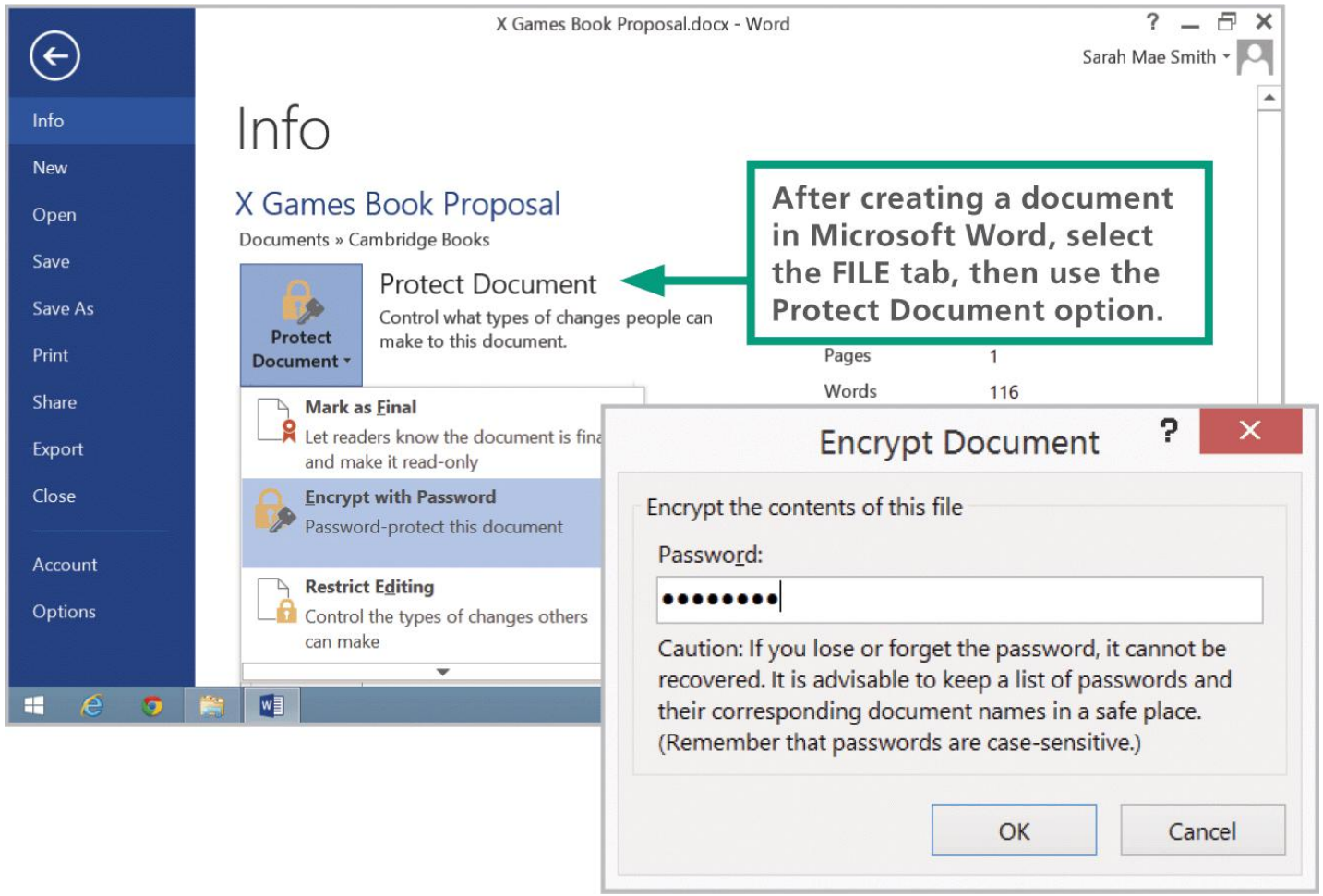
Encryption (1 of 3)

- **Encryption** transforms a message or data file in such a way that its contents are hidden from unauthorized readers
- An original message or file that has not yet been encrypted is referred to as **plaintext** or cleartext
- An encrypted message or file is referred to as **ciphertext**
- The process of converting plaintext into ciphertext is called encryption; the reverse process—converting ciphertext into plaintext—is called **decryption**

Encryption (2 of 3)

- Data is encrypted by using a cryptographic algorithm and a key
  - A **cryptographic algorithm** is a procedure for encryption or decryption
  - A **cryptographic key** (usually just called a key) is a word, number, or phrase that must be known to encrypt or decrypt data
- There are various encryption methods, and some are more secure than others; **AES** (Advanced Encryption Standard) is the encryption standard currently used worldwide

Encryption (3 of 3)



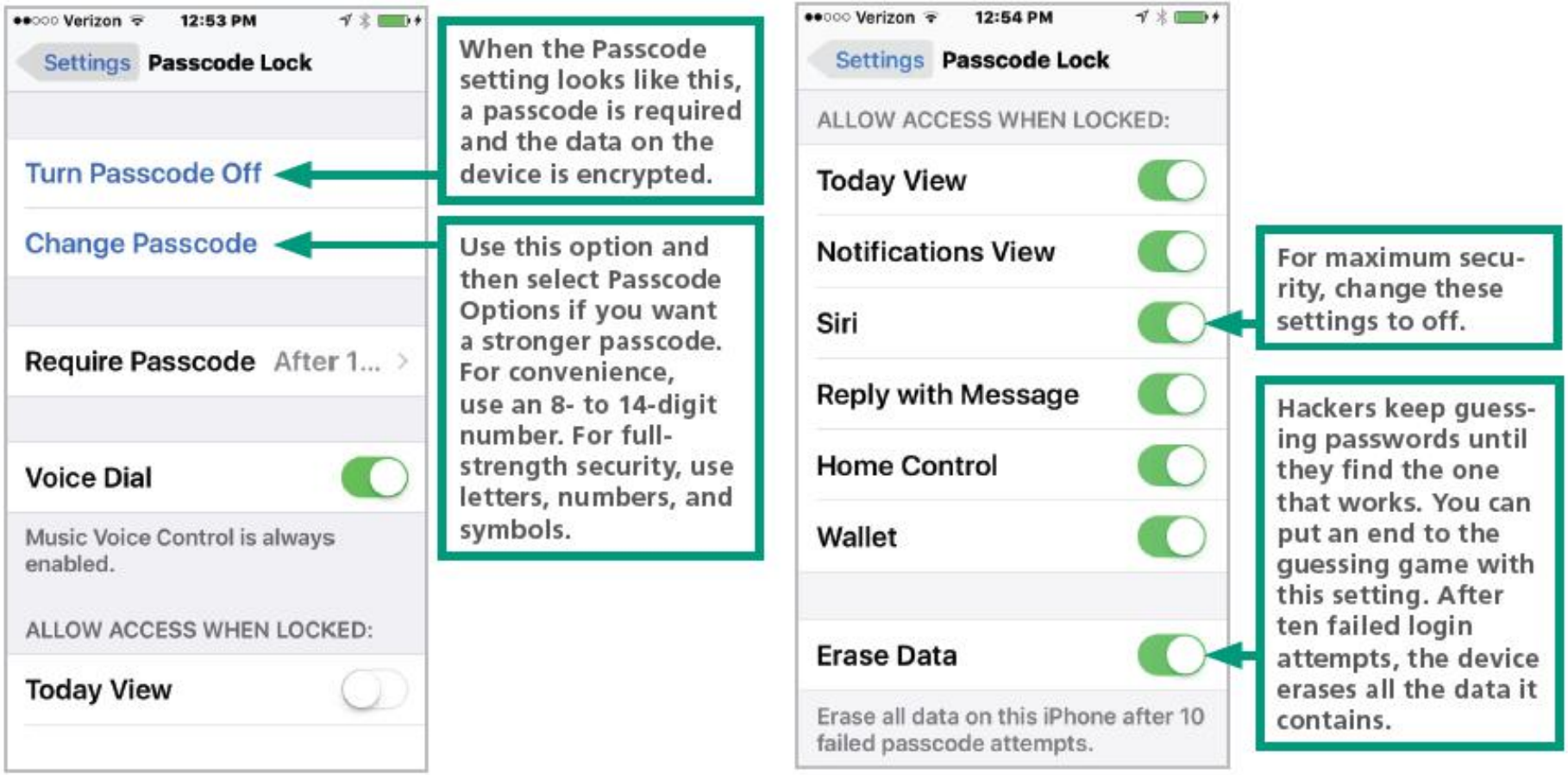
Authentication (1 of 4)

- **Authentication protocols**, such as passwords, PINs, and fingerprint scans and facial recognition are the first line of defense against data thieves and snoopers
- iPhones and iPads should be configured to require a login password, called a passcode, each time the device is used; the standard iOS security setting establishes a four-digit numeric passcode, similar to a PIN (personal identification number)

Authentication (2 of 4)

- Android devices have an overwhelming number of security settings; Android devices do not automatically encrypt data stored on the device when a user activates the login password; configuring a password and activating encryption are two separate steps

Authentication (3 of 4)



Authentication (4 of 4)

- Windows offers several password options that can be configured using the Accounts utility, which is accessed from the Start menu or Control panel; Windows devices can be encrypted using Microsoft's BitLocker or third-party utilities
- Macs offer several password settings, which are accessed from the Security & Privacy preferences; a feature called Automatic Login allows access to a device without a password

Strong Passwords (1 of 10)

- A **strong password** is difficult to hack; conventional wisdom tells us that strong passwords are *at least eight characters* in length and include one or more *uppercase letters*, *numbers*, and *symbols*

Strong Passwords (2 of 10)

- A **brute force attack** uses password-cracking software to generate every possible combination of letters, numerals, and symbols. Because it exhausts all possible combinations to discover a password, it can run for days before a password is cracked
- A **dictionary attack** helps hackers guess your password by stepping through a dictionary containing word lists in common languages such as English, Spanish, French, and German

Strong Passwords (3 of 10)

- Dictionary attacks are effective because many users choose passwords that are easy to remember and likely to be in the most commonly used list

12345	000000	buster	coffee	eeyore
abc123	money	dragon	dave	fishing
password	carmen	jordan	falcon	football
p@sswOrd	mickey	michael	freedom	george
Pa55word	secret	michelle	gandalf	happy
passwordl	summer	mindy	green	iloveyou
!qaz2wsx	internet	patrick	helpme	jennifer
computer	service	123abc	linda	jonathan
123456	canada	andrew	magic	love

