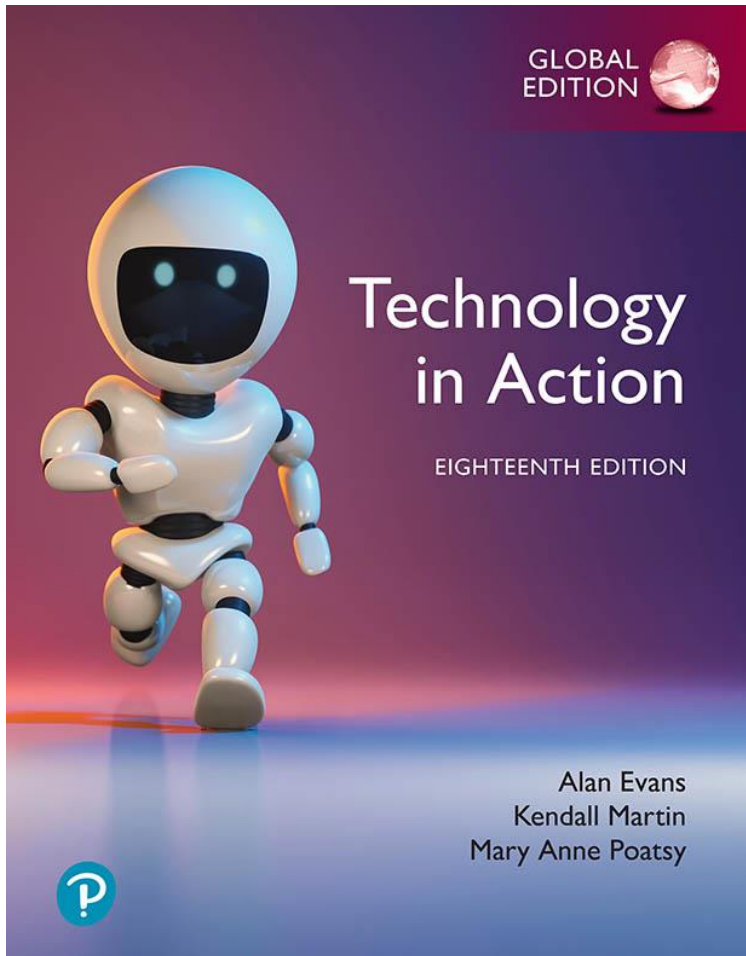


# Technology in Action

Eighteenth Edition

Global Edition



## Chapter 4

### Safety in the Digital World: Protecting Digital Assets and Practising Safe Computing



# Learning objectives

- 4.1** Describe how identity theft is committed, and the types of scams identity thieves perpetrate.
  - 4.2** Describe the different types of hackers and the tools they use.
  - 4.3** Explain what a computer virus is, why it is a threat to your security, how a computing device catches a virus, and the symptoms it may display.
  - 4.4** List the different categories of computer viruses and describe their behaviors.
  - 4.5** Explain what malware, spam, and cookies are and how they impact your security.
-



# Learning objectives

- 4.6** Describe social engineering techniques and explain strategies to avoid falling prey to them.
  - 4.7** Explain what a firewall is and how a firewall protects your computer from hackers.
  - 4.8** Explain how to protect your computer from virus infection.
  - 4.9** Describe how passwords and biometric characteristics can be used for user authentication.
  - 4.10** Describe ways to surf the Web anonymously.
-



# Learning objectives

- 4.11** Describe the types of information you should never share online.
  - 4.12** List the various types of backups you can perform on your computing devices and explain the various places you can store backup files.
  - 4.13** Explain the negative effects environment and power surges can have on computing devices.
  - 4.14** Describe the major concerns when a device is stolen and strategies for solving the problems.
  - 4.15** Describe what cyberbullying is, recognize its forms and effects, and explain strategies to prevent or respond to cyberbullying incidents.
-

# Introduction

- Digitalization?
- Digitalization is completely dealing with data.
- In different forms, data is shared everywhere.
- Sometimes, data is very sensitive and can be misused by anyone.
- Companies and organizations should make sure that when sharing sensitive information, it is essential to keep the data safe.

# Protecting Digital Assets & Practicing Safe Computing

---

- **Secure Your Devices:**  
Install reputable antivirus software, enable firewalls, and keep all devices—computers, smartphones, tablets—up to date.
- **Data Backup:**  
Regularly back up files to cloud storage or external drives, ensuring recovery in case of theft, hardware failure, or ransomware.

# Cyber Security

- According to NIST (National Institute of Standards and Technology), cybersecurity is the protection of assets from unauthorised activities to ensure confidentiality, integrity, and availability (CIA).
- Cyber Security Framework consist of 5 components as below:

1.



## IDENTIFY

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

2.



## PROTECT

- Access Control
- Awareness and Training
- Data Security
- Information Protection Procedures
- Maintenance
- Protective Technology

3.



## DETECT

- Anomalies and Events
- Continuous Monitoring
- Information Protection Procedures
- Detection Process

4.



## RESPOND

- Response Planning
- Communications
- Analysis
- Mitigations
- Improvements

5.



## RECOVER

- Recovery Planning
- Communications
- Improvements

**1M+VIEWS**



simplelearn



# What is Cyber Security?







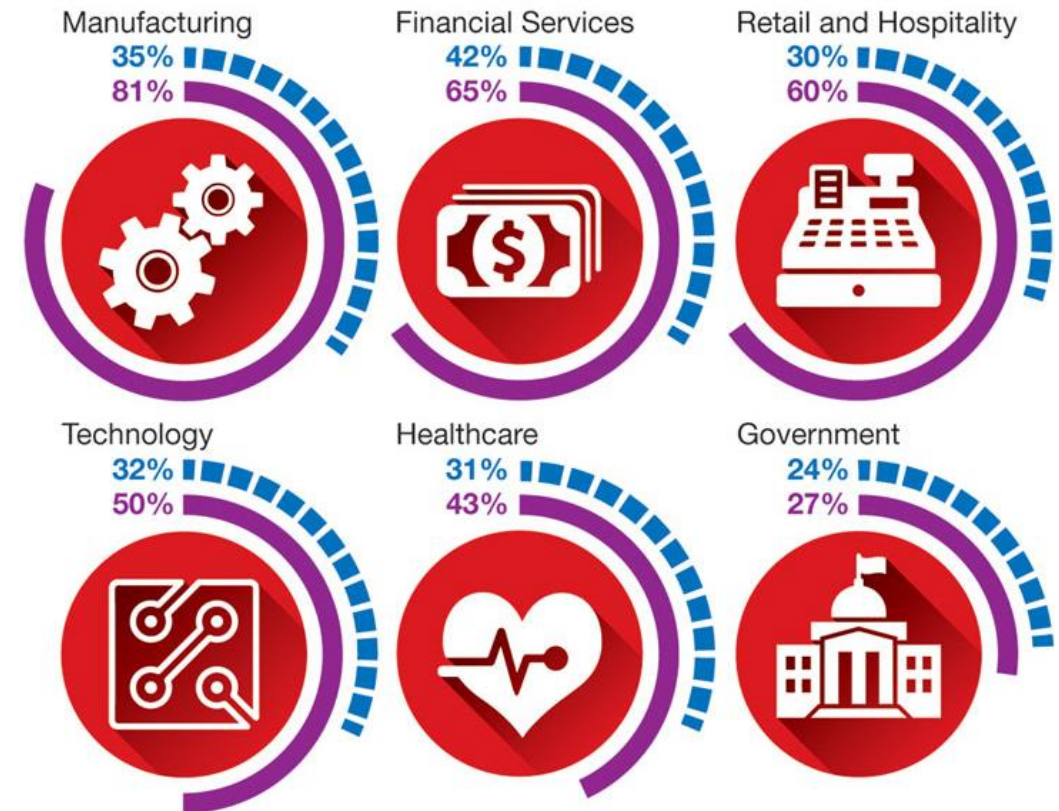
# Cyber Threats

# Common Digital Risks

- Cybercrime
- Cybercriminals
- Common types of cybercrimes
- Four common categories of complaints received were:
  - FBI related scams
  - Identity theft
  - Non-auction/non-delivery or merch
  - Advance free fraud

## Industries Respond to the Threat

■ has strong cybersecurity  
■ compliant with OWASP\* Top 10 Policies



\* OWASP: Open Web Application Security Project

# Cybersecurity Threat


## 1. Identity Theft :

- Thief steals personal information and poses as you in a financial or legal transaction.
- Used your name, address, social security number, birth date, bank account number or credit card information.
- Types of scams:
  - Counterfeiting your existing credit and debit cards
  - Requesting changes of address
  - Opening new credit cards
  - Obtaining medical services
  - Buying a home



# Identity Theft

**Identity theft** involves the unauthorized acquisition and use of someone else's personal information—such as **their name, identification number, or financial details**—for fraudulent purposes.



This crime can lead to significant **financial loss, reputational damage, and emotional distress** for victims

## Recent Identity Theft Cases in Malaysia

- **Norashikin from Kajang (2023)**  
Her **IC was misused** to buy a smartphone; she only found out when applying for a loan and got rejected due to bad credit.
- **Query Smart Search Syndicate (2024)**  
Five arrested in KL, including a **Pakistani mastermind**, for selling **400 million Malaysians' personal data** (IC, phone, bank info) on the Dark Web.
- **Pulau Indah Fake MyKad Case (2024)**  
Three **Filipino men** used fake/borrowed MyKads to get jobs and housing; paid up to **RM500** for the IDs.
- **Johor Company Director (2023)**  
The victim lost **RM6.2 million** due to a **business email compromise**—hackers faked a supplier's payment request.
- **17M MyKad Data Breach Allegation (2024)**  
**NACSA investigated** a major breach where **17 million Malaysians' MyKad data** was allegedly leaked and sold online.

## 28yo chef stuck in Kuching over RM800,000 tax bill after identity theft, urges Inland Revenue action

Jan 4, 2025 @ 15:48



Fang (centre) relating his plight during a press conference with Foo (left) and Wong present at SUPP headquarters on Jan 4, 2025.

