Unit III: Using Technology Effectively & Responsibly

Chapter 15: Cybersecurity & Privacy

15.1: Goal

In this chapter, you will learn how to protect your personal information and digital devices from online threats. You will explore common cybersecurity risks, discover strategies for staying safe online, and understand the importance of privacy in an increasingly connected world. These skills will help you become a more confident and responsible technology user.

15.2: Objectives

- Explain the importance of cybersecurity and digital privacy.
- Differentiate between cybersecurity, information security, and privacy.
- Identify common cyber threats such as malware, phishing, ransomware, and identity theft.
- Describe best practices for creating and managing strong passwords.
- Explain the purpose of multi-factor authentication (MFA).
- Recognize safe browsing and email practices.
- Describe how encryption protects information.
- Explain how organizations collect and use personal data.
- Apply practical strategies for protecting personal information online.

15.3: Think About It

You receive an email that appears to be from your bank. It warns that your account has been locked and asks you to click a link immediately to verify your identity.

The message looks authentic. It includes the bank's logo, uses professional language, and even addresses you by name. Would you click the link?

Knowing how to recognize cyber threats can protect your money, your identity, and your personal information.

15.4: Opening Scenario

Alex receives a text message claiming that a package cannot be delivered until a small shipping fee is paid. The message includes a link to what appears to be a delivery company's website.

Alex enters a credit card number without thinking twice. Within hours, unauthorized purchases begin appearing on the account.

Later, Alex learns that the message was a phishing scam designed to steal personal and financial information.

By understanding cybersecurity principles and recognizing common warning signs, Alex could have avoided becoming a victim.

15.5: Why This Chapter Matters

Nearly every aspect of modern life depends on digital technology. Banking, shopping, education, healthcare, entertainment, and communication all involve sharing information online.

Unfortunately, cybercriminals constantly develop new ways to steal passwords, install malicious software, and trick people into revealing personal information. While organizations invest heavily in cybersecurity, individuals also play an important role in protecting themselves.

Learning safe online habits can help prevent identity theft, financial loss, and unauthorized access to personal information. Whether you are using a computer, smartphone, or cloud service, cybersecurity is a shared responsibility.

15.6: Behind the Scenes

What Happens When You Log In Securely?

When you sign in to a secure website, much more happens than simply checking whether your password is correct.

1. You enter your username and password.
2. The browser establishes a secure encrypted connection with the website.
3. Your login information is encrypted before it is sent over the Internet.
4. The website compares your credentials with securely stored account information.
5. If multi-factor authentication is enabled, a second verification step confirms your identity.
6. After successful verification, the website creates a secure session that allows you to access your account without sending your password repeatedly.
7. When you sign out or the session expires, the secure connection ends.

This process helps protect your information from interception while proving your identity to the website.

15.7: What Is Cybersecurity?

Cybersecurity is the practice of protecting computers, mobile devices, networks, software, and data from unauthorized access, damage, theft, or disruption. Cybersecurity affects nearly everyone because so much of everyday life depends on digital technology. When you log in to an online class, make a purchase, use mobile banking, send an email, or store photographs in the cloud, cybersecurity measures help protect your information and the systems you use.

Cybersecurity involves both **technology and people**. Organizations use tools such as firewalls, encryption, antivirus software, access controls, and security monitoring to protect their systems. Individuals also play an important role by creating strong passwords, using multi-factor authentication, installing security updates, recognizing phishing attempts, and protecting personal information. Even sophisticated security technology can be defeated when someone is tricked into revealing a password or opening a malicious attachment.

One common way to describe the goals of cybersecurity is the **CIA Triad**:

- **Confidentiality** means information is available only to people who are authorized to see it. For example, only you and authorized medical personnel should be able to access your medical records.
- **Integrity** means information remains accurate and is not improperly changed or destroyed. A student should not be able to change a grade stored in a college database.
- **Availability** means information and computer systems are accessible when authorized users need them. For example, a hospital's computer system must remain available so medical staff can access patient information when needed.