Strong Passwords (4 of 10)

111111	hello	calvin	merlin	marina
a1b2c3	ranger	changeme	molson	master
qwerty	shadow	diamond	newyork	missy
adobe123	baseball	matthew	soccer	monday
123123	donald	miller	thomas	monkey
admin	harley	ou812	wizard	natasha
1234567890	hockey	tiger	Monday	ncc1701
photoshop	letmein	12345678	asdfgh	newpass
1234	maggie	apple	bandit	pamela
sunshine	mike	avalon	batman	
azerty	mustang	brandy	boris	
trustno1	snoopy	chelsea	dorothy	

Strong Passwords (5 of 10)

- Many of the clever schemes users devise to create passwords are obvious to hackers and the programmers who create password-cracking tools
- **Weak passwords include the following:**
  - Words from a dictionary, including words that are in languages other than English
  - Doubled words such as passpass or computercomputer
  - Default passwords such as password, admin, system, and guest
  - Sequences of numbers formatted as dates or telephone numbers, such as 01/01/2000 and 888-5566

Strong Passwords (6 of 10)

- Words with a sequence of numbers at the end, such as Secret123 and Dolphins2018
- Words with symbol or numeric mutations, such as p@ssw0rd and V01dem0rt
- Any sequence that includes a user name, such as BillMurray12345
- Any sequence that uses conventional capitalization, such as Book34 and Savannah912

Strong Passwords (7 of 10)

- **Start with a phrase.** Base your high-security password on the first letters of a phrase that generates a password containing numbers and proper nouns.
  - Aim for a length of 8 to 12 characters because some sites limit password length.
  - Use uppercase letters somewhere other than at the beginning of the password.
  - Use numbers somewhere other than at the end of the password.
  - Some sites do not allow symbols, so you may not want to use them in a password that will be modified for use on many sites.

Strong Passwords (8 of 10)

Here is an example of a phrase that produces a fairly secure password:

I went to Detroit Michigan when I was 23 years old
IwtDMwiw23yo

- **Add the site name.** By inserting the name of the site, every password will be unique and you will be able to remember the site on which it is used, like this:

I went to PayPal when I was 23 years old
IwtPayPalwiw23yo

Strong Passwords (9 of 10)

- **Make a low-security password.** A password achieves pretty good entropy when it is composed of four or more words. Create an everyday password using this method. Here is an example: **SpaBraidAmazonNuit**
- **Be careful what you write.** If you have to write down your passwords to remember them, keep them in a safe place that is not connected to your digital device. If your device is stolen, the passwords should not be located where they would also be stolen.

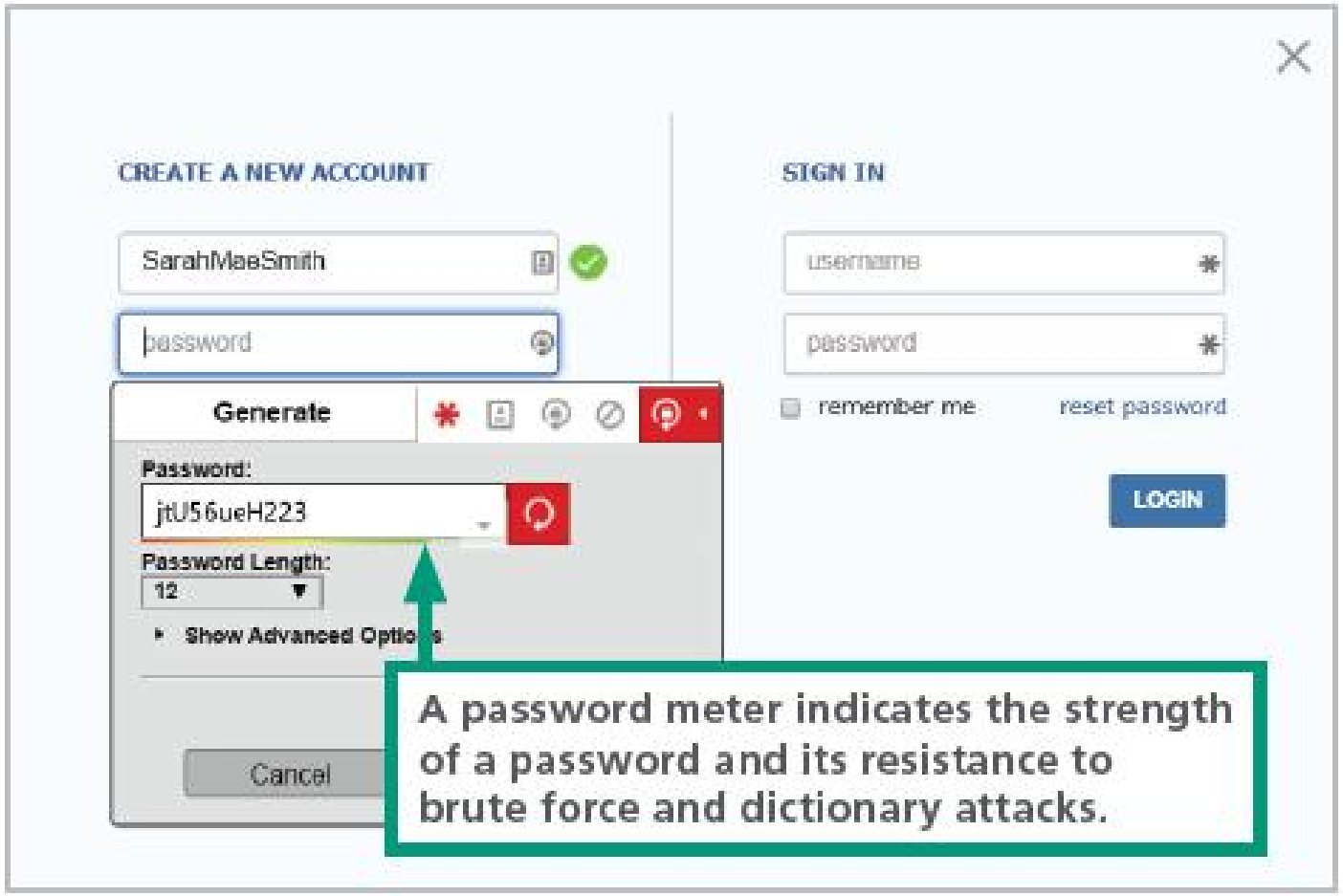
Strong Passwords (10 of 10)

- **Use encryption.** If you want to store passwords on your device, make sure to encrypt the file in which they are stored.
- **Use a password manager.** If you feel more secure with a totally random and unique password for each of your logins, a password manager is an excellent option.

Password Managers (1 of 2)

- The core function of a **password manager** (sometimes called a keychain) is to store user IDs with their corresponding passwords
- Password managers may also include a **strength meter** that indicates password security—a feature that is useful if you create a custom password rather than using one generated by the password manager

Password Managers (2 of 2)



Section B: Malware

- Malware Threats
- Computer Viruses
- Computer Worms
- Trojans
- Antivirus Software

Section B: Objectives (1 of 2)

- List at least five examples of malware payloads
- Describe the characteristics that differentiate computer viruses from other types of malware
- Explain the purpose of a rootkit
- Describe the characteristics of computer worms and list three common infection vectors
- Explain the purpose of malware trojans and how they relate to droppers
- List the two ways that antivirus software is able to detect viruses

Section B: Objectives (2 of 2)

- Explain the three possible actions that antivirus software can take when a virus is detected
- Explain the significance of false positives in the context of virus detection
- Describe how to determine if an email warning about a virus is real or a hoax

Malware Threats (1 of 3)

- **Malware** refers to any computer program designed to surreptitiously enter a digital device
- The action carried out by malware code is referred to as a **malware exploit** or **payload**
- Common classifications of malware include:
  - Viruses
  - Worms
  - Trojans

Malware Threats (2 of 3)

- Display irritating messages and pop-up ads Delete or modify your data
- Encrypt data and demand ransom for the encryption key
- Upload or download files
- Record keystrokes to steal passwords and credit card numbers
- Send messages containing malware and spam to everyone in an email address book or instant messaging buddy list
- Disable antivirus and firewall software

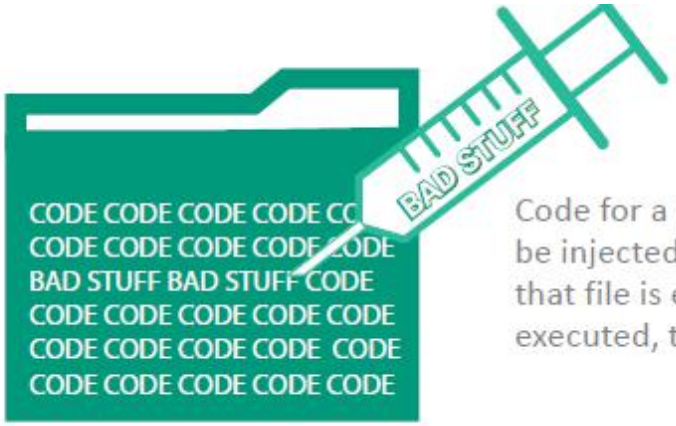
Malware Threats (3 of 3)

- Block access to specific Web sites and redirect a browser to infected Web sites Cause response time slowdowns
- Allow hackers to remotely access data stored on a device
- Allow hackers to take remote control of a device and turn it into a zombie
- Link a device to others in a botnet that can send millions of spam emails or wage denial-of-service attacks against Web sites
- Cause network traffic jams

Computer Viruses (1 of 3)

- A **computer virus** is a set of self-replicating program instructions that surreptitiously attaches itself to a legitimate executable file on a host device
- Today, viruses are a mild threat; they do not spread rapidly, and they are easily filtered out by antivirus software
- Viruses reveal the basic techniques that are still used to inject third-party code into legitimate data streams
- **Code injection** is the process of modifying an executable file or data stream by adding additional commands

Computer Viruses (2 of 3)



Code for a virus or other malware can be injected into a legitimate file. When that file is executed, the virus code is executed, too.

Malicious code can also be injected into a data stream as it travels from one device to another. After the altered data arrives, it is typically stored and eventually executed.

