NEW PERSPECTIVES

Unit 7

Digital Security

Computer Concepts 2016

ENHANCED EDITION

7 Unit Contents

- Section A: Unauthorized Use
- Section B: Malware
- Section C: Online Intrusions
- Section D: Interception
- Section E: Social Engineering

7 Section A: Unauthorized Use

- Encryption
- Authentication
- Strong Password
- Password Managers

7 Encryption

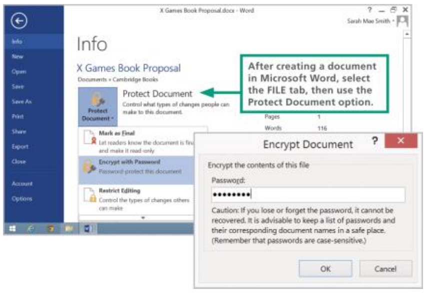
- **Encryption** transforms a message or data file in such a way that its contents are hidden from unauthorized readers
- An original message or file that has not yet been encrypted is referred to as **plaintext** or cleartext
- An encrypted message or file is referred to as **ciphertext**
- The process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

7 Encryption

- 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

7 Encryption

FIGURE 7-1: HOW TO ENCRYPT INDIVIDUAL FILES WITH MICROSOFT WORD



Info

X Games Book Proposal

Documents » Cambridge Books

Protect Document: Control what types of changes people can make to this document.

After creating a document in Microsoft Word, select the FILE tab, then use the Protect Document option.

Mark as Final: Let readers know the document is final and make it read-only

Encrypt with Password: Password-protect this document

Restrict Editing: Control the types of changes others can make

Encrypt Document

Encrypt the contents of this file

Password: ••••••••

Caution: If you lose or forget the password, it cannot be recovered. It is advisable to keep a list of passwords and their corresponding document names in a safe place. (Remember that passwords are case-sensitive.)

7 Authentication

- **Authentication protocols**, such as passwords, PINs, and fingerprint scanners, 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)
- 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

7 Authentication

- 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

7 Strong Passwords

- 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*

7 Strong Passwords

- A **brute force attack** uses password-cracking sortware to generate every possible combination of letters, numerals, and symbols; because it exhausts all possible combinations to discover a pssword, 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

7 Strong Passwords

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

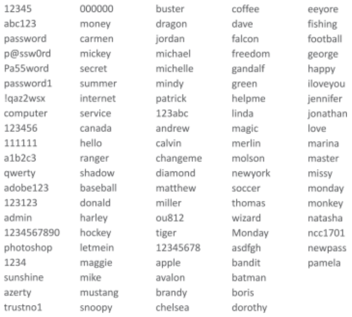


FIGURE 7-6: COMMONLY USED PASSWORDS

12345
abc123
password
p@ssw0rd
Pa55word
password1
!qaz2wsx
computer
123456
111111
a1b2c3
qwerty
adobe123
123123
admin
1234567890
photoshop
1234
sunshine
azerty
trustno1
000000
money
carmen
mickey
secret
summer
internet
service
canada
hello
ranger
shadow
baseball
donald
harley
hockey
letmein
maggie
mike
mustang
snoopy
buster
dragon
jordan
michael
michelle
mindy
patrick
123abc
andrew
calvin
changeme
diamond
matthew
miller
ou812
tiger
12345678
apple
avalon
brandy
chelsea
coffee
dave
falcon
freedom
gandalf
green
helpme
linda
magic
merlin
molson
newyork
soccer
thomas
wizard
Monday
asdfgh
bandit
batman
boris
dorothy
eeyore
fishing
football
george
happy
iloveyou
jennifer
jonathan
love
marina
master
missy
monday
monkey
natasha
ncc1701
newpass
pamela

7 Strong Passwords

- 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:**

7

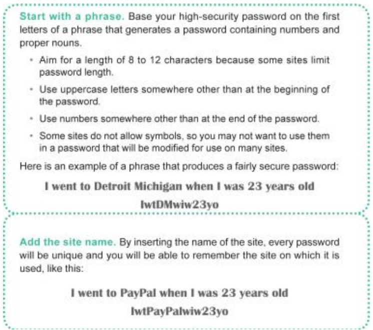
Strong Passwords

- 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
- Words with a sequence of numbers at the end, such as Missy123 and Dolphins2016
- Words with symbol or numeric mutations, such as p@ssw0rd and V01dem0rt
- Sequences of numbers formatted as dates or telephone numbers, such as 01/01/2000 and 888-5566
- Any sequence that includes a user name, such as BillMurray12345
- Any sequence that uses conventional capitalization, such as Book34 and Savannah912

7

Strong Passwords

FIGURE 7-8: PASSWORD ADVICE



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.