Cybersecurity is about reducing risk, protecting valuable information, detecting problems, and responding effectively when security incidents occur.

It is not possible to eliminate every possible risk, no system can be completely secure.

15.8: Cybersecurity Threats

A **cybersecurity threat** is anything that has the potential to damage a computer system, steal information, disrupt services, or gain unauthorized access to devices or networks. Threats may come from cybercriminals seeking money, individuals trying to steal information, organized groups, or even accidental actions by legitimate users. Understanding common threats can help people recognize problems before serious damage occurs.

Malware is a general term for software intentionally designed to harm a computer, network, or user. Malware can steal information, damage files, monitor activity, or allow an attacker to control a device. Several common types of malware include:

- **Virus:** Malicious code that attaches itself to a file or program and spreads when the infected file is opened or shared.
- **Worm:** Malware that can copy itself and spread from one computer to another through a network without requiring the user to open an infected file.
- **Trojan horse:** Malicious software disguised as a legitimate or useful program. Once installed, it may steal information or give an attacker access to the computer.
- **Ransomware:** Malware that locks a device or encrypts files and demands payment to restore access.

Ransomware can be particularly damaging to businesses, schools, hospitals, and government agencies.

- **Spyware:** Software that secretly collects information about a user's activities. It may monitor browsing activity, capture login information, or collect other personal data.
- **Adware:** Software that displays unwanted advertisements and may track a user's online behavior. Not all adware is malicious, but some can create privacy and security problems.
- **Botnet:** A collection of infected computers and other devices that an attacker controls remotely. Botnets can be used to send spam, spread malware, or overwhelm websites with traffic.

15.9: How Does Malware Get Onto a Computer?

Malware often reaches a device because someone unknowingly opens an infected attachment, clicks a malicious link, downloads software from an untrustworthy source, or uses outdated software containing a security vulnerability. Attackers may also disguise malware as games, utilities, browser extensions, or software updates.

Cybersecurity threats continually change as technology changes. However, one of the most effective defenses remains surprisingly simple: **be cautious about what you click, download, install, and share.** Keeping devices and software updated also helps close security weaknesses that attackers might otherwise exploit.

15.10: Social Engineering

Social engineering is the use of deception or manipulation to persuade people to reveal confidential information, provide access to a system, send money, or perform an action that compromises security. Instead of attacking a computer directly, a social engineer targets the **person using the computer**. Attackers often create a sense of urgency, fear, curiosity, or trust to convince someone to act without carefully considering the request.

For example, a student might receive a message that appears to come from the college saying, “Your account will be disabled today. Click here to verify your password.” The link may lead to a fake login page designed to steal the student's username and password. Social engineering attacks can arrive through email, text messages, telephone calls, social media, or even face-to-face interactions.

Common Types of Social Engineering

- **Phishing:** Fraudulent emails or messages that appear to come from a legitimate organization or person. They often contain malicious links or attachments or ask for sensitive information.
- **Smishing:** Phishing conducted through **SMS or text messages**. A message might claim that a package cannot be delivered or that there is suspicious activity on a bank account.
- **Vishing: Voice phishing** conducted by telephone. A caller may pretend to represent a bank, government agency, technical support department, or other trusted organization.
- **Impersonation:** An attacker pretends to be someone the victim trusts, such as a supervisor, professor, coworker, family member, or company representative.
- **Tech-Support Scam:** A criminal claims that the victim's computer has a virus or other problem and offers to fix it. The victim may be asked to install software that gives the criminal remote access to the computer.
- **Baiting:** An attacker offers something tempting, such as a free download, prize, or gift, to persuade someone to click a link, download a file, or provide information.

Recognizing Social Engineering

Social engineering attempts often include warning signs. Be suspicious of messages that create **extreme urgency**, request passwords or verification codes, demand unusual payments, contain unexpected attachments, or ask you to bypass normal procedures. A message may also come from an address, phone number, or website that looks legitimate at first glance but is slightly different from the real one.