Computer Viruses (3 of 3)

- Viruses spread when people exchange infected files on disks and CDs, as email attachments, and on file sharing networks; they can also be inadvertently obtained from unauthorized app stores
- Through a process called **side-loading**, an app from a source other than an official app store is installed on a device
- Any code that is designed to hide the existence of processes and privileges is referred to as a **rootkit**; these were originally designed to allow “root” or administrative access to digital devices and computer systems

Computer Worms (1 of 2)

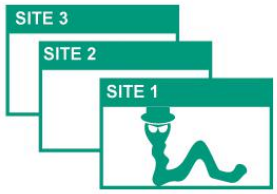
- A **computer worm** is a self-replicating, self-distributing program designed to carry out unauthorized activity on a victim's device
- A **mass-mailing worm** spreads by sending itself to every address in the address book of an infected device
- An **internet worm** looks for vulnerabilities in operating systems, open communication ports, and JavaScripts on Web pages
- A **file-sharing worm** copies itself into a shared folder under an innocuous name

Computer Worms (2 of 2)

The worm sends a copy of itself as an email attachment.

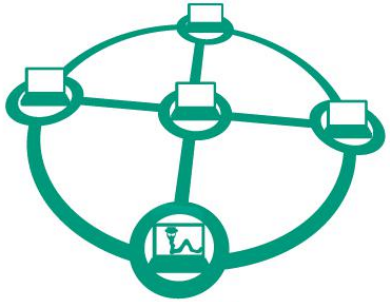
Open the attachment, and the worm is copied to your device.

The worm scans the Web looking for exploitable HTML pages.



Visit the Web site, and the worm is downloaded to your device.

The worm looks for open ports for file sharing in a LAN.



Connect to the network, and the worm is transmitted to your device.

Trojans (1 of 2)

- A **trojan** (sometimes called a “Trojan Horse”) is a computer program that seems to perform one function while actually doing something else. Most trojans are not designed to replicate themselves
- A **dropper** is designed to deliver or “drop” malicious code into a device; they are usually the first phase of a sophisticated malware attack

Trojans (2 of 2)

1. A USB drive containing the Stuxnet dropper in disguise is inserted into a computer.

2. A security hole in Windows runs the dropper when the USB directory is viewed.

3. The dropper executes a second file containing a worm.

4. The worm spreads through the LAN, looking for a specific type of hardware device that Stuxnet is designed to destroy.

5. When the worm arrives at a target device, in this case a centrifuge, it downloads a more comprehensive file containing instructions for the payload.

6. The malware payload causes the nuclear centrifuges to fail.

Antivirus Software (1 of 8)

- **Antivirus software** is a type of utility software that looks for and eliminates viruses, trojans, worms, and other malware
- A **virus signature** is a section of program code that contains a unique series of instructions known to be part of a malware exploit; they are discovered by security experts who examine the bit sequences contained in malware program code

Antivirus Software (2 of 8)

- Antivirus software can use techniques called **heuristic analysis** to detect malware by analyzing the characteristics and behavior of suspicious files
- Heuristics may produce **false positives** that mistakenly identify a legitimate file as malware

Antivirus Software (3 of 8)

- **Repair.** Antivirus software can sometimes remove the malware code from infected files. This strategy is benefi-cial for files containing important documents that have become infected. Many of today's malware exploits are embedded in executable files and are difficult to remove. When malware cannot be removed, the file should not be used.
- **Quarantine.** In the context of antivirus software, a **quarantined file** contains code that is suspected of being part of a virus. For your protection, most antivirus software encrypts the file's contents and isolates it in a quarantine folder so it can't be inadvertently opened or accessed by a hacker.

Antivirus Software (4 of 8)

Quarantined files cannot be run, but they can be moved out of quarantine if they are later found to have been falsely identified as malware.

- **Delete.** Quarantined files should eventually be deleted. Most antivirus software allows users to specify how long an infected file should remain in quarantine before it is deleted. Most users rarely retrieve files from quarantine because it is risky to work with files that are suspected of harboring malicious code. There is no need, therefore, to delay deletion for more than a few days.

Antivirus Software (5 of 8)

- **For the most extensive protection from malware, you should look for and enable the following features of your antivirus software:**
  - Start scanning when the device boots
  - Scan all programs when they are launched, and scan document files when they are opened
  - Scan other types of files, such as graphics, if you engage in some risky computing behaviors and are not concerned with the extra time required to open files as they are scanned
  - Scan incoming email and attachments
  - Scan incoming instant message attachments

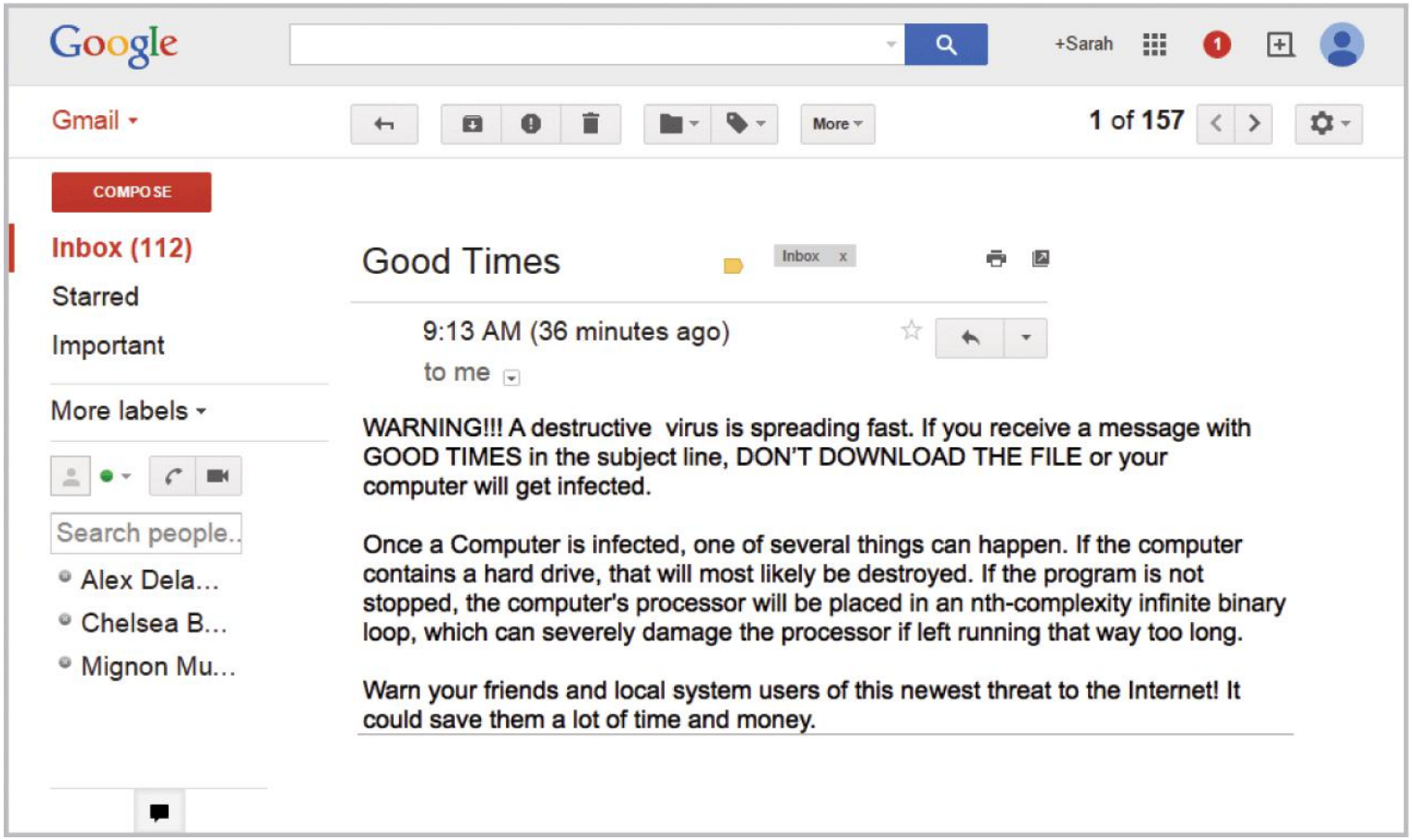
Antivirus Software (6 of 8)

- Scan outgoing email for worm activity such as mass-mailing worms
- Scan zipped (compressed) files.
- Scan for spyware and PUAs (potentially unwanted applications)
- Scan all files on the device's storage volume at least once a week

Antivirus Software (7 of 8)

- Some virus threats are very real, but you're also likely to get email messages about so-called viruses that don't really exist
- A **virus hoax** usually arrives as an email message containing dire warnings about a supposedly new virus on the loose
- Never forward a viral email to others, even if you think it's just a virus hoax

Antivirus Software (8 of 8)



Section C: Online Intrusions

- Intrusion Threats
- Anti-exploit Software
- Netstat
- Firewalls

Section C: Objectives (1 of 2)

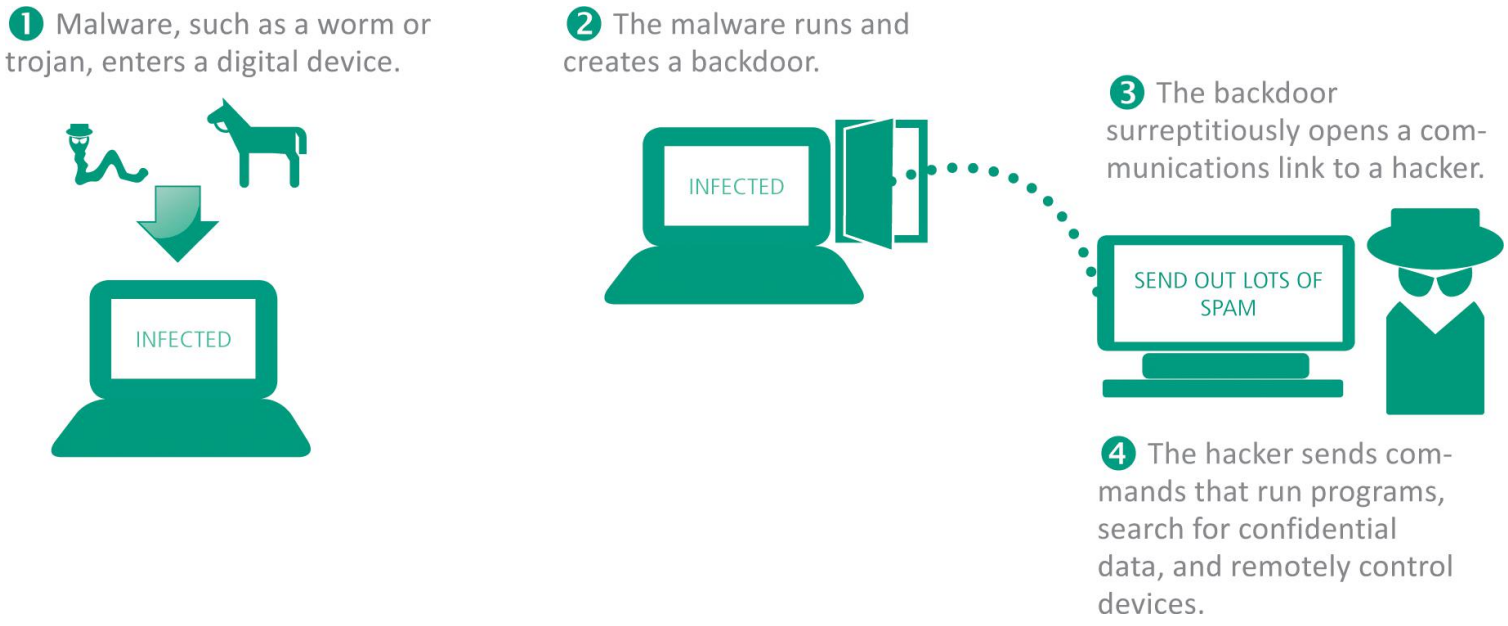
- Provide an overview that describes how an online intrusion takes place.
- List and describe at least seven types of online intrusions
- Explain how a DDoS attack takes place
- Describe the difference between an on-demand scan and on-access scanning
- Summarize the significance of communications ports in online intrusions
- State the purpose of a personal firewall and describe how one works