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:

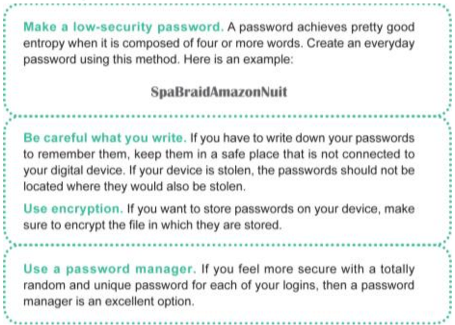
I went to PayPal when I was 23 years old

IwtPayPalwiw23yo

7

Strong Passwords

FIGURE 7-8: PASSWORD ADVICE



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.

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, then a password manager is an excellent option.

7

Password Managers

- 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

7

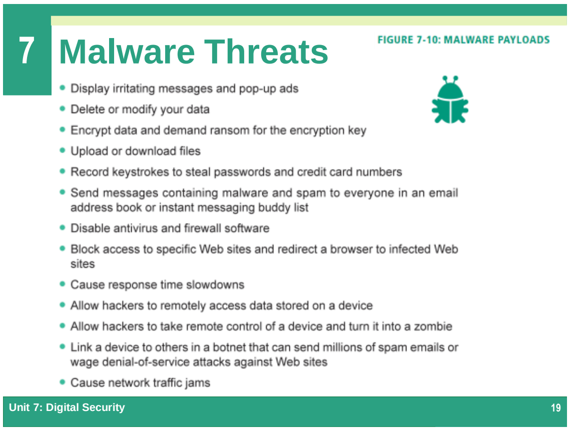
Section B: Malware

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

7

Malware Threats

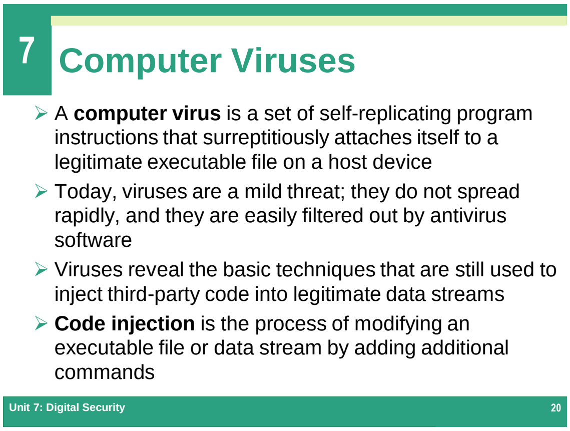
- **Malware** refers to any computer program designed to surreptitiously enter a digital device
- The action carried out by malware code is referred to as a **payload**
- Common classifications of malware include:
  - Viruses
  - Worms
  - Trojans



7 Malware Threats

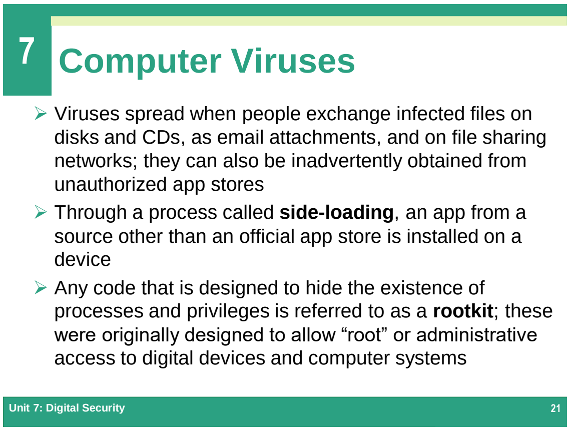
FIGURE 7-10: MALWARE PAYLOADS

- 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
- 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