When a request seems suspicious, **do not use the contact information or links contained in the message to verify it**. Instead, contact the person or organization independently using a phone number, website, or other method you already know is legitimate.

AI and Social Engineering

Artificial intelligence can make social engineering more convincing. Generative AI can help criminals create professional-looking phishing messages with fewer spelling and grammar mistakes. AI can also be used to create **deepfake images, videos, and cloned voices** that imitate real people. For example, an attacker might imitate a manager's voice and request an urgent money transfer.

These developments make an important cybersecurity habit even more valuable: **verify the request, not just the identity the message appears to present.** If a message, call, or video asks you to reveal sensitive information, send money, or take an unusual action, verify the request through a separate trusted method before responding.

15.11: Passwords and Authentication

Authentication is the process of verifying that a person attempting to access a computer, account, or network is really who they claim to be. For many years, usernames and passwords have been the most common form of authentication. Today, organizations increasingly use additional methods such as multi-factor authentication, biometrics, and passkeys to provide stronger protection.

Strong Passwords and Passphrases

A strong password should be **long, unique, and difficult to guess**. Length is especially important. A **passphrase**, a sequence of several unrelated words, can be easier to remember while still being difficult to crack. Avoid using easily discovered information such as your name, birthday, pet's name, or common patterns.

One of the greatest password risks is **password reuse**. If you use the same password for several accounts and one organization suffers a data breach, criminals may try the stolen password on your email, banking, shopping, and social media accounts. Each important account should therefore have a different password.

Password Managers

Remembering a unique password for every account can be difficult. A **password manager** is software that securely stores passwords and can generate long, unique passwords for different accounts. The user needs to remember one strong master password or use another secure authentication method to access the password manager.

Password managers can also reduce the temptation to use simple passwords or reuse the same password on multiple websites.

Multi-Factor Authentication

Multi-factor authentication (MFA) requires users to provide two or more forms of evidence before gaining access to an account. Authentication factors generally fall into three categories:

- **Something you know** — a password or PIN
- **Something you have** — a phone, security key, or other trusted device
- **Something you are** — a fingerprint, face, or other biometric characteristic

For example, after entering a password, a user might be required to approve the login on a trusted device. Even if a criminal obtains the password, the additional authentication factor can help prevent unauthorized access.

Biometrics

Biometric authentication identifies people using physical characteristics such as fingerprints, facial features, or other biological traits. Smartphones and computers commonly use fingerprint readers and facial recognition to unlock devices.

Biometrics are convenient because users do not have to remember them. However, biometric information must be protected carefully. Unlike a password, a person's fingerprint or face cannot simply be changed if biometric data is compromised.

Passkeys

A **passkey** is a newer authentication method designed to reduce dependence on traditional passwords.

Passkeys use cryptographic technology and are typically unlocked with the same method used to unlock a device, such as a fingerprint, facial recognition, or PIN. The secret information needed for authentication is not sent to the website during login.

Passkeys also provide strong protection against many phishing attacks because they are associated with the legitimate website or service. A fake login page cannot simply trick a user into typing in a reusable password.

Good Authentication Habits

Students should remember a few basic practices: use **long and unique passwords**, consider using a **password manager**, enable **MFA whenever possible**, and use **passkeys when they are available and appropriate**. Never give another person your password or an authentication code simply because they ask for it. A request for an MFA code may itself be part of a social engineering attack.

15.12: Protecting Your Devices

Computers, smartphones, and tablets contain a great deal of valuable information, including photographs, email, schoolwork, financial information, passwords, and access to online accounts. Protecting a device involves more than preventing someone from physically stealing it. Users must also protect devices from malware, unauthorized access, software vulnerabilities, and data loss.

Keep Software Updated

Operating systems, applications, browsers, and other software should be kept **up to date**. Software sometimes contains security weaknesses called **vulnerabilities**. When developers discover these weaknesses, they may release a **security patch** to correct them. Installing updates promptly reduces the opportunity for attackers to exploit known vulnerabilities. Automatic updates can make this process easier.