Section C: Objectives (2 of 2)

- Explain how NAT works in conjunction with a router to provide a hardware firewall
- Explain why security experts recommend using both NAT and a personal firewall
- Describe the security vulnerability associated with remote access utilities

Intrusion Threats (1 of 3)

- An **online intrusion** takes place when an unauthorized person gains access to a digital device by using an Internet connection and exploiting vulnerabilities in hardware or software



Intrusion Threats (2 of 3)

- **Different types of intrusions include:**
  - **RATs** (Remote Access Trojan) – malware that arrives in a trojan disguised as a legitimate software; sets up a secret communication link with the hacker
  - **Backdoor** is an undocumented method of accessing a digital device
  - **Ransomware** – locks a device and then requests payment for an unlocking code; commonly exploits the Find My iPhone feature

Intrusion Threats (3 of 3)

- **Botnets** – a client-server network created by hackers who gain control over several computers; this network is hidden from the victims, who continue to use their devices
- **DDoS (distributed denial of service)** – attacks designed to flood a legitimate Web site or Internet router with so much traffic that it can no longer function

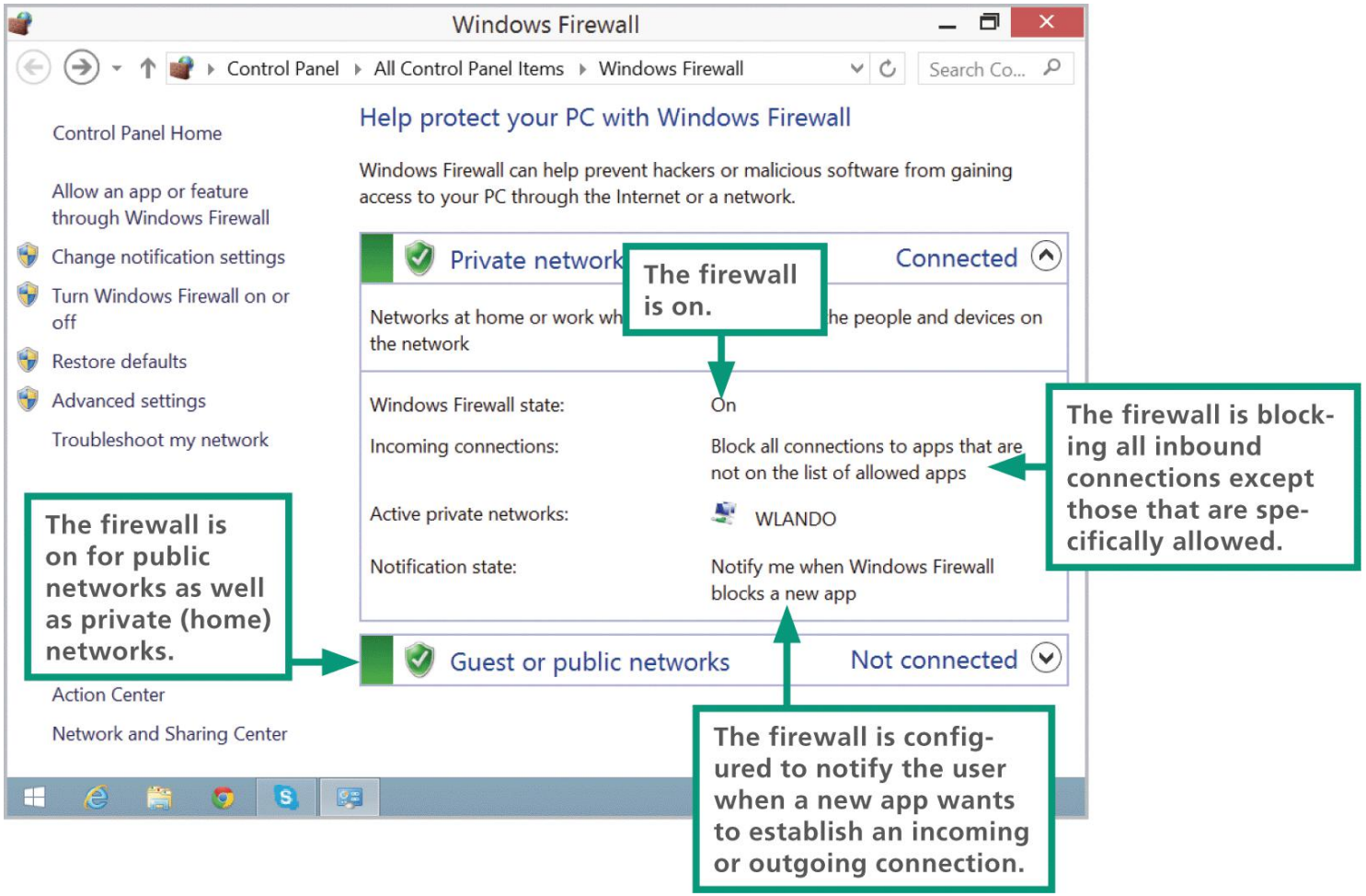
Anti-exploit Software

- A **zero-day attack** exploits previously unknown vulnerabilities in software applications, hardware, and operating system program code
- Anti-exploit security software offers an additional defense against zero-day attacks
- **Anti-exploit software** shields certain applications against behaviors commonly exhibited by intrusions and other exploits

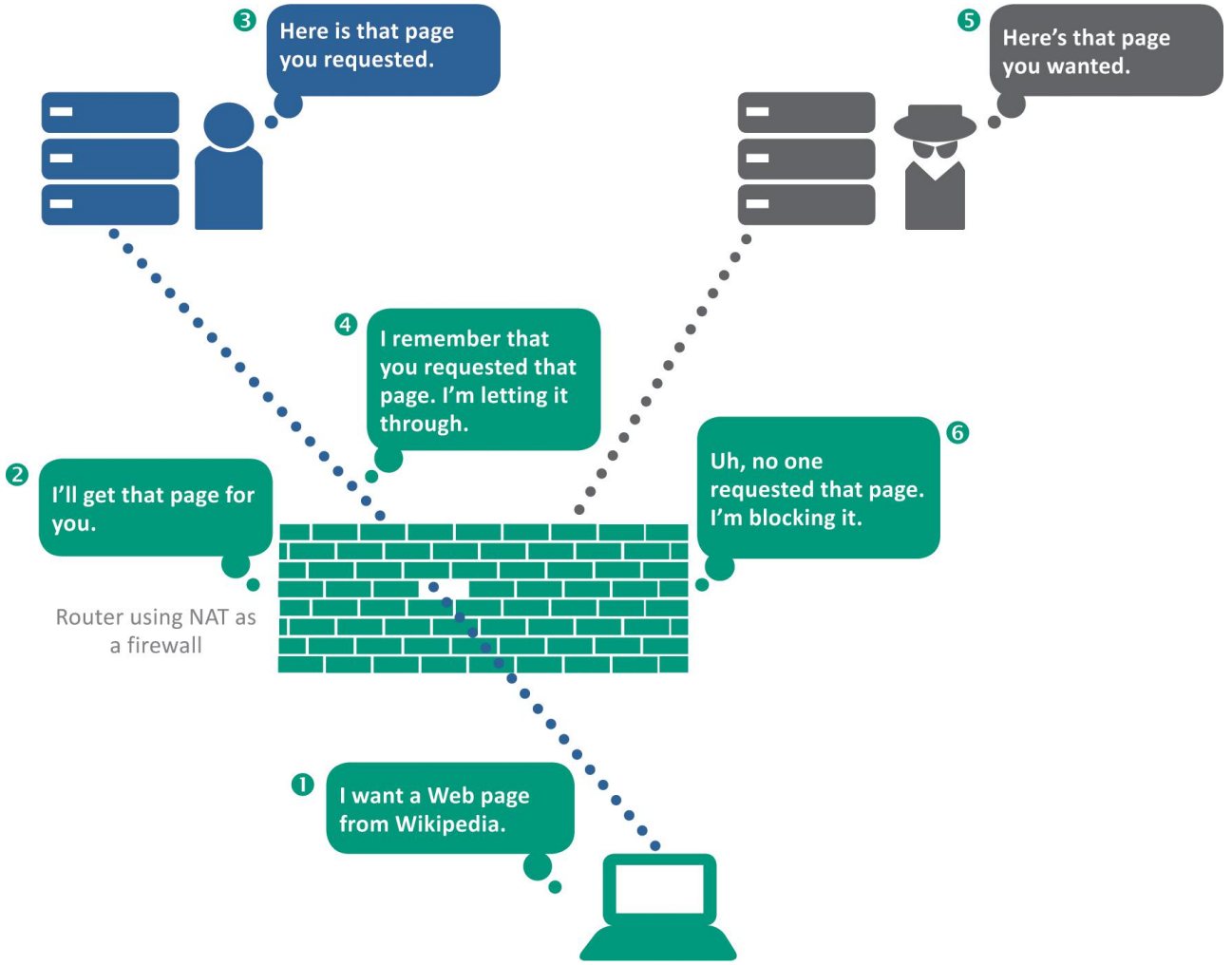
Firewalls (1 of 3)