# Hackers

---

- Hacker—anyone who unlawfully breaks into a computer system
- Types of hackers
  - White-hat (ethical hackers)
  - Black-hat hackers
  - Grey-hat hackers
- Packet analyzer (sniffer)
  - a program deployed by hackers that looks at (or sniffs) each packet as it travels on the Internet.
- Keylogger
  - is a program that captures all keystrokes made on a computer





## Case Study: Government Data Breach Attempt (2024)

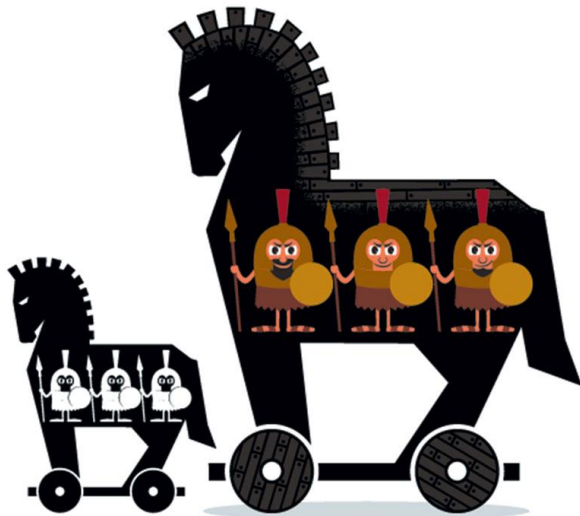
- **Date:** December 25, 2023
- **Incident:** A 24-year-old IT specialist was arrested for hacking into a Malaysian government agency's system.
- **Action:** The individual attempted to sell the stolen data on the Dark Web for **US\$200 (~RM927)** per dataset, with payments requested in cryptocurrency.
- **Detection:** The **Bukit Aman Commercial Crime Investigation Department (CCID)** traced the suspect through their **Cryptocurrency Crime Investigation Unit**.
- **Legal Proceedings:** The suspect was released on bail and is being investigated under **Section 4(1) of the Computer Crimes Act 1997**



# Identity Theft and Hackers

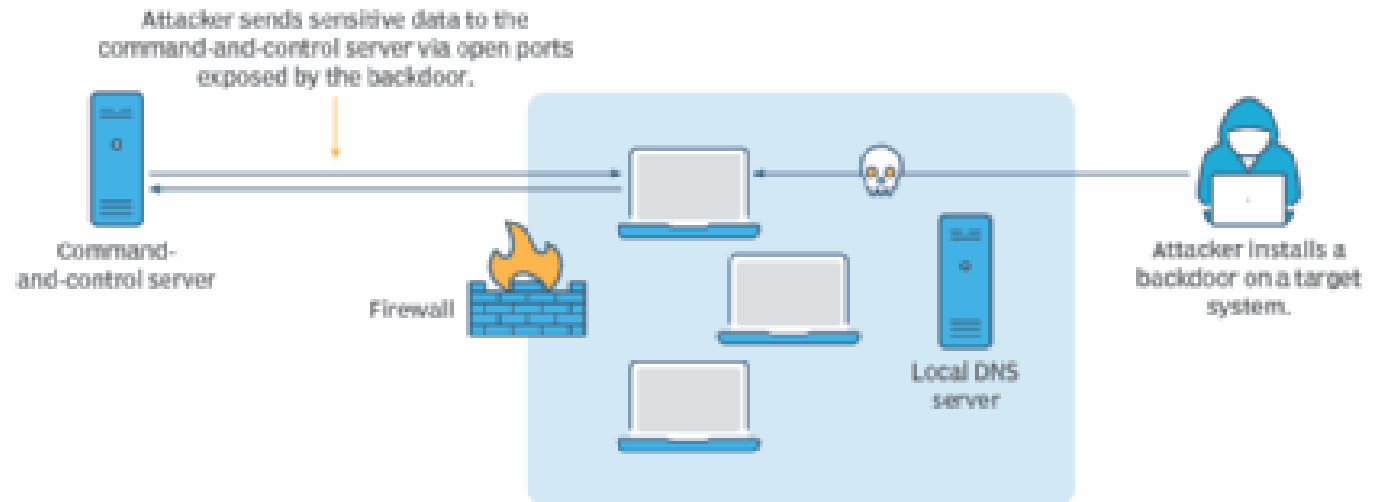
## - Hacking

- **Trojan horses**—appear to be useful but run malicious code
- **Backdoor programs and rootkits** allow hackers to gain access to a computer



Copyright © 2024 by Pearson Education, Inc.

## How a backdoor attack works





# Identity Theft and Hackers

## Hacking

- Zombies—computers that a hacker controls
- Denial-of-service
  - Legitimate users are denied access to a computer system
  - System shuts down
- DDoS

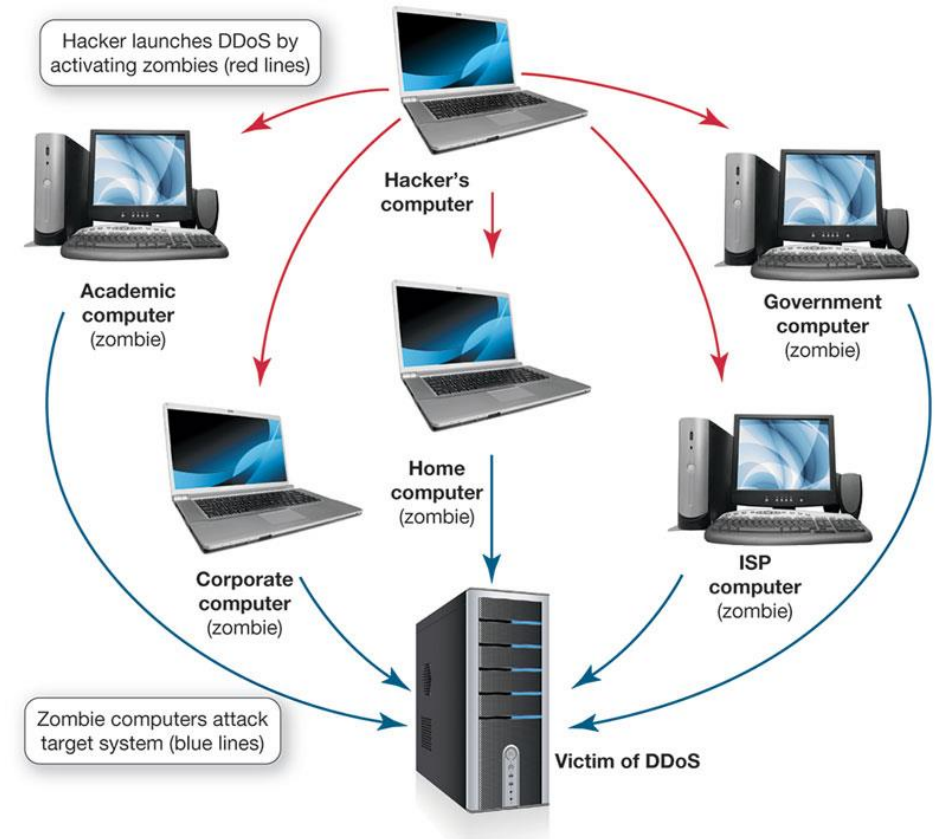
```
C:\WINDOWS\system32\cmd.exe
10/04/2007 04:51 PM <DIR> Start Menu
10/04/2007 04:51 PM <DIR> Templates
10/04/2007 04:51 PM <DIR> WINDOWS
10/04/2007 04:51 PM File(s) 238,543 bytes
10/04/2007 04:51 PM Dir(s) 49,378,472,960 bytes free

C:\Documents and Settings\hointo>cd ..
C:\Documents and Settings>cd ..
C:\>dir
Volume in drive C is media 02
Volume Serial Number is BC2E-0ED8

Directory of C:\

06/10/2004 03:59 PM 0 0000
07/15/2003 10:01 AM 98 AUTOEXEC.BAT
02/07/2003 12:13 PM 2 autoreg.txt
10/21/2006 01:18 PM Batch Upload
01/27/2003 03:19 PM 0 COMPTON
06/11/2005 02:58 PM 3,197 DEMO.TXT
02/28/2005 02:47 PM del
01/10/2007 07:12 PM <DIR> diex
10/11/2006 03:56 PM <DIR> Documents and Settings
02/28/2005 02:48 PM <DIR> devtemp
04/28/2007 01:52 PM <DIR> ev7dms
02/11/2007 12:14 PM 338,347 Folog.txt
02/18/2007 05:27 PM 4,125,482 Folog.txt.old
05/10/2006 03:58 PM <DIR> KFCPS
07/09/2007 11:12 AM <DIR> Kircach
04/16/2007 05:59 PM <DIR> My Downloads
01/27/2003 05:19 PM <DIR> My Music
10/24/2005 01:42 PM <DIR> NFS
11/06/2006 04:43 PM <DIR> pentest
04/16/2007 06:10 PM <DIR> Program Files
12/09/2006 06:27 PM 56,710 service.txt
11/07/2005 11:13 AM <DIR> spoolerlogs
02/28/2005 10:40 PM <DIR> temp
07/15/2003 10:01 AM <DIR> 0 tempfile.txt
04/16/2007 06:15 PM <DIR> WINDOWS
11/06/2006 02:17 PM <DIR> WTemp
10/04/2007 04:51 PM File(s) 4,584,748 bytes
10/04/2007 04:51 PM Dir(s) 49,378,472,960 bytes free

C:\>
```