Use Antivirus and Anti-Malware Software

Antivirus and anti-malware software can detect, block, and remove many types of malicious software. Modern operating systems often include built-in security tools, but these tools must be kept updated to recognize new threats. Security software provides an important layer of protection, but it cannot replace safe behavior when downloading files or clicking links.

Use a Firewall

A **firewall** monitors network traffic entering and leaving a computer or network and can block connections that violate security rules. Firewalls may be built into an operating system, included in a home router, or used by organizations to protect an entire network.

Think of a firewall as a **security checkpoint** between a device or network and the outside world. It allows acceptable network traffic to pass while helping block suspicious or unauthorized connections.

Lock Your Devices

Computers and mobile devices should be protected with a **PIN, password, passkey, fingerprint, or facial recognition**. Devices should also be configured to lock automatically after a period of inactivity. A screen lock can prevent someone who finds or steals a device from immediately accessing its contents.

Use Device Encryption

Encryption converts readable information into a coded form that cannot easily be understood without the appropriate key. Many modern computers and smartphones can encrypt the information stored on the device. If an encrypted device is lost or stolen, encryption can make it much more difficult for someone to access the files stored on it.

Install Software Carefully

Applications should be downloaded from **trusted sources**, such as official app stores or the software developer's legitimate website. Free programs, browser extensions, games, and fake software updates can sometimes contain malware.

Before installing an application, consider whether you recognize the developer and whether the program really needs the permissions it requests. For example, a simple calculator application probably does not need access to your contacts, microphone, and location.

Back Up Important Files

A **backup** is an additional copy of important data stored separately from the original. Backups can help recover files if a device is damaged, lost, stolen, infected with ransomware, or experiences hardware failure.

Important files can be backed up to an external storage device, a cloud service, or both. Automated backups are particularly helpful because they do not depend on the user remembering to make copies manually. **Layers of Protection**

No single security measure can protect a device from every threat. Effective cybersecurity uses **multiple layers of protection**. Keeping software updated, using security tools, locking and

encrypting devices, installing software carefully, and maintaining backups work together to reduce risk. This approach is sometimes called **defense in depth**—if one security measure fails, another may still help protect the device and its data.

15.13: Network and Wi-Fi Security

Computers, smartphones, smart televisions, printers, and many other devices connect to networks to communicate and access the Internet. Because information travels across these networks, an insecure network can create opportunities for attackers to intercept information, gain unauthorized access, or compromise connected devices. **Network security** involves protecting networks and the devices and data that use them.

Securing Your Home Wi-Fi

A home wireless network should be protected with a **strong, unique Wi-Fi password** and modern wireless security. Current routers generally support **WPA2 or WPA3 encryption**, with WPA3 providing newer protections when supported by your devices.

The router's administrative account should also have a strong password that is different from the Wi-Fi password. Routers should be kept updated because manufacturers may release firmware updates that correct security vulnerabilities.

It is also a good idea to change default router settings when necessary. Default administrator usernames and passwords can sometimes be widely known, making an improperly configured router easier to attack.

Public Wi-Fi

Free Wi-Fi is convenient in airports, hotels, libraries, restaurants, and other public places, but users should be cautious when using networks they do not control. A criminal may create a **fake Wi-Fi hotspot** with a name similar to that of a legitimate business in hopes that people will connect to it.

Before joining a public network, verify its correct name when possible. Avoid sending highly sensitive information over networks you do not trust, and turn off automatic Wi-Fi connections so that your device does not connect to unfamiliar networks without your knowledge.

HTTPS and Secure Websites

When visiting a website, look for **HTTPS** at the beginning of the web address. HTTPS uses encryption to protect information traveling between your browser and the website.

HTTPS is especially important when entering passwords, payment information, or other sensitive data. However, HTTPS does **not** guarantee that a website itself is trustworthy. A fraudulent website can also use HTTPS. Users still need to verify that they are visiting the correct website.

Routers and Firewalls

A **router** directs data between devices on a local network and other networks, including the Internet. Most home routers also include firewall features.