- A **firewall** is a device or software that is designed to block unauthorized access while allowing authorized communications
- A **personal firewall** uses a set of rules to block data or allow it to enter a digital device
- Most personal firewalls are configured to block all communication unless an app and its corresponding communication port are on a list of allowed exceptions

Firewalls (2 of 3)



Firewalls (3 of 3)



Section D: Interception

- Interception Basics
- Evil Twins
- Address Spoofing
- Digital Certificate Hacks
- IMSI Catchers

Section D: Objectives

- List four types of intercept exploits
- Draw a diagram illustrating a basic man-in-the-middle exploit
- Describe the Evil Twin exploit and how to avoid it
- List four types of address spoofs
- List the three important security components of a digital certificate
- Describe or diagram how a digital certificate encrypts the connection between a client and a server
- Explain how a fake digital certificate can defeat encryption.
- Describe how an IMSI catcher works

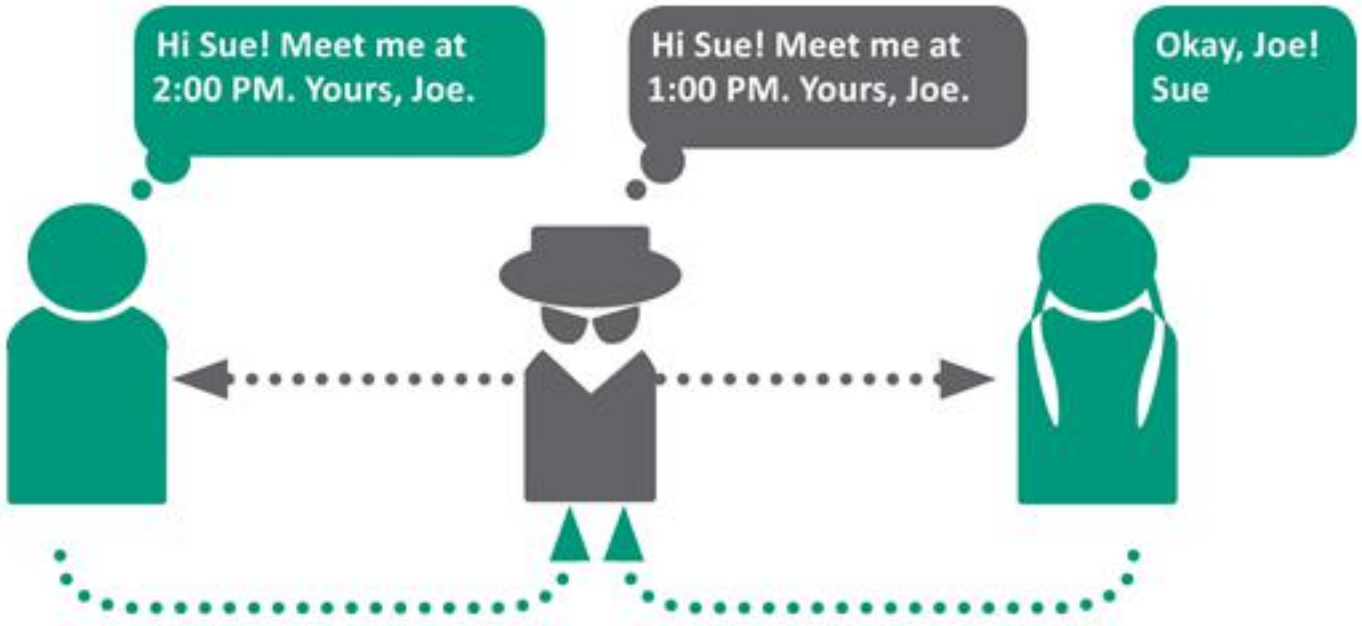
Interception Basics (1 of 3)

- Interception exploits that are current threats to consumers include the following:
  - **Spyware** – any software that secretly gathers personal information without the victim's knowledge
  - **Adware** – monitors Web browsing activity to supply ad-serving sites with data used to generate targeted ads

Interception Basics (2 of 3)

- **Keyloggers** – a common type of spyware, it records keystrokes and sends them to a hacker who sifts out user passwords to access the victim's accounts; often used by identity thieves and industrial spies
- **Man-in-the-Middle** (MITM) – in the context of cyber security, it is an eavesdropping exploit; MITM attacks include Evil Twins, address spoofing, digital certificate hacks, and IMSI catchers

Interception Basics (3 of 3)

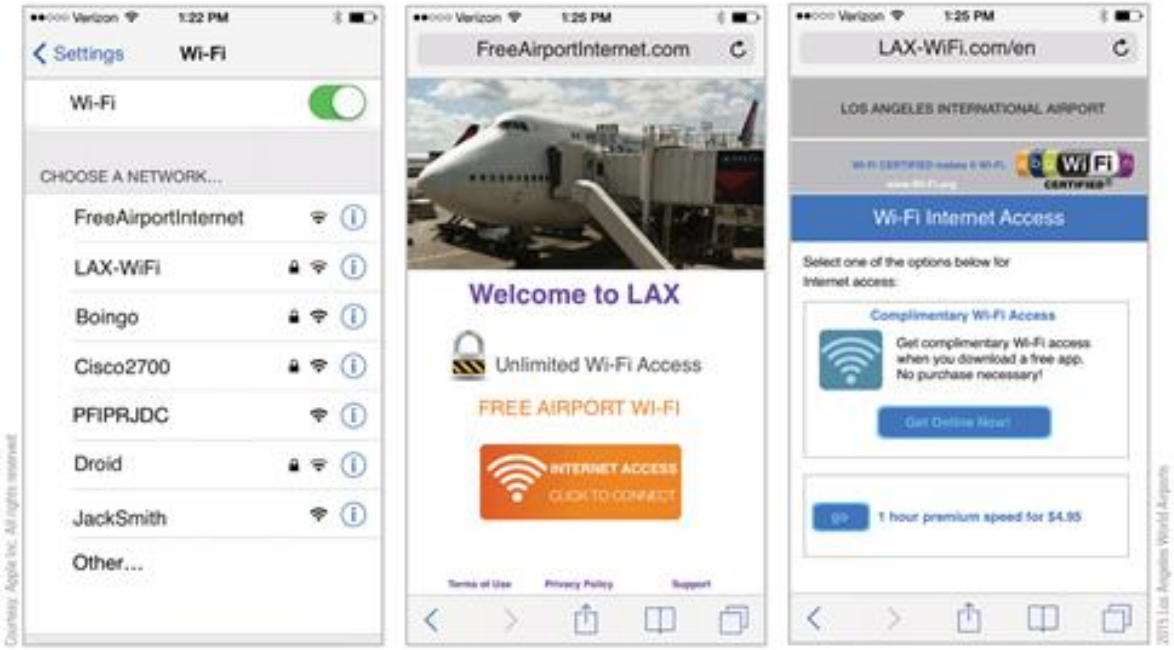


In an MITM attack, two parties believe they are communicating directly with each other when, in fact, they are communicating with a third party.

Evil Twins (1 of 2)

- An **Evil Twin** is a LAN server that is designed to look like a legitimate Wi-Fi hotspot
- Evil Twins are difficult to detect; to avoid this exploit, refrain from entering sensitive data while using any questionable network, and avoid using unsecured networks

Evil Twins (2 of 2)



Three public Wi-Fi services appear to be offered at the LAX airport: FreeAirportInternet, LAX-WiFi, and Boingo. The remaining Wi-Fi hotspots are operated by individuals using their phones as a tethering device. Of the three public Wi-Fi services, FreeAirportInternet is not secured; therefore, it is most likely to be an Evil Twin.

Address Spoofing (1 of 2)

- Broadly speaking, **address spoofing** changes an originating address or a destination address to redirect the flow of data between two parties
- In the context of security exploits, address spoofing can take place on various levels of communication
- **Email address spoof**
  - Changes the sender's address. The spoofed address masks the source of spam.
- **IP address spoof**
  - Modifies the source IP address of data packets used in a denial-of-service attack.

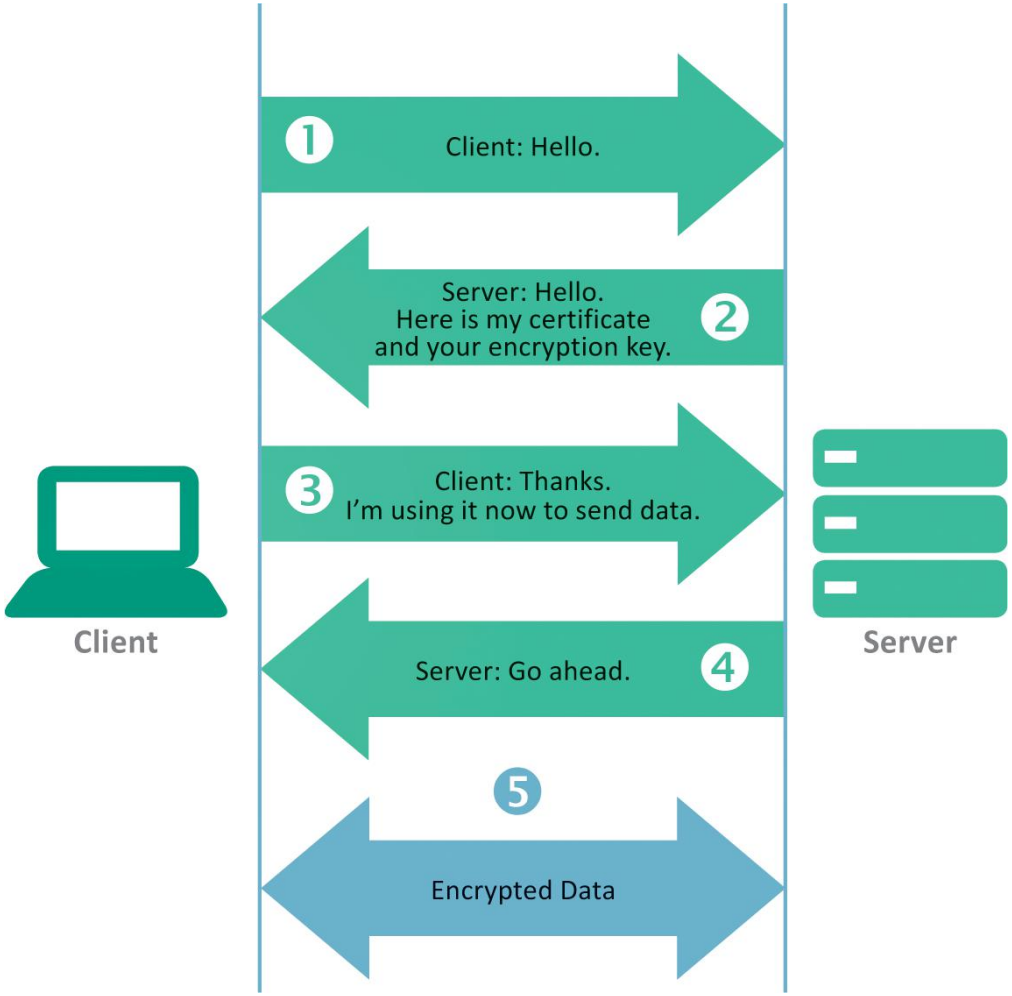
Address Spoofing (2 of 2)

- **DNS address spoof**
  - Changes the IP address that corresponds to a URL. The spoofed URL directs victims to a fraudulent Web site.
- **ARP address spoof**
  - Changes the ARP (Address Resolution Protocol) routing table on a local area network. The spoofed address redirects traffic through a secondary, potentially malicious device.