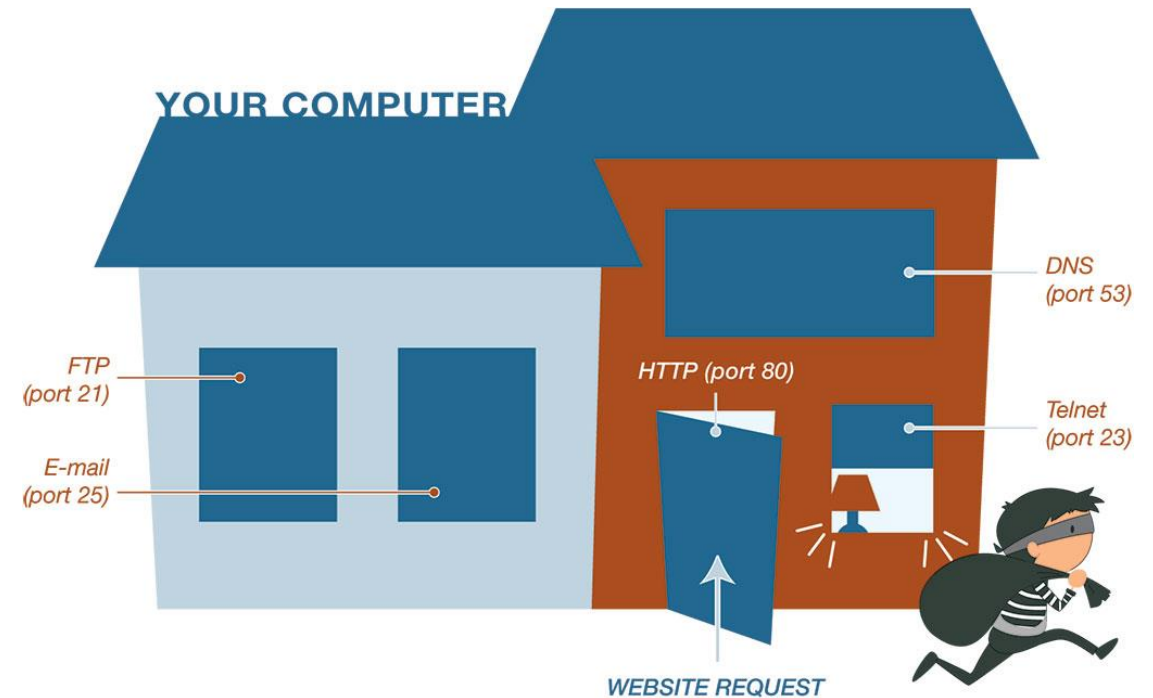
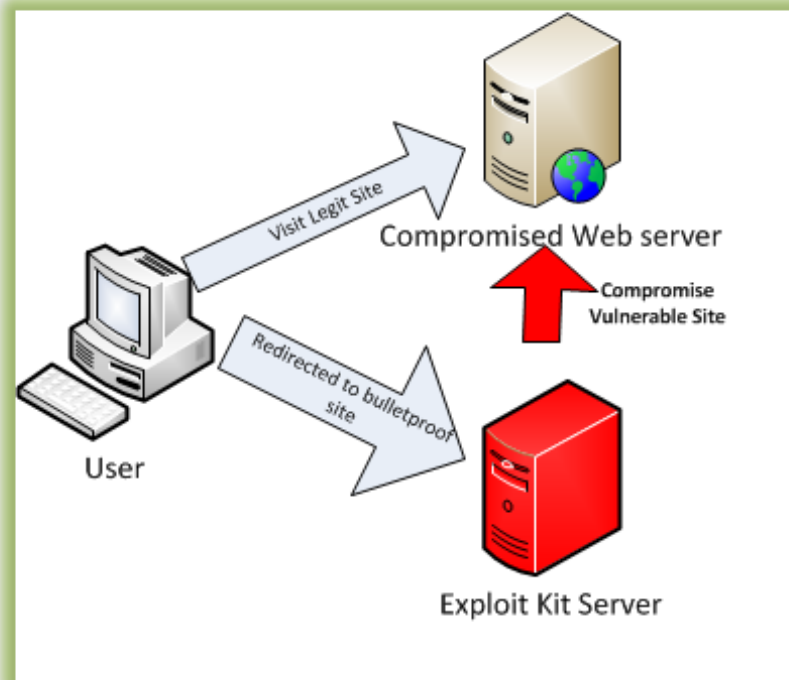
Copyright © 2024 by Pearson Education, Inc.

- Botnet—a large group of devices that have been infected by software programs

# Identity Theft and Hackers

## - Hacking

- Exploit kits—software that runs on servers searching for vulnerabilities
- Logical ports are virtual, not physical, communications paths



Copyright © 2024 by Pearson Education, Inc.

# Cybersecurity Threat

## 2. Computer Virus: Virus Basic

- Virus—a program that attaches to a computer program to spread to other computers
  - Main purpose—replicate itself and copy its code into as many other host files as possible
  - Secondary objectives can be destructive
- Smartphones and tablets can be infected with viruses

# Computer Viruses

## - Virus Basics

---



# Types of Viruses



Boot-sector viruses



Logic bombs and time bombs



Worms



Script and macro viruses



E-mail viruses



Encryption viruses

# 8 TYPES OF COMPUTER VIRUSES

1.

## BOOT SECTOR VIRUS



A COMPUTER VIRUS THAT INFECTS A COMPUTER'S MASTER BOOT RECORD

2.

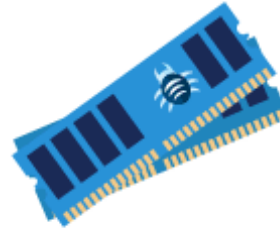
## OVERWRITE VIRUS



A COMPUTER VIRUS THAT INFECTS YOUR FILES AND DESTROYS THEM

3.

## RESIDENT VIRUS



THIS KIND OF COMPUTER VIRUS EMBEDS ITSELF IN THE COMPUTER'S MEMORY

4.

## FILE-INFECTING VIRUS



A COMPUTER VIRUS THAT OVERWRITES OR INSERTS INFECTED CODE INTO EXECUTABLE FILES

5.

## MACRO VIRUS



A COMPUTER VIRUS WRITTEN IN THE SAME LANGUAGE AS SOFTWARE PROGRAMS LIKE MICROSOFT OFFICE

6.

## WEB SCRIPTING VIRUS



A VIRUS THAT HIDES IN THE CODE OF WEB PAGES AND WEB BROWSERS

7.

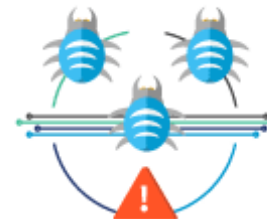
## POLYMORPHIC VIRUS



THIS VIRUS ACQUIRES A DIFFERENT FORM EACH TIME THE INFECTED FILE OR PROGRAM IS EXECUTED

8.

## MULTIPARTITE VIRUS




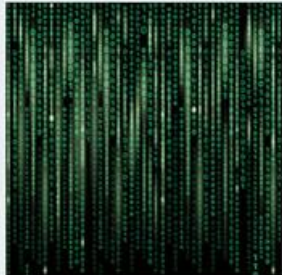




A COMBINATION OF THE DIFFERENT TYPES OF VIRUSES LISTED PREVIOUSLY



# Types of Viruses

---

<b>Boot-Sector Viruses</b>  Execute when a computer boots up	<b>Logic Bombs/Time Bombs</b>  Execute when certain conditions or dates are reached	<b>Worms</b>  Spread on their own with no human interaction needed
<b>Scripts and Macro Viruses</b>  Series of commands with malicious intent	<b>E-mail Viruses</b>  Spread as attachments to e-mail, often using address books	<b>Encryption Viruses</b>  Hold files "hostage" by encrypting them; ask for ransom to unlock them

*(Glinskaja Olga/Shutterstock; KsanderDN/Shutterstock; David Martyn Hughes/123RF; Neyro2008/123RF; Bannosuke/Shutterstock; Lukas Gojda/Shutterstock)*

Copyright © 2024 by Pearson Education, Inc.

# Computer Viruses

Virus classified as avoid detection

---

- Classified by methods used to avoid detection
  - **Polymorphic**—change their code or periodically rewrite themselves to avoid detection
  - **Multi-partite**—are designed to infect multiple file types
  - **Stealth**—temporarily erase their code from the files where they reside and hide in active memory





# Dangerous Virus Timeline



## 1. ILOVEYOU (2000)

- **Type:** Worm
- **Damage:** Over **\$10 billion** in damages.
- **How it spread:** Email attachment titled *"ILOVEYOU.txt.vbs"*.
- **Impact:** Overwrote files and sent itself to all contacts in the victim's Outlook.

## 2. Mydoom (2004)

- **Type:** Email worm
- **Damage:** Estimated **\$38 billion** in global losses.
- **Speed:** One of the **fastest-spreading** email worms ever.
- **Effect:** Opened a backdoor for hackers and launched DDoS attacks.

## 3. Stuxnet (2010)

- **Type:** Worm
- **Target:** Industrial systems (e.g., Iran's nuclear facilities).
- **Origin:** Believed to be state-sponsored (US/Israel).
- **Unique Feature:** First virus known to physically **damage hardware** (centrifuges).

## 4. WannaCry (2017)

- **Type:** Ransomware
- **Spread via:** Windows exploit "EternalBlue".
- **Damage:** Affected **over 200,000 systems** in 150+ countries.
- **Target:** Hospitals, businesses, and governments.

## 5. NotPetya (2017)

- **Type:** Wiper disguised as ransomware
- **Target:** Ukraine (but spread globally)
- **Damage:** Estimated **\$10 billion** in losses.
- **Effect:** Permanently destroyed data on infected machines.