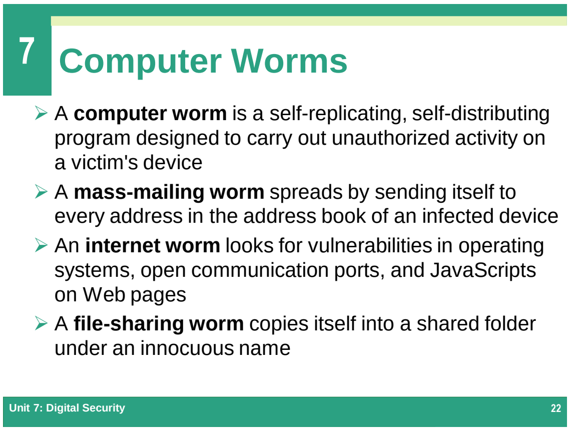
7 Computer Viruses

- 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



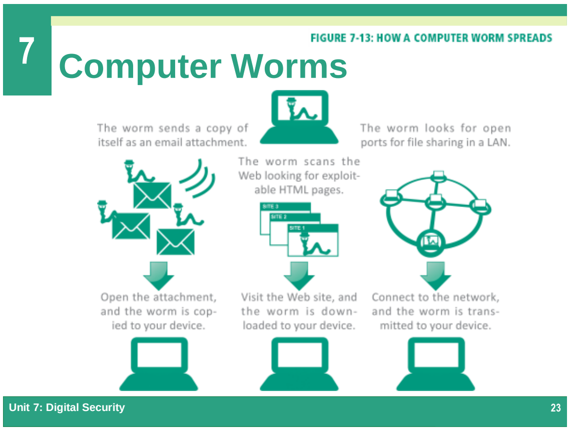
7 Computer Viruses

- 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



7 Computer Worms

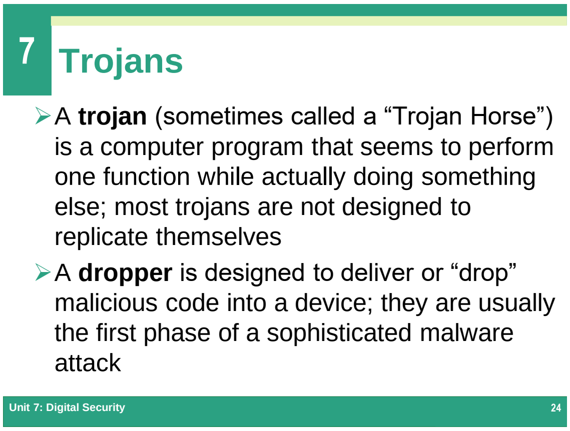
- A **computer worm** is a self-replicating, self-distributing program designed to carry out unauthorized activity on a victim's device
- A **mass-mailing worm** spreads by sending itself to every address in the address book of an infected device
- An **internet worm** looks for vulnerabilities in operating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



7 Computer Worms

FIGURE 7-13: HOW A COMPUTER WORM SPREADS

The worm sends a copy of itself as an email attachment.
The worm scans the Web looking for exploitable HTML pages.
The worm looks for open ports for file sharing in a LAN.
SITE 3
SITE 2
SITE 1
Open the attachment, and the worm is copied to your device.
Visit the Web site, and the worm is downloaded to your device.
Connect to the network, and the worm is transmitted to your device.



7 Trojans

- 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

7 Antivirus Software

- **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 maleware exploit; they are discovered by security experts who examine the bit sequences contained in malware program code

7 Antivirus Software

- 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

7 Antivirus Software

FIGURE 7-16: MALWARE DETECTED

Repair. Antivirus software can sometimes remove the malware code from infected files. This strategy is beneficial 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. 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.