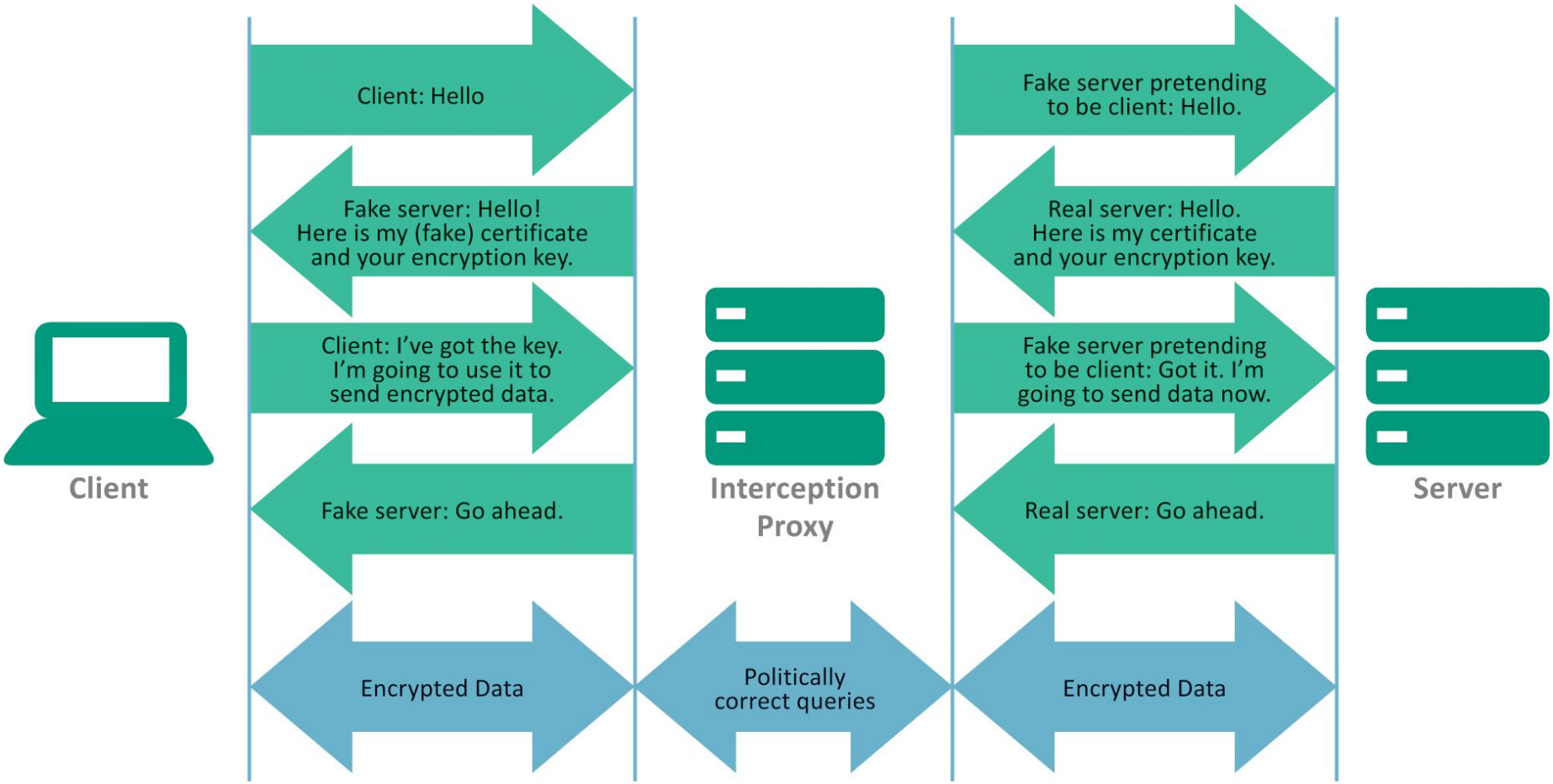
Digital Certificate Hacks (1 of 3)

- The current method of encrypting communication between a client and a server depends on a security protocol called **TLS** (Transport Layer Security)
- TLS checks a **digital certificate** to verify a server's identity and pass a public key to the client
- The client then uses the public key to encrypt data that is sent to the server

Digital Certificate Hacks (2 of 3)



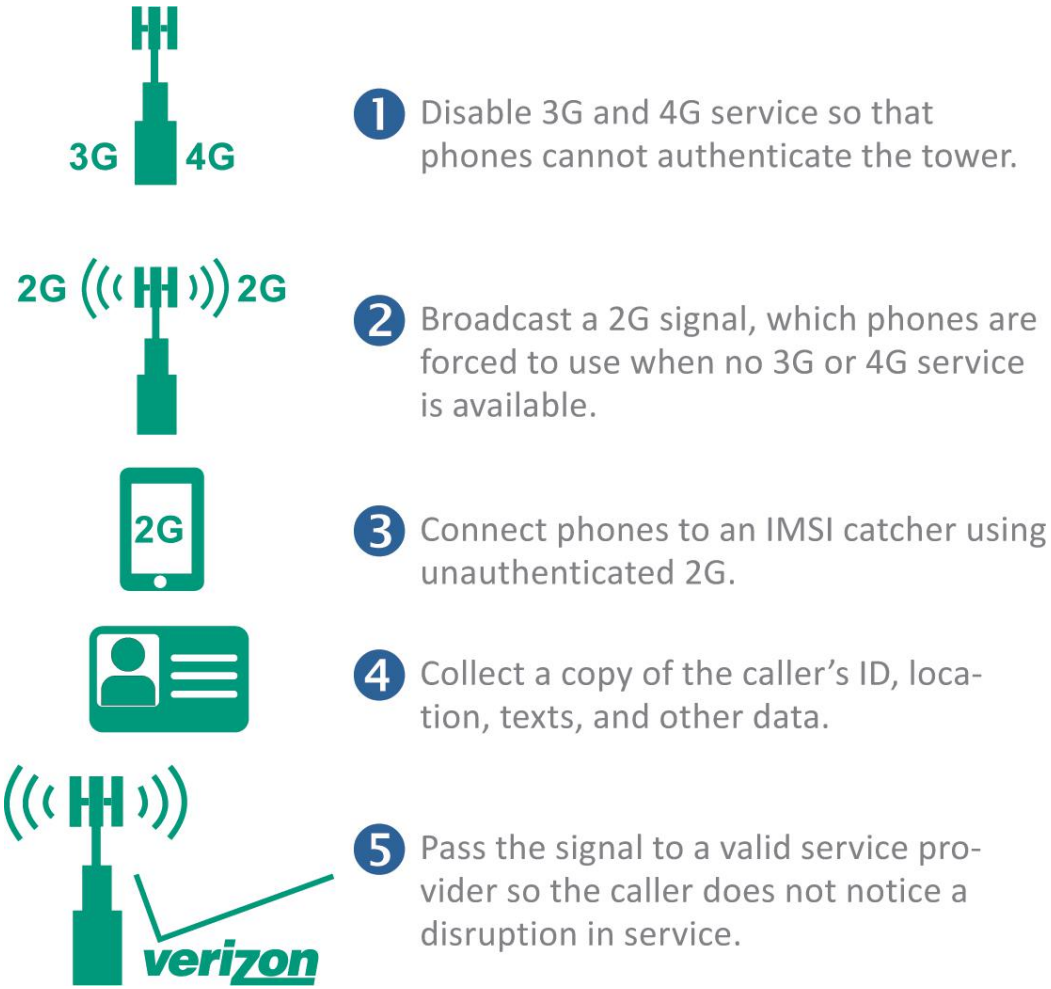
Digital Certificate Hacks (3 of 3)



IMSI Catchers (1 of 2)

- **IMSI** is an acronym for International Mobile Subscriber Identity
- It is a 64-bit number that uniquely identifies a cellular device
- An IMSI catcher is an eavesdropping device used for intercepting mobile phone signals and tracking the location of cellular devices
- IMSI catchers are used for MITM attacks

IMSI Catchers (2 of 2)



1. Disable 3G and 4G service so that phones cannot authenticate the tower.
2. Broadcast a 2G signal, which phones are forced to use when no 3G or 4G service is available.
3. Connect phones to an IMSI catcher using unauthenticated 2G.
4. Collect a copy of the caller's ID, location, texts, and other data.
5. Pass the signal to a valid service provider so the caller does not notice a disruption in service.