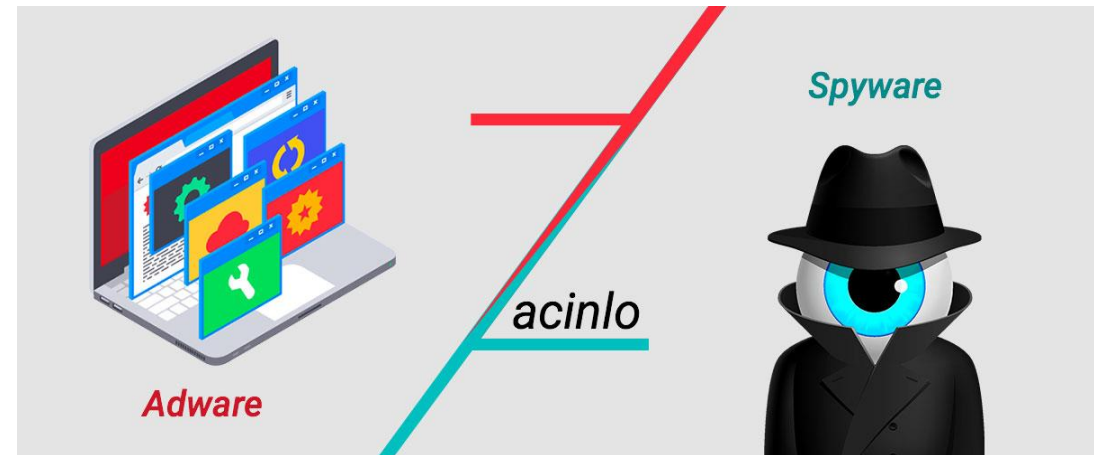
## 6. VenomRAT (2025)

- **Type:** Remote Access Trojan (RAT)
- **How it Works:** Spread through phishing emails with malicious attachments or links. Once installed, it gives attackers **full control** over the infected system.
- **Impact:** Can execute commands, steal data, and download additional malware. Targets sectors like **finance** and **healthcare**.

# Cybersecurity Threat

## 3. Malware

- It is a harmful & malicious program that stops the functioning of the entire system.
- Adware—software that displays unsponsored advertisements
- Spyware—unwanted piggyback software
  - Transmits information
  - Uses tracking cookies
  - Keystroke logger



# Cybersecurity Threat

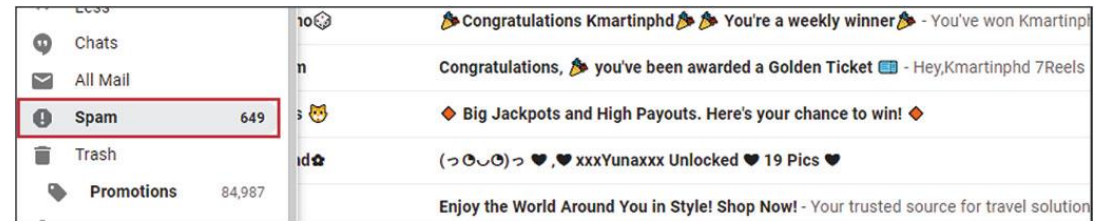
## 4. Botnet

- A botnet consists of a collection of devices interconnected to launch cybercrime. These interconnected devices are controlled by bootmaster.
- Criminals use botnets to launch a DoS (Denial of Service) attack, credential stealing, click fraud, spam sending, bank account & credit card theft and downloading other malware.

# Cybersecurity Threat

## 5. Online Annoyances

- Spam—unwanted software or junk e-mail
- Tactics to minimise spam (spam filter)



Copyright © 2024 by Pearson Education, Inc.

# 5. Online Annoyances

---

- Cookies—small text files received when visiting a website
  - Help companies determine the effectiveness of their marketing
  - They do not search a hard drive for personal information
  - May invade your privacy
  - Pose no security threat

## Two Basic Types of Tracking Cookies



### First Party

Determine users' information relevant to making customers' experience better



### Third Party

Placed on your computer by the ads on pages you visit, even if you don't click on the ads

# Cybersecurity Threat

## 6. Social Engineering

- Change in people's behaviour to indulge in wrong actions with data.
- A technique using social skills to generate human interaction.
- Lures individuals to reveal sensitive information



# Social Engineering

## Phishing

- A trusted resource is imitated to get personal information from people.
- Eg: organisation requesting banking-related information (like credit card/debit card)

## Baiting

- This attack is launched by relying on the greed/curiosity of the people.
- The attacker gives a fake offers to the people to get their personal and sensitive information.

## Vishing

- An attack is launched through VoIP (Voice over IP).
- It involves the spoofing of legitimate phone numbers that lead people to believe that the call is legitimate and share their information.

# Social engineering



**Pretexting**—creating a scenario that sounds legitimate



**Pharming**—malicious code planted on a computer to gather information



**Spear Phishing** - Targeted phishing aimed at specific individuals or organizations using personal details to seem credible.



**Quid Pro Quo** - Offering something in return for information (e.g. fake IT help in exchange for login credentials)



**Smishing (SMS Phishing)** – Using text messages with links or urgent requests to trick victims into revealing data or downloading malware.



# Another Types of Threats

## 7. **Ransomware :**

- Another class of malware from cryptovirology that terrorizes and manipulates public data or suppresses it without their knowledge.

## 8. **Backdoors**

- Allows access to the assets without the user's knowledge.

## 9. **Cryptojacking**

- Cryptojacking is a malicious crypto-mining software used by unauthorised people to mine cryptocurrency.

## 10. **Formjacking**

- Insert malicious JavaScript code into the payment application to seize the customer's details.

# Another Types of Threats

## 11. Cyberbully

- An aggressive, intentional act carried out by a group or individual, using electronic means of interaction, repeatedly and over time, against a victim who cannot easily defend himself or herself.
- Cyberbully content may also be posted anonymously in the form of texts, images or videos.

# Another Types of Threats

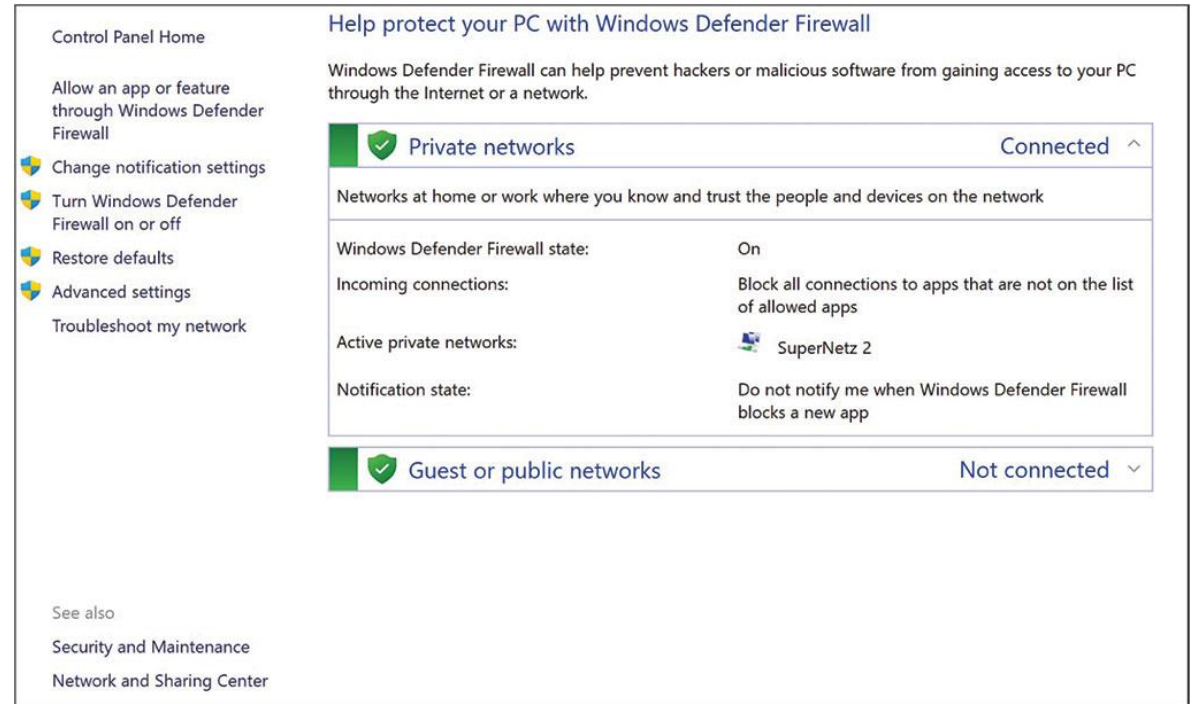
- 12.Scareware**—malware that attempts to convince you something is wrong ... and to pay money to fix it.
- 13.Auto-Playing Media**— Videos or audio that start playing without your consent on websites.
- 14.Chain Messages**— “Forward this to 10 people or something bad will happen!”—a digital version of old-school chain letters.
- 15.Fake Notifications**— Alerts (e.g., “You’ve won!”) that mimic real system messages to grab your attention or trick you.
- 16.Adware**— Software that displays unwanted ads, often bundled with free downloads.