7 Antivirus Software

- **For the most extensive protection from malware, you should look for and enable the following features of your antivirus software:**

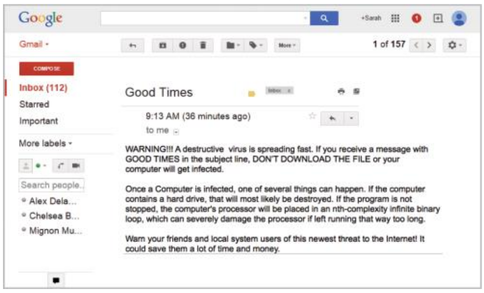
- Start scanning when the device boots.
- Scan all programs when they are launched, and scan document files when they are opened.
- Scan other types of files, such as graphics, if you engage in some risky computing behaviors and are not concerned with the extra time required to open files as they are scanned.
- Scan incoming email and attachments.
- Scan incoming instant message attachments.
- 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.

7 Antivirus Software

- 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

7 Antivirus Software

FIGURE 7-20: A TYPICAL VIRUS HOAX



Good Times

9:13 AM (36 minutes ago)

to me

WARNING!!! A destructive virus is spreading fast. If you receive a message with GOOD TIMES in the subject line, DON'T DOWNLOAD THE FILE or your computer will get infected.

Once a Computer is infected, one of several things can happen. If the computer contains a hard drive, that will most likely be destroyed. If the program is not stopped, the computer's processor will be placed in an nth-complexity infinite binary loop, which can severely damage the processor if left running that way too long.

Warn your friends and local system users of this newest threat to the Internet! It could save them a lot of time and money.

7

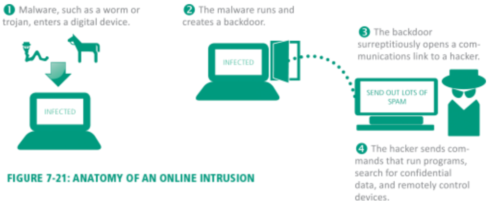
Section C: Online Intrusions

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

7

Intrusion Threats

- 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



1 Malware, such as a worm or trojan, enters a digital device.

2 The malware runs and creates a backdoor.

3 The backdoor surreptitiously opens a communications link to a hacker.

4 The hacker sends commands that run programs, search for confidential data, and remotely control devices.

FIGURE 7-21: ANATOMY OF AN ONLINE INTRUSION

7

Intrusion Threats

- **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
  - **Ransomware** – locks a device and then requests payment for an unlocking code; commonly exploits the Find My iPhone feature

Cont…

7

Intrusion Threats

- **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
- **Backdoor** – an undocumented method of accessing a digital device; RATs create a backdoor to a victim's device that can be used by a hacker to obtain photos and videos
- **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

7

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

7

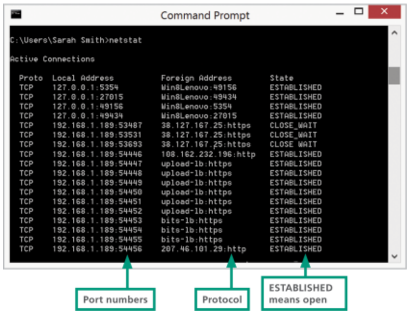
Netstat

- Hackers use a technique called port scanning to discover which ports are open on a device
- A **port scan** pings a packet of data to the port; if a reply is received, then the port is open
- Open ports are used for communications between botnets and their masters
- A network utility called Netstat produces a detailed list of open ports on a device; although it is not clear which open ports are being used by botnets