Section E: Social Engineering

- Social Engineering Basics
- Spam
- Phishing
- Pharming
- Rogue Antivirus
- PUAs

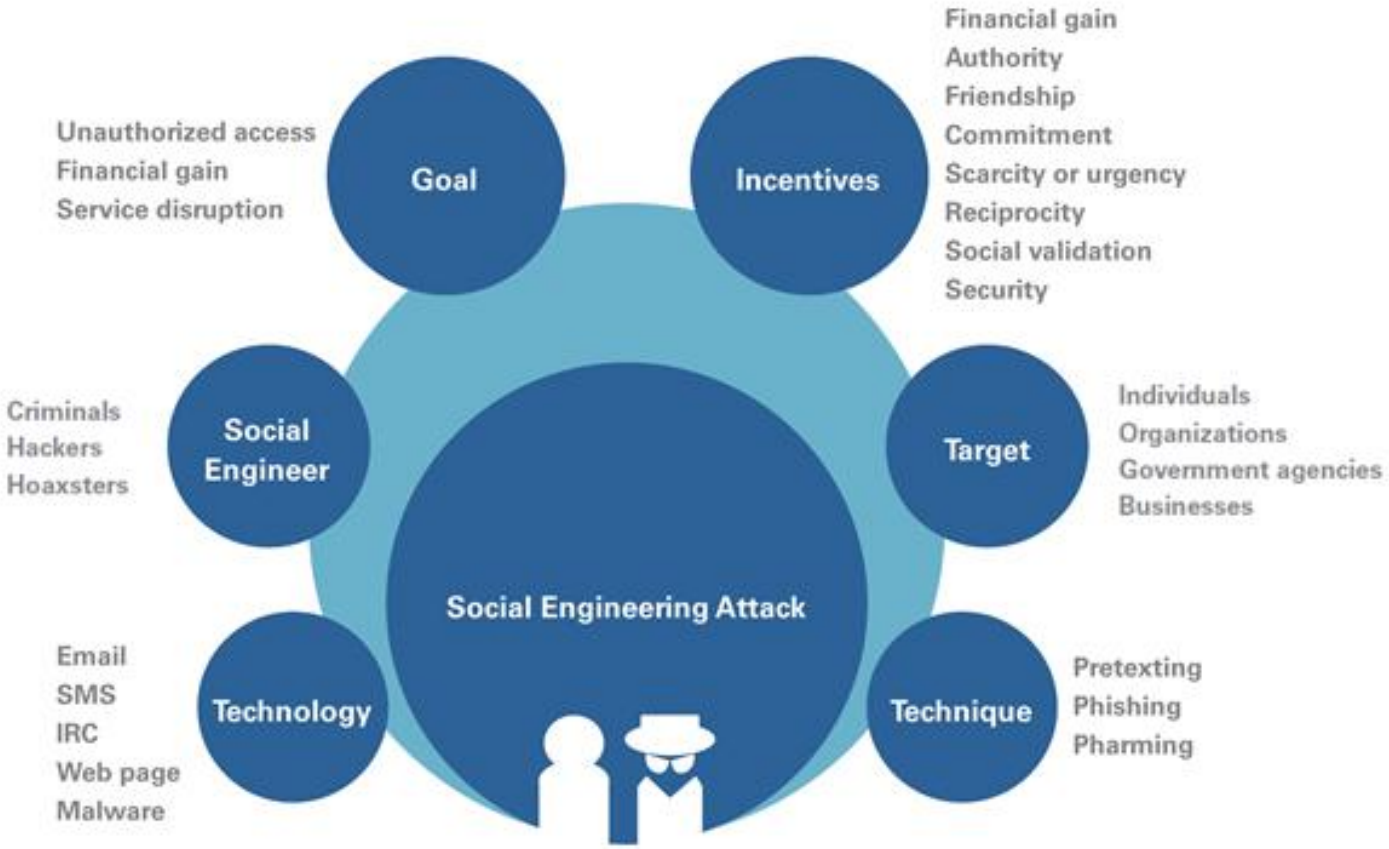
Section E: Objectives

- Create a diagram that illustrates the six elements of a social engineering attack
- Describe advance fee fraud and the stranded traveler scam
- List the three limitations placed on spam by the CAN-SPAM Act of 2003
- List at least six best practices for avoiding spam
- Describe the four types of spam filters
- Explain the difference between phishing and pharming attacks
- Explain the purpose of Safe Browsing
- Describe how a rogue antivirus exploit works
- Give two examples of PUAs

Social Engineering Basics (1 of 3)

- In the context of cyber security, **social engineering** (SE) is a deceptive practice that exploits human psychology by inducing victims to interact with a digital device in a way that is not in their best interest
- **Social engineer** is a judgment-neutral term for a person who devises and carries out a scam in order to accomplish a goal, such as financial gain or service disruption
- The target of a social engineering exploit is an individual or organization that may be tricked into participating in the scam

Social Engineering Basics (2 of 3)



Social Engineering Basics (3 of 3)

- The poster child for social engineering scams is called **advance fee fraud**, in which the victim is promised a large sum of money in exchange for a bank account number from which a small advance fee is withdrawn

FROM: **dbrownpastor@stmatthews.org**

TO: SarahMaeSmith@Gmail.com

Need Assistance

Dear Sarah,

So sorry to bother you as I know you are quite busy this time of year. But my trip to the Philippines has turned into something of a disaster. Last night I was attacked and robbed. Thankfully, my injuries are minor and the hospital saw fit to release me this morning. The attackers got my wallet and phone, but I am glad that I locked my passport and airline ticket in the hotel safe.

I am left without any funds to pay my hotel bill or meet expenses to return home. Could you see it in your heart to loan me $2,000 just until I can get back to the States, when I can immediately pay you back? If so, I can give you instructions for wiring the money. It should not be difficult.

Sincerely,

Donald Brown

Spam (1 of 8)

- **Spam** is defined as unsolicited messages that are usually sent in massive numbers using electronic mail systems; it accounts for approximately 70% of all email
- Everyone gets spam; mass-mailing databases obtain millions of email addresses at low costs
- In 2003, the U.S. Congress passed a so-called anti-spam law, the **CAN-SPAM Act** (Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003)

Spam (2 of 8)

- Most ISPs and email services use filtering techniques to block spam coming from IP addresses and senders that are known to generate spam
- Spammers have developed techniques to bypass these barriers, and spam continues to make its way into consumer mailboxes
- Defending against spam requires careful Inbox management

Spam (3 of 8)

- **To reduce the amount of spam you receive, consider the following recommendations:**
  - Share your primary email address only with people or businesses that you trust not to distribute it to others. Businesses sometimes share mailing lists with affiliates, and lists may fall into the hands of illegitimate spammers. Keeping your email address off one list can keep it from propagating to multiple lists
  - Never reply to spam. Mailing lists contain a high percentage of invalid addresses. Replying to a spam message marks your email address as valid, which only generates more unwanted mail

Spam (4 of 8)

- Do not click links in spam messages. If you are curious about where a link might lead, hover over it with the pointer and look at the destination URL. Links in spam often are designed to direct victims to fake sites where malware is waiting
- Do not open attachments in email messages unless you are certain that the sender is trusted and the attached file is expected
- Use a complex email address with a user name that would not be found in a telephone directory. For example, add a number or symbol to your name

Spam (5 of 8)

- Use a disposable email address in situations where an email address is required but you don't want to receive solicitations. Disposable email addresses are useful when registering to use Web apps and when signing up for merchant loyalty programs
- When displaying your real email address—for example, on your Web site—disguise it by posting it as a graphic. You can create a graphic containing your email address by using graphics software, such as Paint, typing your name, and saving it as a PNG file

Spam (6 of 8)

- Use an opt-out link only if the email originated from a reputable national company. Before clicking the opt-out link, hover over it to make sure it leads to a legitimate URL
- Remember that if a deal seems too good to be true, it is probably a scam
- In iCloud, delete spam before opening it by using Mailto→Preferences→Viewing and deselecting "Display remote images in HTML messages."

Spam (7 of 8)

- Be suspicious of shortened URLs that do not reveal the genuine domain
- Be wary of email messages addressed to "undisclosed recipients" or addressed to numerous recipients that you don't know
- Be cautious of email messages addressed to your email user name rather than your real name
- Use the spam filters provided by your email client

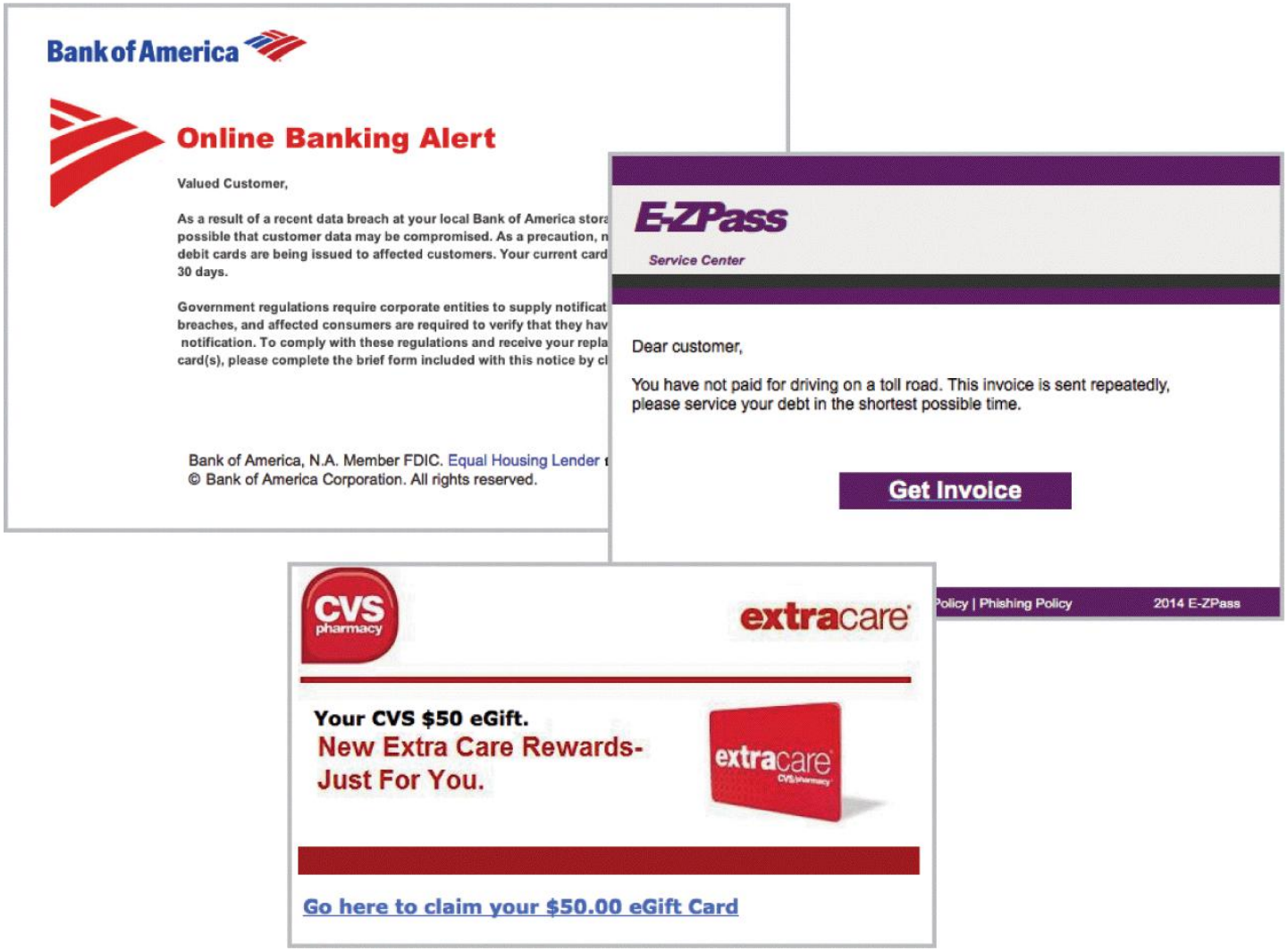
Spam (8 of 8)