# Cyber Hygiene Essential



# Restricting Access to Your Digital Assets - Firewalls

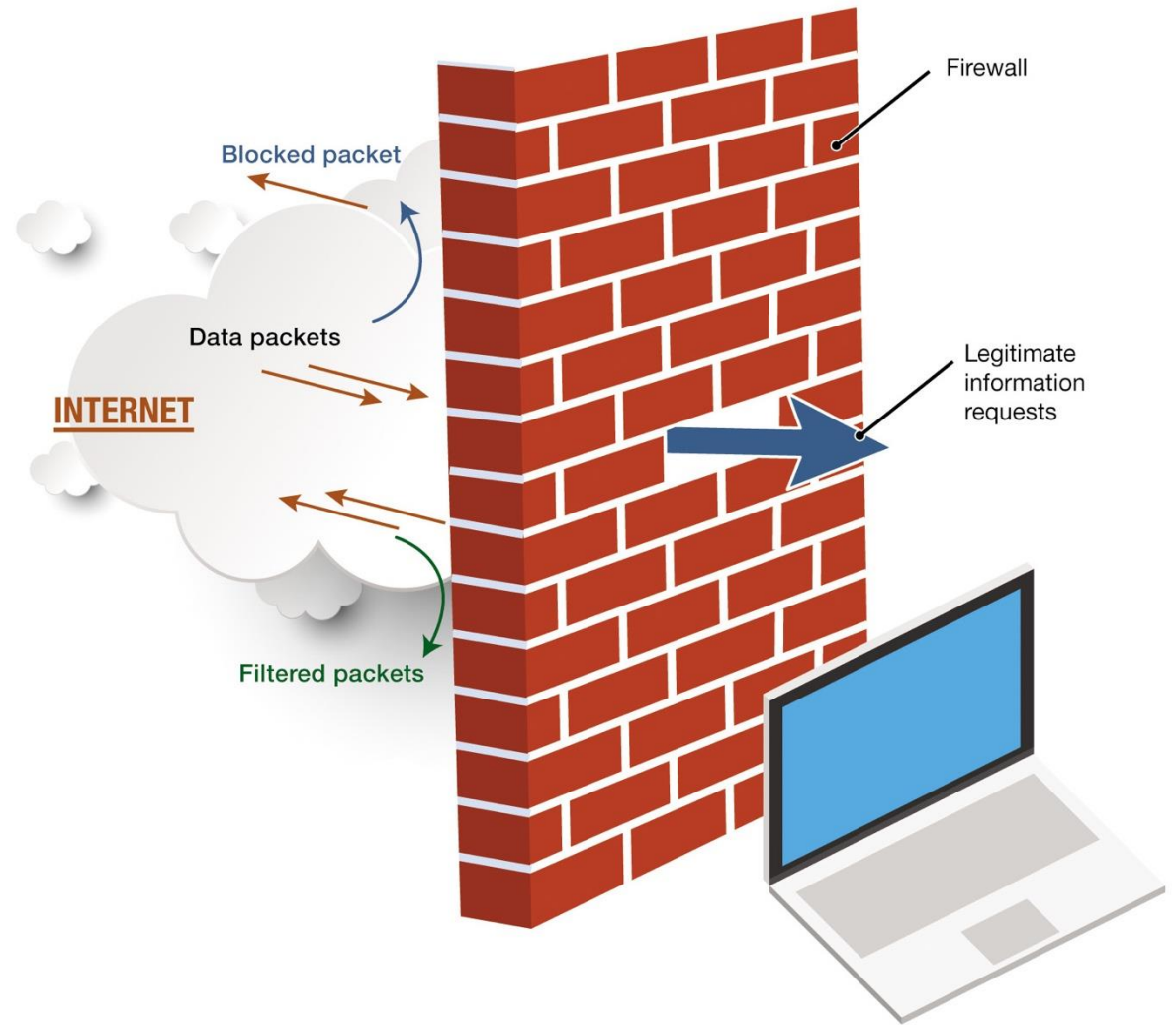
Firewall—software or hardware designed to protect computers from hackers



Copyright © 2024 by Pearson Education, Inc.

# Restricting Access to Your Digital Assets - Firewalls

Windows and macOS provide firewalls





# Restricting Access to Your Digital Assets

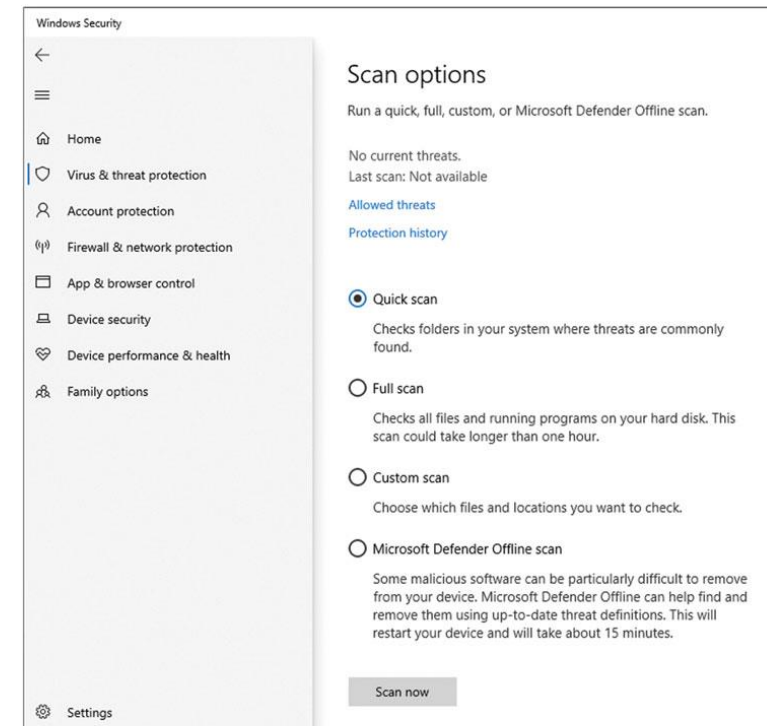
## - Firewalls

- Packet filtering
    - Filter out packets sent to logical ports
  - Logical port blocking
    - Completely refuses requests from the Internet asking for access to specific ports
  - Network address translation (NAT)
    - Assign internal I P addresses on a network
-

# Restricting Access to Your Digital Assets

## - Preventing Virus Infections

- Antivirus software
  - Detects viruses and protects your computer & files from harm.
- Popular programs
  - Norton
  - Trend Micro





# Restricting Access to Your Digital Assets (2 of 3)

## - Preventing Virus Infections

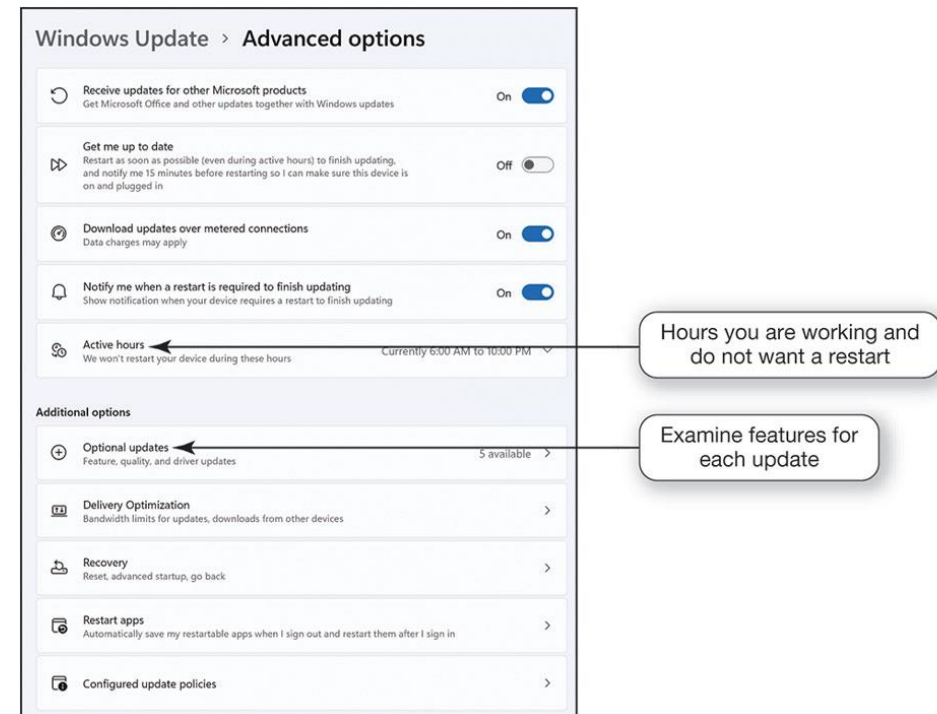
- Virus signature
  - Portion of the virus code that's unique to a particular computer virus
- Quarantining
  - Placing the virus in a secure area so that it won't spread to other files
- Inoculation
  - Records key attributes about your computer files and keeps stats in a secure place



# Restricting Access to Your Digital Assets (3 of 3)

## Preventing Virus Infections

- Drive-by download
  - Exploits weaknesses in operating systems
  - Combat by keeping OS up to date



# Restricting Access to Your Digital Assets (1 of 2)

## Authentication: Passwords and Biometrics

- Strong passwords—at least eight characters and use:
  - Uppercase
  - Lowercase
  - Numeric
  - Symbols

password is weak

Create new password

password

weak

password1 is medium

Create new password

password1

medium

p@ssword1 is strong

Create new password

p@ssword1

strong

# Restricting Access to Your Digital Assets (2 of 2)

## Authentication: Passwords and Biometrics

- Biometric Authentication Devices
  - Fingerprint
  - Iris pattern in the eye
  - Voice authentication
  - Face pattern recognition
  - Provide a high level of security



Copyright © 2024 by Pearson Education, Inc.

# PAY-by-Palm

This iteration of palm payment adopts a dual-factor verification method using palm prints and palm veins, significantly enhancing anti-fraud capabilities, and achieving the media-free, contactless and highly precise user experience.

## How It Works:

1. **Palm Scan** – The user hovers their hand over a palm scanner.
2. **Pattern Recognition** – The system scans vein patterns, which are **unique to every person**, even identical twins.
3. **Match & Approve** – The scan is matched with stored encrypted data to authenticate the user and approve the payment.

## Why It's Secure:

- **Difficult to fake or steal** (unlike passwords or cards)
- **Contactless** – reduces hygiene risks
- Data is often stored in **encrypted form** and linked to a cloud-based secure identity system



## Used By:

- Amazon One (for payments and entry at stores/events)
- Some banks and retail outlets in Japan, China, and the U.S.