7

Netstat

FIGURE 7-26: NETSTAT DETECTS OPEN PORTS



```
C:\Users\Sarah Smith>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:5354         Win8Lenovo:49156       ESTABLISHED
  TCP    127.0.0.1:27015        Win8Lenovo:49434       ESTABLISHED
  TCP    127.0.0.1:49156        Win8Lenovo:5354        ESTABLISHED
  TCP    127.0.0.1:49434        Win8Lenovo:27015       ESTABLISHED
  TCP    192.168.1.189:53487    38.127.167.25:https    CLOSE_WAIT
  TCP    192.168.1.189:53531    38.127.167.25:https    CLOSE_WAIT
  TCP    192.168.1.189:53693    38.127.167.25:https    CLOSE WAIT
  TCP    192.168.1.189:54446    108.162.232.196:http   ESTABLISHED
  TCP    192.168.1.189:54447    upload-lb:https        ESTABLISHED
  TCP    192.168.1.189:54448    upload-lb:https        ESTABLISHED
  TCP    192.168.1.189:54449    upload-lb:https        ESTABLISHED
  TCP    192.168.1.189:54450    upload-lb:https        ESTABLISHED
  TCP    192.168.1.189:54451    upload-lb:https        ESTABLISHED
  TCP    192.168.1.189:54452    upload-lb:https        ESTABLISHED
  TCP    192.168.1.189:54453    bits-lb:https          ESTABLISHED
  TCP    192.168.1.189:54454    bits-lb:https          ESTABLISHED
  TCP    192.168.1.189:54455    bits-lb:https          ESTABLISHED
  TCP    192.168.1.189:54456    207.46.101.29:http     ESTABLISHED
```

7

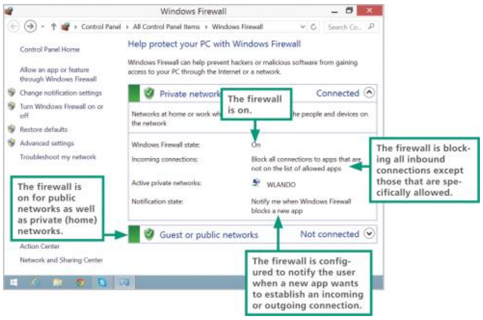
Firewalls

- 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

7

Firewalls

FIGURE 7-27: FIREWALL CONFIGURATION



Windows Firewall
Control Panel › All Control Panel Items › Windows Firewall
Search Co...
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Action Center
Network and Sharing Center

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private network Connected

Networks at home or work wh... he people and devices on the network

Windows Firewall state: On

Incoming connections: Block all connections to apps that are not on the list of allowed apps

Active private networks: WLANDO

Notification state: Notify me when Windows Firewall blocks a new app

Guest or public networks Not connected

The firewall is on.

The firewall is blocking all inbound connections except those that are specifically allowed.

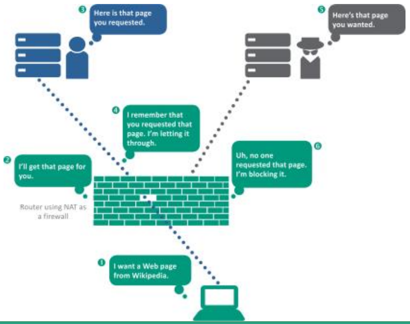
The firewall is on for public networks as well as private (home) networks.

The firewall is configured to notify the user when a new app wants to establish an incoming or outgoing connection.

7

Firewalls

FIGURE 7-29: A ROUTER WITH NAT PROVIDES A HARDWARE FIREWALL



1 I want a Web page from Wikipedia.
2 I'll get that page for you.
3 Here is that page you requested.
4 I remember that you requested that page. I'm letting it through.
5 Here's that page you wanted.
6 Uh, no one requested that page. I'm blocking it.
Router using NAT as a firewall

7

Section D: Interception

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

7

Interception Basics

- 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

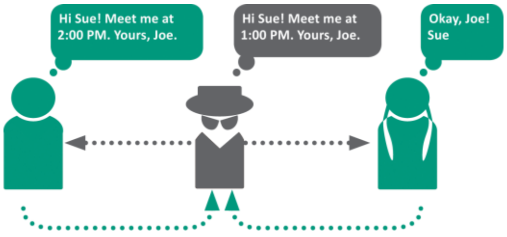
Cont…

7 Interception Basics

- **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

7 Interception Basics

FIGURE 7-30: A BASIC MAN-IN-THE-MIDDLE ATTACK


Hi Sue! Meet me at 2:00 PM. Yours, Joe.
Hi Sue! Meet me at 1:00 PM. Yours, Joe.
Okay, Joe! Sue

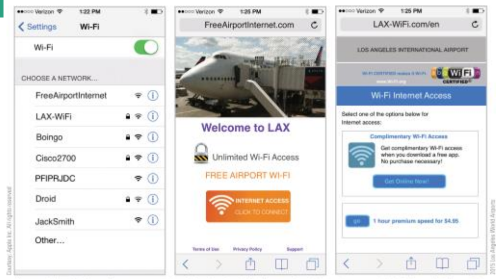
In an MITM attack, two parties believe they are communicating directly with each other when, in fact, they are communicating with a third party.