- A **spam filter** uses a set of rules to examine email messages and determine which are spam
  - Content filters
  - Header filters
  - Blacklist filters
  - Permission filters

Phishing (1 of 2)

- **Phishing** is an email scam that masquerades as a message from a legitimate company or agency of authority, such as the IRS
- The goal of a phishing scam is to obtain private information such as passwords and bankcard numbers
- A **spear phishing** attack is more targeted and typically sent only to members of a specific organization
- Some of the most common attacks appear to originate from FedEx, UPS, DHL, or the U.S. Postal Service

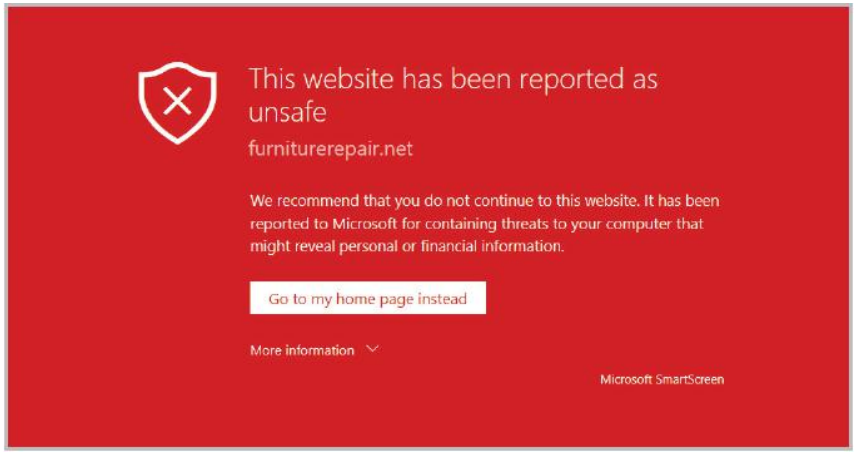
Phishing (2 of 2)

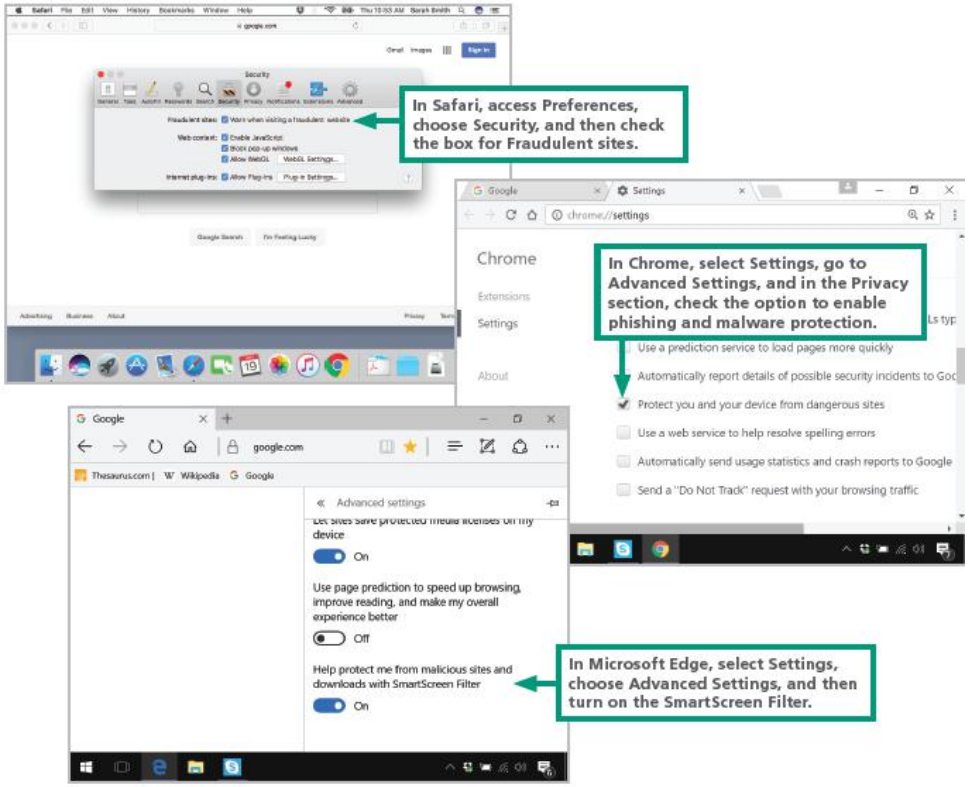


Pharming (1 of 2)

- **Pharming** redirects Web site traffic to fraudulent Web sites that distribute malware, collect personal data, and perpetrate other scams
- **Safe Browsing** is a service offered by Google that checks URLs against a list of suspicious Web site URLs
- Chrome, Safari, and Firefox use Safe Browsing to alert users about sites to avoid; Microsoft offers a similar service called **SmartScreen Filter**

Pharming (2 of 2)





Rogue Antivirus (1 of 2)

- A **rogue antivirus exploit** usually begins with a virus warning and an offer to disinfect the infected device
- The goal of this exploit is to trick consumers into clicking a link that downloads malware
- Fake virus alerts, which appear in pop-up windows, commonly appear when browsing the Web at slightly sketchy Web sites

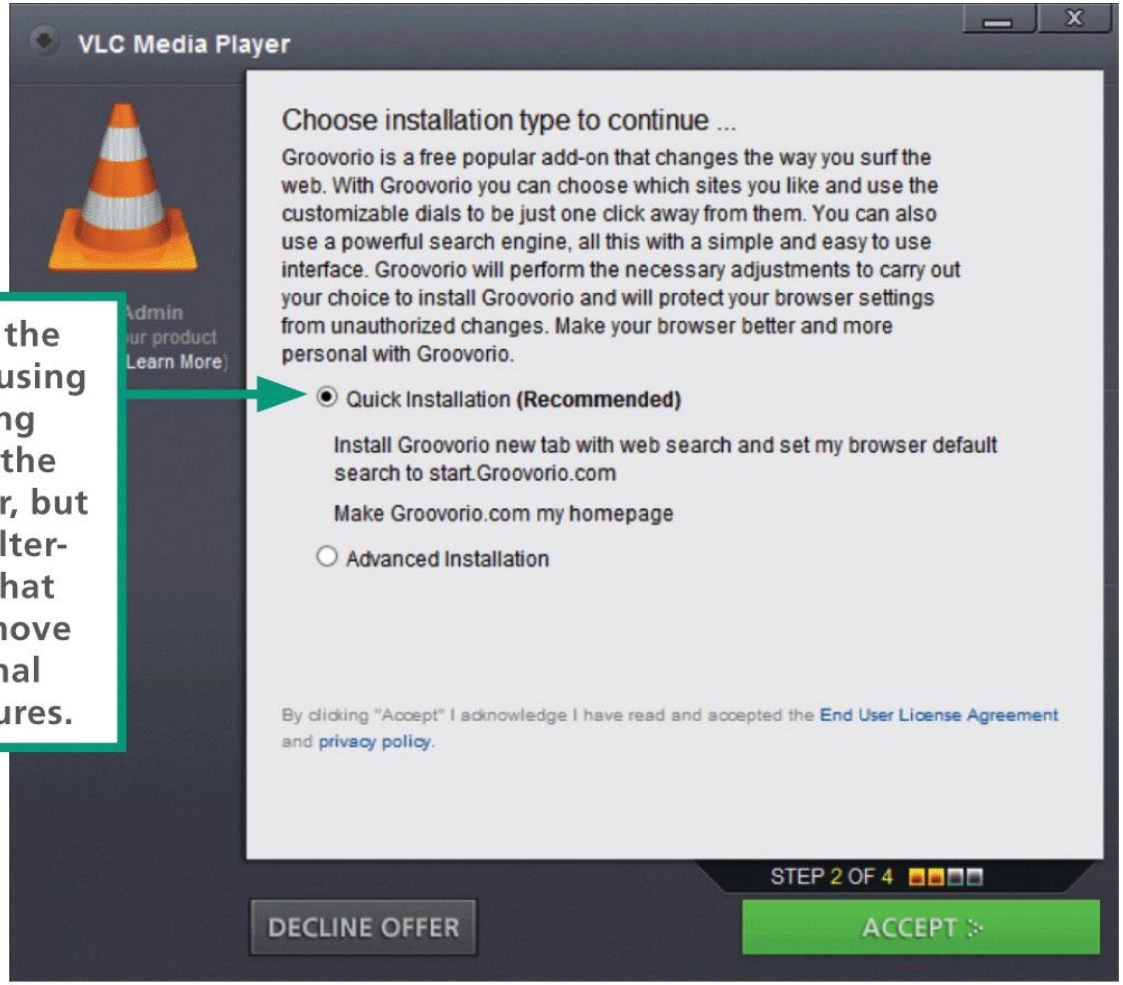
Rogue Antivirus (2 of 2)

Fake virus alerts can look realistic, so it is important to be familiar with the legitimate alerts displayed by your antivirus software. The two warnings on the left are fake. The three warnings on the right were produced by legitimate antivirus software.

PUAs (1 of 2)

- The acronym **PUP** stands for *potentially unwanted program*
- The acronym **PUA** stands for *potentially unwanted application* *(both PUP and PUA are used interchangeably)
- If you suddenly notice that an odd browser has become the default on your device and your attempts to reset to Chrome, IE, or Safari fail, then your computer is likely to have a PUA
- PUAs are installed using social engineering techniques, such as hoping consumers will mistakenly accept a PUA application during software installation

PUAs (2 of 2)



Proceeding with the installation and using the default setting not only installs the VLC Media Player, but also installs an alternative browser that is difficult to remove using conventional uninstall procedures.