# Keeping Your Data Safe (1 of 2)

## Backing Up Your Data

- Backups—copies of files used to replace lost or damaged originals
  - Files to backup
    - Data files
    - Program files
  - Types of backups
    - Full - creates a copy of all application and data files.
    - Incremental (partial b/u)- only backs up files that have changed or have been created since the last backup was performed.
    - Image (System b/u) - that all operating system files are backed up, not just the

# Keeping Your Data Safe (2 of 2)

## Backing Up Your Data

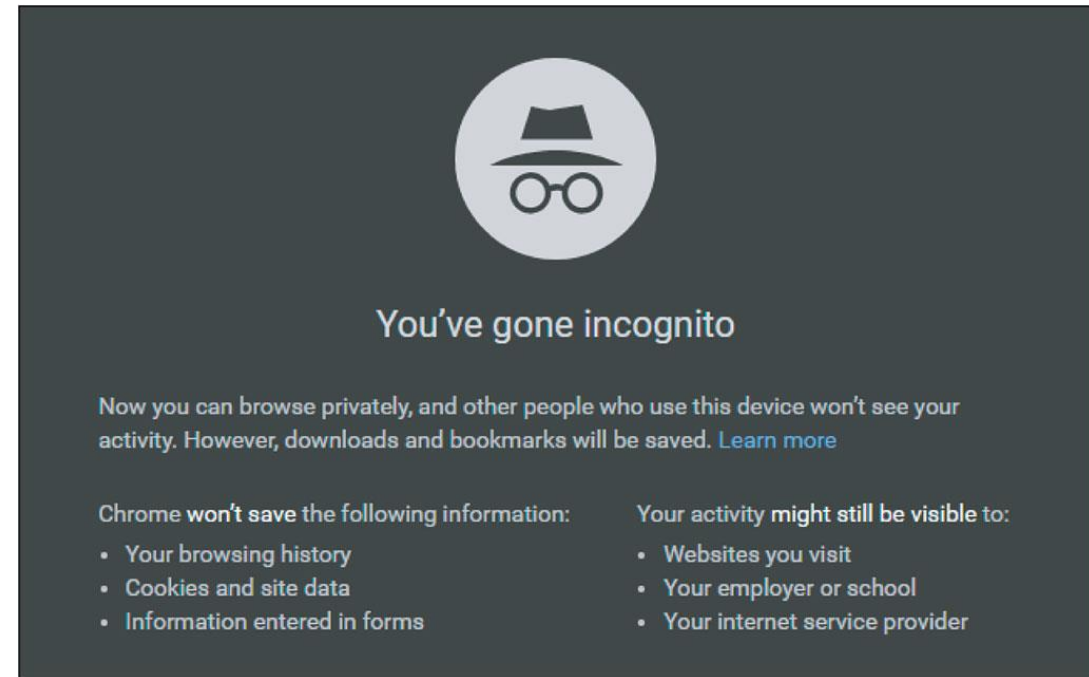
Backup location	Pros	Cons
<b>Online (in the cloud)</b>	<ul style="list-style-type: none"><li>• Files stored at a secure, remote location</li><li>• Files/backups accessible anywhere through a browser</li></ul>	<ul style="list-style-type: none"><li>• Most free storage sites don't provide enough space for image backups</li></ul>
<b>External hard drive</b>	<ul style="list-style-type: none"><li>• Inexpensive, One-time cost</li><li>• Fast backups with U S B 3.0 devices connected directly to your computer</li></ul>	<ul style="list-style-type: none"><li>• Could be destroyed in one event (fire/flood) with your computer</li><li>• Can be stolen</li><li>• Slightly more difficult to back up multiple computers with one device</li></ul>
<b>Network-attached storage device and home server</b>	<ul style="list-style-type: none"><li>• Makes backups much easier for multiple computing devices</li></ul>	<ul style="list-style-type: none"><li>• More expensive than a stand-alone external hard drive</li><li>• Could be destroyed in one event (fire/flood) with your computer</li><li>• Can be stolen</li></ul>



# Restricting Access to Your Digital Assets (1 of 2)

## Anonymous Web Surfing: Hiding from Prying Eyes

- Privacy tools
  - Private Browsing (Mozilla Firefox)
  - InPrivate (Microsoft Edge)
  - Incognito (Google Chrome)
- Virtual private networks (VPNs)
  - Secure networks that are established using the public Internet infrastructure



Copyright © 2024 by Pearson Education, Inc.



# Restricting Access to Your Digital Assets (2 of 2) Multifactor authentication



**Something you KNOW:**  
Something the user knows  
(password, PIN)



**Something you HAVE:**  
Something the user has  
(ATM card, mobile phone,  
YubiKey)



**Something you ARE:**  
Something only the user is  
(fingerprints, iris patterns)



**Strong Authentication:**  
Two of the three factors

(Ground Picture/Shutterstock; Jmiks/Shutterstock; Jamie  
Cross/123RF; Art Pencil Studio/Shutterstock)

Copyright © 2024 by Pearson Education, Inc.

# Protecting Your Physical Computing Assets (1 of 2)

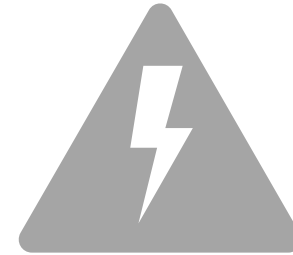
## Environmental Factors and Power Surges

---



### Environmental factor

- Sits on a flat surface
- Don't be exposed to excessive heat/cold
- Avoid food crumbs and liquids



### Power surges

- Old or faulty wiring
- Downed power lines
- Lightning strikes
- Electric substation malfunctions

# Protecting Your Physical Computing Assets (2 of 2)

## Environmental Factors and Power Surges

---

- Surge protector/Whole-house surge protector
  - Replace every 2–3 years
  - Use with all devices that have solid-state components
- Uninterruptible Power Supply (UPS)
  - Battery backup for power outages



Copyright © 2024 by Pearson Education, Inc.

# Protecting Your Physical Computing Assets (3 of 2)

## Environmental Factors and Power Surges

---

- ⚠️ **Teen Electrocuted on Bus While Charging Phone (Malaysia, 2024)**
- **Victim:** Mohamad Nur Asymawi Jasmadi, teen passenger
- **Date:** November 2, 2024
- **Location:** Express bus (Penang Sentral → KL Sentral)
- **Cause: Faulty wiring** in power socket
- **Incident:** Electrocuted while charging phone; witnessed foaming at the mouth
- **Action Taken:**
  - Govt banned **3-pin sockets** on buses
  - Stricter safety checks ordered by Transport Ministry



# Youth electrocuted to death while charging phone on bus

---



A young man died while charging his phone on an express bus at the Penang Sentral bus terminal here yesterday evening (Nov 2). PIC COURTESY OF READER



# Cyber Detox



# Why Do You need a Digital Detox

- All time online can cause:
  - Self-image problems
  - Low self-esteem
  - Sleep problems
  - Depression
  - Anxiety
  - Weight gain
  - Unhealthy eating
  - Lack of exercise
  - Lack of time management
  - Work ethic problems





# Benefits of Digital Detox



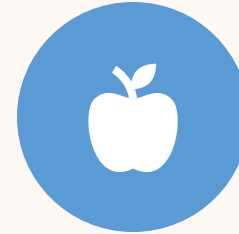
CALM DOWN &  
FELL CONTENT



BE MORE  
PRODUCTIVE



FEEL BETTER  
ABOUT YOURSELF



GET HEALTHIER



SLEEP BETTER

# Strategies for effective cyber detox

- **Established digital boundaries**
  - Set defined periods for device use (e.g., no screens after 9 p.m., tech-free weekends).
  - Create physical boundaries by keeping devices out of bedrooms or during meals.
  - Designate “no tech” zones at home or work.
- **Monitor and limit screen time**
  - Use built-in screen time trackers and apps to monitor usage.
  - Set daily/weekly limits for social media, gaming, or streaming.
  - Identify “digital triggers” (apps, notifications) that drive unhealthy habits and minimize or silence them.

# Strategies for effective cyber detox

- **Promote physical activity**
  - Schedule regular breaks from screens—stand, stretch, or walk every hour.
  - Consider “walk and talk” meetings instead of video calls.
- **Use digital well-being tools**
  - Explore apps that encourage healthy use—meditation, guided breathing, reminder apps for breaks.
  - Leverage device features (night mode, blue-light filters) to reduce eye strain.
- **Sleep hygiene**
  - Remove devices from your sleeping area.
  - Avoid screens at least 30–60 minutes before bedtime, as blue light can disrupt melatonin production and sleep quality.



# Cyber Awareness

# Password Policies Awareness

1

Never reuse or  
recycle  
passwords

2

Never share  
passwords, not  
even with the  
CEO

3

Never write  
passwords down

4

Never store  
passwords in a  
digital file

# Keeping Your Data Safe

## - Protecting Your Personal Information

- Reveal as little information as possible
- In Facebook, change your privacy settings

### Information Identity Thieves Crave



- Social Security Number
- Full Date of Birth
- Phone Number
- Street Address

Never make this information visible on websites!

### Other Sensitive Information



- Full Legal Name
- E-mail Address
- Zip Code
- Gender
- School or Workplace

Only reveal this information to people you know—don't make it visible to everyone!



# Social Networking Sites

- Make sure the social networking sites you visit are safe before sharing any information.
- Learn about their privacy and security settings and use them.
- Be careful with the type of information you share on social networking sites.
- Avoid clicking suspicious links, emails, tweets, posts, and online advertising. These are often how cybercriminals try to steal your personal information or hijack accounts - if it looks suspicious, delete it.
- Use strong passwords, as they will make it more difficult to break into your device if it is lost or stolen.
- As always, keep your software and devices current.
- Use the latest security software, web browsers, and operating systems, and encrypt with a VPN.





# How to prevent phishing attack : Email

---

Sign that an email might be malicious:

- **Poor spelling and grammar:** Professional companies or organizations usually have an editorial staff to ensure customers receive high-quality, professional email content. If an email message is fraught with errors, it is much more likely to be a scam.
- **Suspicious link :** One way of testing the legitimacy of a link is to rest the mouse – without clicking –over the link, to see if the address matches information in the message.
- **Suspicious attachment :** It is recommended that attachments are never opened until their authenticity is verified.
  - The icon associated with an attachment cannot be trusted without other verification.
  - They should be wary of combined file extensions, such as 'pdf.exe', 'rar.exe', or 'txt.hta'.
  - The best course of action, if in doubt, is to contact the person who ostensibly sent the email message in question, to ask them to confirm that the email and attachment are legitimate.

# How to prevent phishing attack : Email

---

- **Coercive messaging:** These emails are meant to cause a sense of panic or pressure, to generate a quick and unconsidered response from the recipient.
  - For example, they may include a statement like, 'You must respond by end of day!' or they may imply that the recipient faces potential financial penalties for failing to respond.
- **Spoofing :** Spoofing emails use **suspicious links** that appear to connect to legitimate websites or companies and may display legitimate-looking pop-up windows, but which take users to phony scam sites. One form of spoofing uses **altered web addresses** that very closely resemble the names of well-known company websites, such as 'www.micorsoft.com' or 'www.mircosoft.com'.
- **Mismatches :** Recipient should be suspicious if the text of a link and URL do not match, or if the sender's name, signature, and URL do not match.