A **firewall** monitors network traffic and helps prevent unauthorized connections. Organizations may use more advanced firewalls and network security systems to monitor large amounts of traffic and identify suspicious activity.

Virtual Private Networks (VPNs)

A **Virtual Private Network (VPN)** creates an encrypted connection between a device and a VPN service or an organization's network. Businesses and colleges may use VPNs to allow employees or students to securely access internal resources from another location.

Commercial VPN services can also provide additional protection for network traffic, particularly on networks you do not control. However, a VPN does **not** make a person anonymous or protect against every cybersecurity threat. It cannot prevent someone from entering a password into a phishing site, downloading malware, or falling for a scam.

Think Before You Connect

Network security involves both technology and good decisions. Secure your home Wi-Fi, keep your router updated, be cautious when connecting to public networks, and verify websites before entering sensitive information. A useful rule to remember is: **just because a network is available does not mean it is safe to use.**

15.13: Protecting Personal Information

Every time people shop online, use social media, complete a form, visit a doctor, attend school, or use a mobile app, they may provide personal information. Protecting this information is an

important part of cybersecurity because criminals can use stolen information to commit fraud, access accounts, or impersonate another person.

Personally Identifiable Information (PII)

Personally identifiable information (PII) is information that can identify a specific individual, either by itself or when combined with other information. Examples include a person's full name, home address, telephone number, email address, date of birth, driver's license number, and Social Security number.

Some information requires especially careful protection. Financial account numbers, passwords, authentication codes, government identification numbers, and other sensitive records should not be shared unless there is a legitimate reason and the recipient can be trusted.

Identity Theft

Identity theft occurs when someone uses another person's personal information without permission, often for financial gain. A criminal might use stolen information to open an account, make purchases, apply for credit, or attempt to gain access to existing accounts.

Identity theft can result from phishing, stolen passwords, malware, lost devices, mail theft, scams, or information exposed in a data breach. Protecting personal information therefore requires both good cybersecurity practices and careful decisions about when and where information is shared.

Data Breaches

A **data breach** occurs when confidential or sensitive information is accessed, exposed, or stolen by an unauthorized person. Businesses, schools, hospitals, government agencies, and other organizations can experience data breaches.

If an organization you use reports a breach, determine what type of information was affected. Depending on the situation, you may need to change a password, monitor financial accounts, replace a payment card, or take other protective measures.

Be Careful What You Share

Information does not have to be stolen from a computer to create a security risk. People sometimes voluntarily reveal information that criminals can use. Social media posts may reveal birthdays, family members, workplaces, travel plans, or other details.

Before posting information online, consider **who can see it, how it might be used, and whether it needs to be shared at all**. Privacy settings can help limit access, but they should not be considered a guarantee that information will remain private.

Protect Financial and Account Information

Never provide passwords, PINs, or multi-factor authentication codes in response to an unexpected email, text message, or telephone call. Be particularly cautious when someone creates a sense of urgency or asks for immediate payment.

When accessing financial or other sensitive accounts, use the organization's official app or navigate to its known website rather than following an unexpected link. Regularly reviewing account activity can also help identify unauthorized transactions quickly.

Your Information Has Value

Personal information has value even when it may seem unimportant. A single piece of information may not be enough to commit fraud, but criminals can combine information collected from **data breaches, social media, public records, and scams** to create a more complete picture of an individual. A good cybersecurity habit is to treat personal information as a valuable resource: **know what you are sharing, why it is needed, and who will have access to it.**

15.14: Cybersecurity and Artificial Intelligence

Artificial intelligence is changing cybersecurity in two important ways. Cybercriminals can use AI to make attacks more convincing and efficient, while cybersecurity professionals can use AI to identify and respond to threats. As AI tools become more widely available, understanding both sides of this relationship is increasingly important.

AI-Generated Phishing and Scams

Traditional phishing messages often contained spelling errors, awkward wording, or other clues that made them easier to recognize. **Generative AI** can produce polished emails, text messages, and social media posts that closely resemble legitimate communications. Attackers may also use information found online to personalize a message for a particular person or organization.