7 Evil Twins

- 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

7 Evil Twins

FIGURE 7-31: WHICH NETWORK IS THE EVIL TWIN?



Settings Wi-Fi

Wi-Fi

CHOOSE A NETWORK...

FreeAirportInternet
LAX-WiFi
Boingo
Cisco2700
PFIPRJDC
Droid
JackSmith
Other...

FreeAirportInternet.com

Welcome to LAX

Unlimited Wi-Fi Access

FREE AIRPORT WI-FI

INTERNET ACCESS CLICK TO CONNECT

LAX-WiFi.com/en

LOS ANGELES INTERNATIONAL AIRPORT

Wi-Fi Internet Access

Select one of the options below for Internet access:

Complimentary Wi-Fi Access

Get complimentary Wi-Fi access when you download a free app. No purchase necessary!

Get Online Now!

1 hour premium speed for $4.95

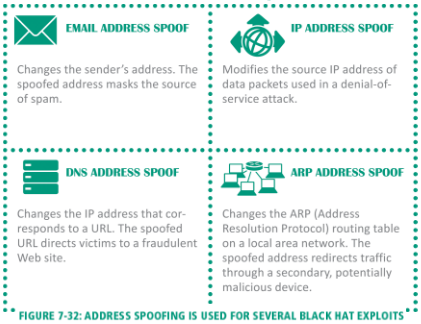
Courtesy: Apple Inc. All rights reserved
2015 Los Angeles World Airports

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.

7 Address Spoofing

- 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

7 Address Spoofing



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.

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.

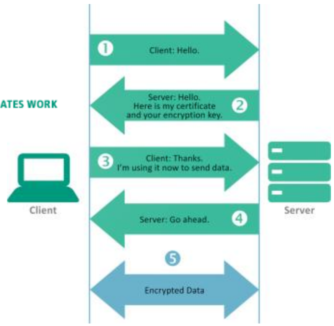
FIGURE 7-32: ADDRESS SPOOFING IS USED FOR SEVERAL BLACK HAT EXPLOITS

7 Digital Certificate Hacks

- 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

7 Digital Certificate Hacks

FIGURE 7-33: HOW DIGITAL CERTIFICATES WORK



1 Client: Hello.

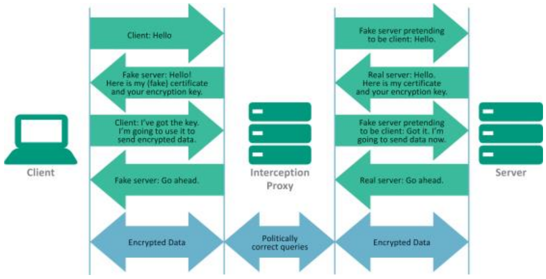
2 Server: Hello. Here is my certificate and your encryption key.

3 Client: Thanks. I'm using it now to send data.

4 Server: Go ahead.

5 Encrypted Data

7 Digital Certificate Hacks



Client: Hello

Fake server: Hello! Here is my (fake) certificate and your encryption key.

Client: I've got the key. I'm going to use it to send encrypted data.

Fake server: Go ahead.

Encrypted Data

Politically correct queries

Fake server pretending to be client: Hello.

Real server: Hello. Here is my certificate and your encryption key.

Fake server pretending to be client: Got it. I'm going to send data now.

Real server: Go ahead.