# Guidelines to avoid schemes

---

- Don't click on a link in an e-mail.
- Check with the company asking for information.
- Never give personal information over the Internet unless you know the site is secure.
- Use phishing filters.
- Use Internet security software that's constantly being updated.



# Practical Cyber Hygiene

# Safe browsing practice: Desktop Software

---

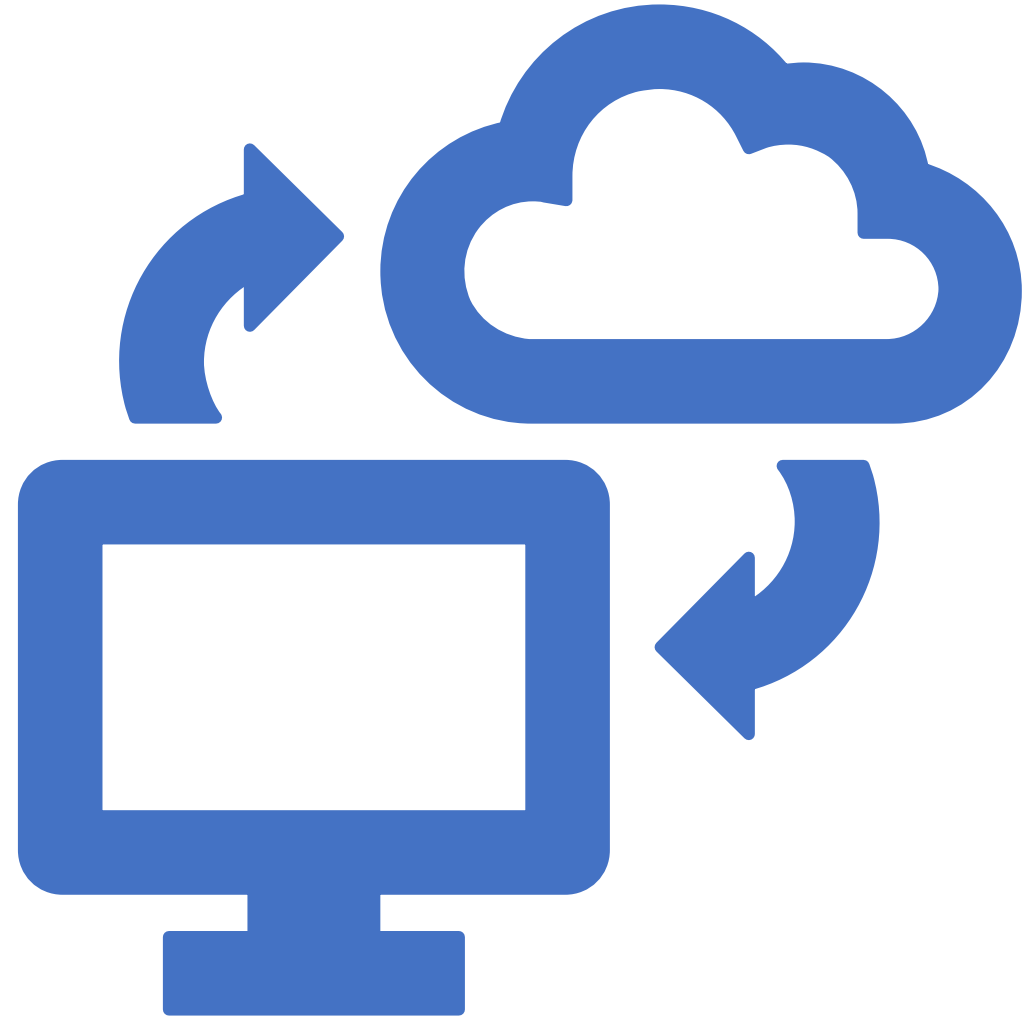
- Use strong passwords and MFA
- Store PCs in a physically secure location
- Lock them when not in use
- Use good antivirus/anti-malware and VPN software
- Enable automatic updates
- Only browse HTTPS websites and keep software properly configured and updated.



## Safe browsing practice: Corporate Network

---

- Limit access.
- Choose internal network sharing on company-owned hardware for sharing, storage, and collaboration.
- Use cloud (Box, OneDrive, or Google Drive).



# Safe browsing practice: Using Public WiFi

---

- Use a VPN on all your devices
- Only visit HTTPS sites that are well-known
- Use your phone as a hotspot. Cellular networks are encrypted
- Disable automatic WI-FI connection settings
- Don't access personal or financial information on public WI-FI

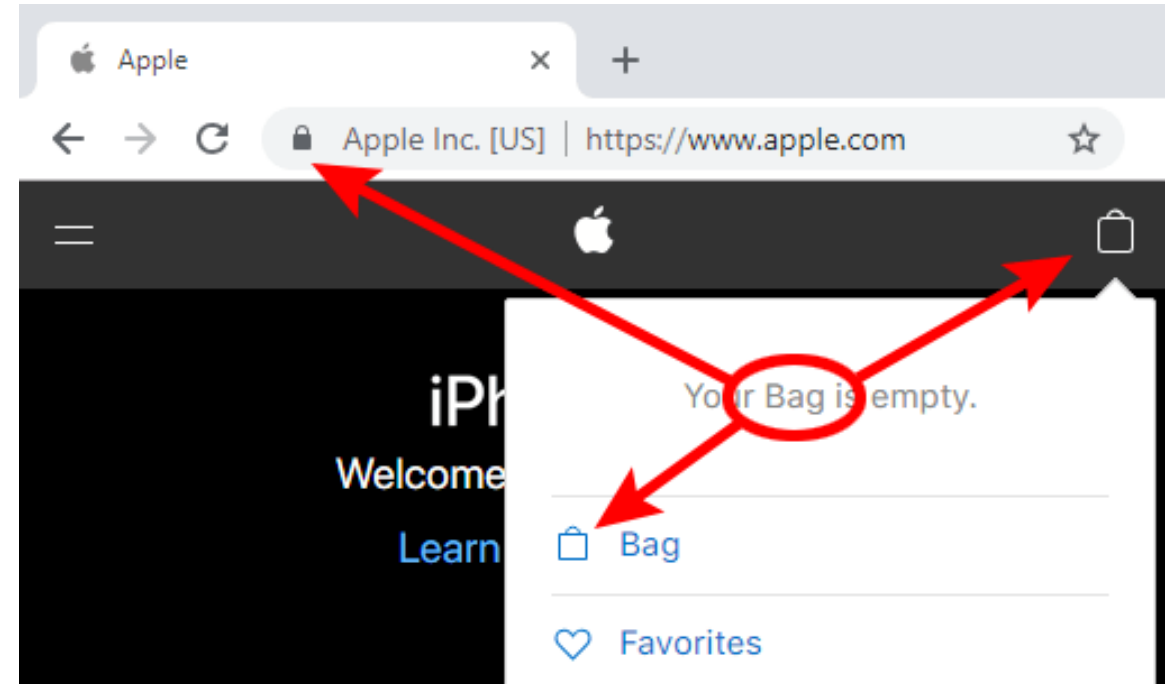




# Safe browsing practice: Internet Browser

---

- HTTP, or HTTPS, protocol provides an encrypted connection between you and the sites that use it.
- How do you know a website you're visiting is using secure HTTP?
  - URL starts with HTTP or HTTPS
  - Lock icon in your browser's URL window

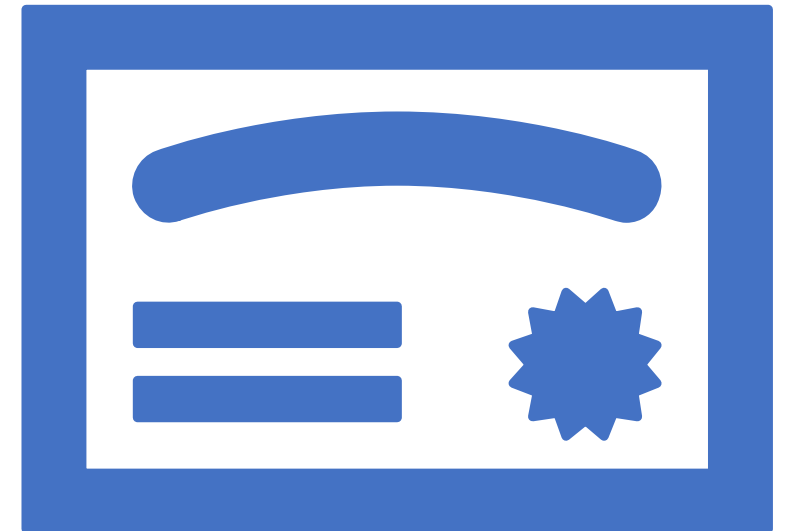


# Safe browsing practice:

## SSL Certificate

---

- Security certificates, or secure sockets layer (SSL) certificates, authenticate a website's identity and enable an encrypted connection between a web server and a browser.
- SSL certificates come from organisations called root certificate stores or **Certificates of Authority (CA)**.
- Businesses need SSL security certificates for their websites so they can:
  - keep user data secure,
  - verify their ownership of the site,
  - prevent attackers from creating fake versions of their site,
  - to convey trust to users.
- They also need them if they want to have an HTTPS web address.





# Protecting Your Physical Computing Assets

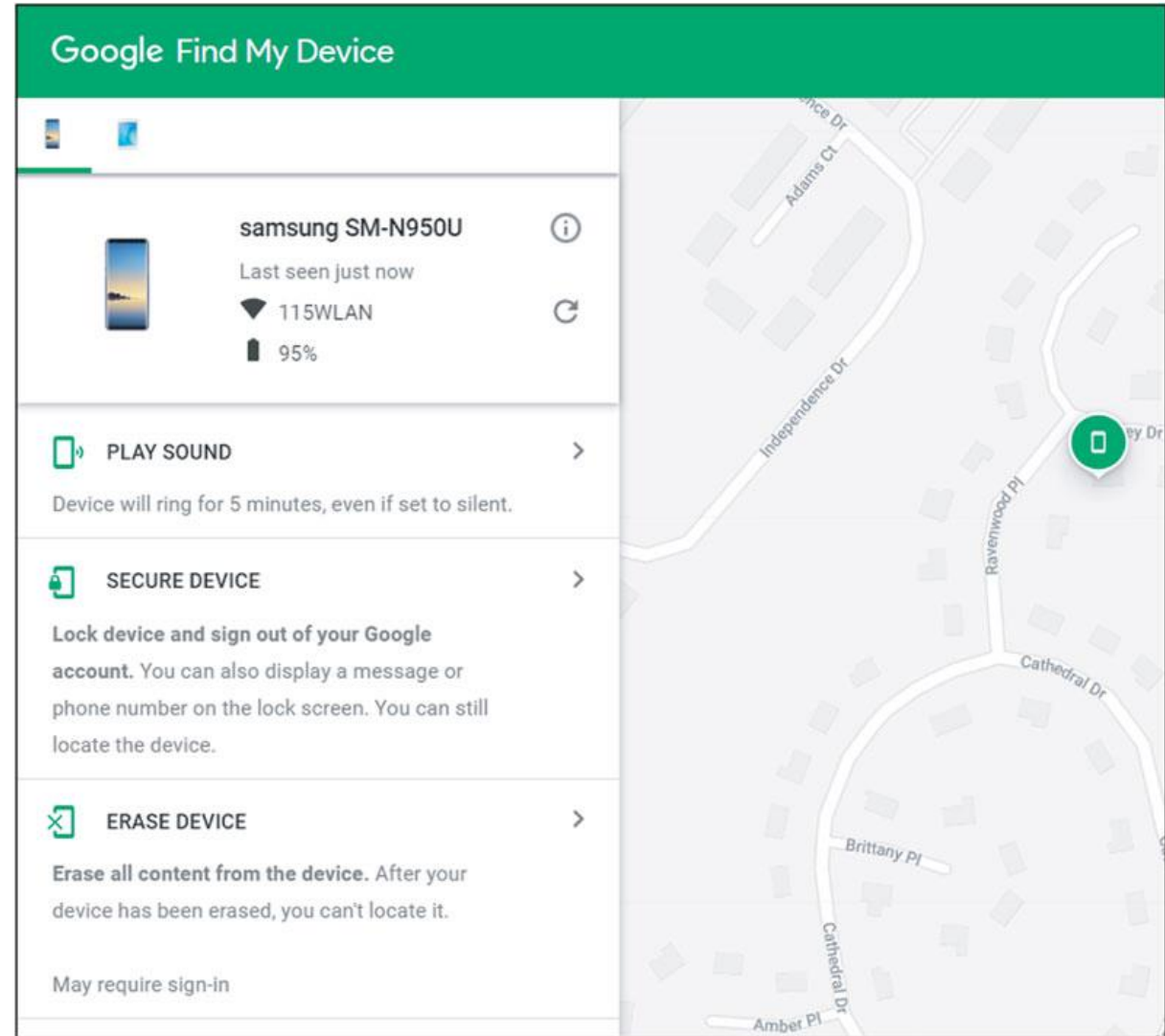
## - Preventing and Handling Theft

- Three main security concerns with devices:
    - Keeping them from being stolen
    - Keeping data secure in case they are stolen
    - Finding a device if it is stolen
-

# Protecting Your Physical Computing Assets

## - Preventing and Handling Theft




Android Device Manager can be used to locate any Android device.



Copyright © 2024 by Pearson Education, Inc.

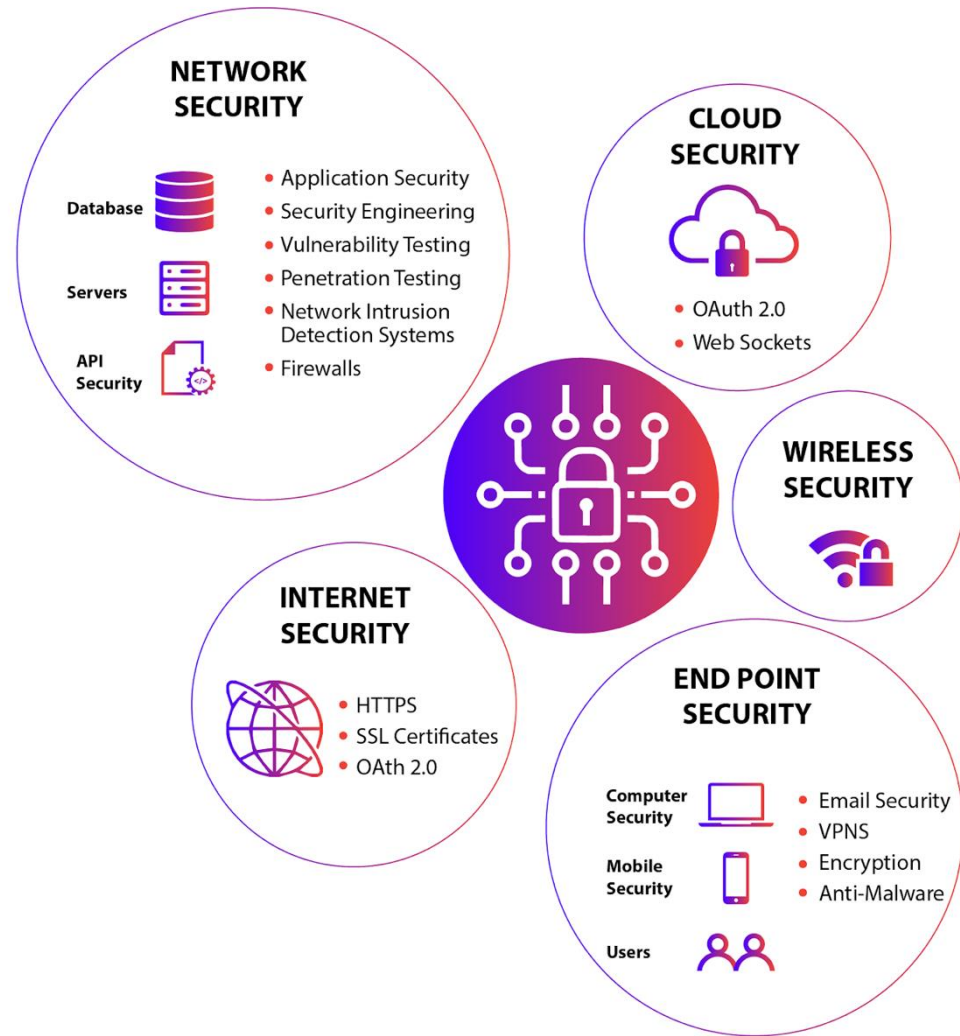
# Protecting Your Physical Computing Assets

## - Preventing and Handling Theft

- Solutions to Device Security Concerns
-  **Data Theft**
  - Use **device encryption** (e.g., BitLocker or FileVault)
  - Enable **remote wipe** for lost/stolen devices
  - Avoid storing sensitive data unnecessarily
-  **Malware Infection**
  - Install and update **reputable antivirus software**
  - Avoid downloading from untrusted sources
  - Keep operating systems and apps **up to date**
-  **Unauthorized Access**
  - Use **strong, unique passwords** or passphrases
  - Enable **screen lock and auto-lock**
  - Activate **two-factor authentication (2FA)**



# What are the main types of device security?



# Risk management

---

Risk management enables proactive identification, prioritization, and handling of cyber threats:

- **Risk Assessments:** Conduct regular reviews using tools and frameworks (NIST, ISO/IEC 27001) to identify vulnerabilities and assess their impact.
- **Mitigation Strategies:** Address risks through multi-layered controls—technical (firewalls, encryption), procedural (policies, training), and people-focused (strong password policies, continuous education).
- **Continuous Monitoring:** Implement systems to monitor network traffic and device behavior for anomalies. Automated alerting allows for timely incident detection.
- **Incident Response Plan:** Draft, review, and regularly test a well-structured incident response plan so all team members know their roles in case of an attack. Simulations help refine the plan.
- **Compliance:** Keep up with evolving regulations and security standards, adapting practices as needed for frameworks like NIST, ISO, CIS, and CISA.

# Incident response and recover

---

- **Incident response and recovery** : critical components of cyber hygiene, aiming to minimize the damage and disruption caused by cyberattacks, restore normal operations, and strengthen defenses for the future.
- **Incident Response**: refer to the structure process organization use to identify, manage, and mitigate cybersecurity threats such as malware, ransomware, and data breaches.
- The goal is to minimize harm, preserve evidence, and restore operations quickly



# Key Steps in Incident Response

---

## 1. Preparation

- Develop and regularly update an incident response plan.
- Assemble and train an incident response team.
- Established tools, procedures and communication strategies for various attack scenarios.

## 2. Detection and Identification

- Monitor systems for signs of malicious activity using security tools (antivirus, SIEM).
- Distinguish actual threats from false positives and document findings, inform stakeholders as needed.

# Key Steps in Incident Response

---

## 3. Containment

- Isolate affected systems to prevent the attack from spreading.
- Apply short-term containment (taking infected devices offline) and long-term containment (segregating sensitive database, strengthening controls).

## 4. Eradication

- Identify all malicious elements (malware, unauthorized user) and remove them from affected systems.
- Update security measures like patching vulnerabilities and changing password to prevent repeat incidents.

# Key Steps in Incident Response

---

## 5. Recovery

- Restore systems and data from clean backups by deploy necessary patches and updates.
- Bring affected devices back online, monitor for residual threats and confirm that operations return to normal safely.

## 6. Lesson learned

- Conduct thorough post-incident analysis to understand what happened, what worked, and what needs improvement.
- Update incident plans and security protocols based on insights gained.
- Train staff and strengthen security posture to prevent future incidents.

# Why incident response & recovery important?

- **Minimizes Damage:** Rapid, organized response prevents further spread and loss, protecting assets and operations.
- **Protects Data:** Quick containment and eradication keep sensitive data safe and help comply with regulations.
- **Ensures Business Continuity:** Effective recovery restores services and reassures customers, reducing downtime and reputational risk.
- **Improves Defenses:** Post-incident reviews drive ongoing improvements in security systems and staff awareness.

# The End