Encrypted Data

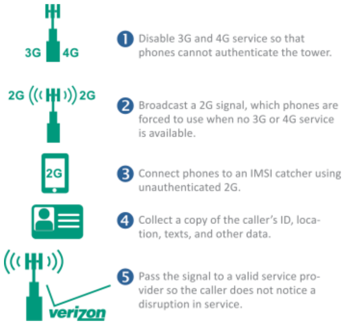
FIGURE 7-34: HOW FAKE DIGITAL CERTIFICATES DEFEAT ENCRYPTION

7 IMSI Catchers

- **IMSI** is an acronym for International Mobile Subscriber Identity
- It's 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

7 IMSI Catchers

FIGURE 7-37: ANATOMY OF AN IMSI CATCHER EXPLOIT



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.

7 Section E: Social Engineering

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

7 Social Engineering Basics

- 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

7 Social Engineering Basics

FIGURE 7-38: ELEMENTS OF A SOCIAL ENGINEERING ATTACK

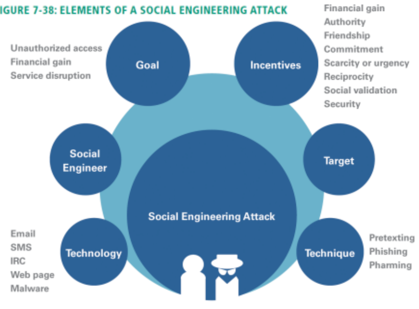
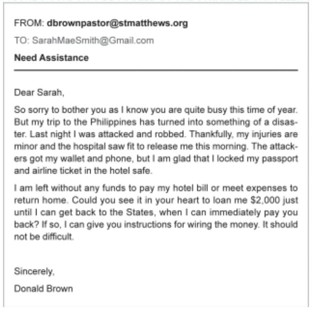


Diagram adapted from F. Mouton et al. Towards an Ontological Model Defining the Social Engineering Domain.

7 Social Engineering Basics

- 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

FIGURE 7-39: DON'T BE FOOLED BY THE STRANDED TRAVELER SCAM



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

7 Spam

- **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)

7 Spam

- Most ISPs and email services use filtering techniques to block spam coming from IP addresses and senders that are know 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
- **To reduce the amount of spam you receive, consider the following recommendations:**

7 Spam

- 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.
- 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.

7 Spam

- 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.
- 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."

7 Spam

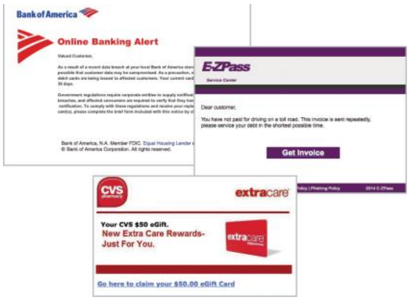
- Be suspicious of shortened URLs that do not reveal the genuine domain.
- Be wary of email messages addressed to "undisclosed recipients" or addressed to numerous recipients that you don't know.
- Be cautious of email messages addressed to your email user name rather than your real name.
- Use the spam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

7 Phishing

- **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
- Some of the most common attacks appear to originate from FedEx, UPS, DHL, or the U.S. Postal service

7 Phishing

FIGURE 7-43: PHISHING ATTACKS APPEAR TO ORIGINATE FROM TRUSTED BUSINESSES



Bank of America

Online Banking Alert

Valued Customer,

As a result of a recent data breach at your local Bank of America stor possible that customer data may be compromised. As a precaution, debit cards are being issued to affected customers. Your current card 30 days.

Government regulations require corporate entities to supply notificat breaches, and affected consumers are required to verify that they hav notification. To comply with these regulations and receive your repla card(s), please complete the brief form included with this notice by cl

Bank of America, N.A. Member FDIC. Equal Housing Lender
© Bank of America Corporation. All rights reserved.

E-ZPass
Service Center

Dear customer,

You have not paid for driving on a toll road. This invoice is sent repeatedly, please service your debt in the shortest possible time.

Get Invoice

olicy | Phishing Policy 2014 E-ZPass

CVS pharmacy extracare

Your CVS $50 eGift.
New Extra Care Rewards-
Just For You.

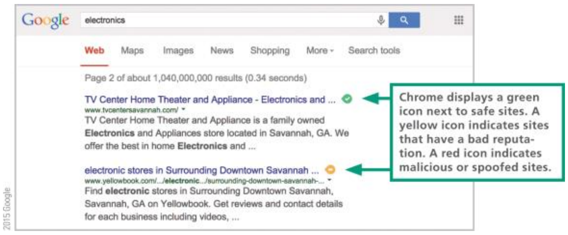
Go here to claim your $50.00 eGift Card

7 Pharming

- **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**

7 Pharming

FIGURE 7-45: GOOGLE USES COLORED ICONS TO INDICATE SKETCHY SITES



Page 2 of about 1,040,000,000 results (0.34 seconds)

TV Center Home Theater and Appliance - Electronics and ...
www.tvcentersavannah.com/
TV Center Home Theater and Appliance is a family owned **Electronics** and Appliances store located in Savannah, GA. We offer the best in home **Electronics** and ...

electronic stores in Surrounding Downtown Savannah ...
www.yellowbook.com/.../**electronic**.../surrounding-downtown-savannah-...
Find **electronic** stores in Surrounding Downtown Savannah, Savannah, GA on Yellowbook. Get reviews and contact details for each business including videos, ...

Chrome displays a green icon next to safe sites. A yellow icon indicates sites that have a bad reputation. A red icon indicates malicious or spoofed sites.

2015 Google

7

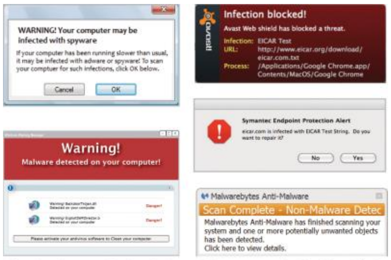
Rogue Antivirus

- 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

7

Rogue Antivirus

FIGURE 7-47: MALWARE ALERTS: WHICH ARE FAKE?



WARNING! Your computer may be infected with spyware

If your computer has been running slower than usual, it may be infected with adware or spyware! To scan your comptuer for such infections, click OK below.

Cancel OK

Infection blocked!

Avast Web shield has blocked a threat.

Infection: EICAR Test
URL: http://www.eicar.org/download/eicar.com.txt
Process: /Applications/Google Chrome.app/Contents/MacOS/Google Chrome

Symantec Endpoint Protection Alert

eicar.com is infected with EICAR Test String. Do you want to repair it?

No Yes

Warning!

Malware detected on your computer!

Danger!

Danger!

Please activate your antivirus software to Clean your computer

Malwarebytes Anti-Malware

Scan Complete - Non-Malware Detec

Malwarebytes Anti-Malware has finished scanning your system and one or more potentially unwanted objects has been detected.
Click here to view details.

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.

7

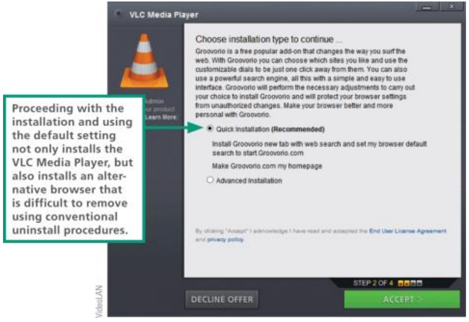
PUAs

- 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

7

PUAs

FIGURE 7-48: WHEN INSTALLING SOFTWARE, STAY ALERT FOR PUAS



VLC Media Player

Choose installation type to continue ...

Groovorio is a free popular add-on that changes the way you surf the web. With Groovorio you can choose which sites you like and use the customizable dials to be just one click away from them. You can also use a powerful search engine, all this with a simple and easy to use interface. Groovorio will perform the necessary adjustments to carry out your choice to install Groovorio and will protect your browser settings from unauthorized changes. Make your browser better and more personal with Groovorio.

● Quick Installation **(Recommended)**

Install Groovorio new tab with web search and set my browser default search to start.Groovorio.com

Make Groovorio.com my homepage

○ Advanced Installation

By clicking "Accept" I acknowledge I have read and accepted the End User License Agreement and privacy policy

STEP 2 OF 4

DECLINE OFFER ACCEPT >

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.

VideoLAN

NEW PERSPECTIVES

Unit 7 Complete

Computer Concepts 2016