As a result, users should not assume that a professional-looking message is legitimate. Unexpected requests for passwords, authentication codes, money, or sensitive information should always be verified independently.

Deepfakes and Voice Cloning

AI can create realistic-looking images, video, and audio of people saying or doing things that never occurred. This type of manipulated media is often called a **deepfake**. AI can also be used for **voice cloning**, creating audio that sounds like a particular person.

A criminal might imitate a family member asking for emergency money or impersonate an executive requesting a financial transaction. Because seeing a face or hearing a familiar voice may no longer be sufficient proof of identity, people should verify unusual or urgent requests through a separate trusted method.

AI-Assisted Cyberattacks

Cybercriminals can use AI to assist with tasks such as researching potential targets, creating fraudulent messages, analyzing stolen information, or modifying malicious software. AI may allow attackers to perform some tasks more quickly and at a larger scale.

However, AI does not eliminate the need for attackers to find a way into a system. Basic security practices— including software updates, strong authentication, careful handling of links and attachments, and limited access privileges—remain important defenses.

AI as a Cybersecurity Tool

Cybersecurity professionals also use **AI and machine learning to defend systems**. Security systems can analyze large amounts of network and computer activity and look for patterns that may indicate an attack.

For example, an AI-based security system might notice that an employee's account suddenly attempts to access hundreds of files at an unusual time or logs in from an unexpected location. The system can flag the activity for investigation or, in some cases, automatically take protective action.

AI can help cybersecurity teams:

- Detect unusual network activity
- Identify possible malware

- Analyze large amounts of security data
- Detect fraudulent transactions
- Prioritize security alerts
- Identify patterns associated with previous attacks

AI Is Not a Perfect Security Solution

AI systems can make mistakes. They may identify legitimate activity as suspicious, fail to recognize a new type of attack, or produce inaccurate conclusions. Attackers may also deliberately attempt to deceive AI based security systems.

For these reasons, AI is best viewed as **another cybersecurity tool rather than a replacement for human judgment**. Security professionals still need to investigate alerts, make decisions, establish policies, and respond to incidents.

Verify, Even When It Looks Real

AI makes it increasingly difficult to judge authenticity based only on appearance, writing quality, or even a familiar voice. A useful cybersecurity principle for the AI era is: **when a request involves money, sensitive information, passwords, or unusual actions, verify it through a second trusted method before responding.**

15.15: Cybersecurity in Organizations

Businesses, colleges, hospitals, government agencies, and other organizations store large amounts of valuable information and depend on computer systems for their daily operations. A successful cyberattack can expose confidential information, interrupt services, cause financial losses, and damage an organization's reputation. For this reason, cybersecurity is the responsibility of **everyone in an organization—not just the IT department**.

Employee Responsibilities

Employees are often the first line of defense against cyberattacks. They should follow their organization's security policies, protect passwords, use multi-factor authentication, install approved software only, and report suspicious activity. Employees must also learn to recognize phishing attempts and other forms of social engineering.

Even an accidental action, such as sending confidential information to the wrong person, clicking a malicious link, or losing an unlocked laptop, can create a security incident.

Access Controls and Permissions

Not everyone in an organization should have access to every file or system. **Access controls** determine which resources a user is permitted to view, modify, or use.

For example, a college student might be able to view their own grades but not change them. An instructor may be able to enter grades for students in their classes, while certain administrators may have broader access to academic records. Access controls help prevent both accidental and intentional misuse of information.

The Principle of Least Privilege

The **principle of least privilege** means that users should receive only the access necessary to perform their jobs. An employee who does not need access to payroll records, for example, should not have permission to view them.

Limiting privileges reduces the potential damage if an account is compromised. If an attacker steals an employee's login credentials, the attacker is limited to the resources that account can access.

Security Policies

Organizations establish **security policies** that describe how employees should use technology and protect information. Policies may cover passwords, mobile devices, remote work, email, software installation, data storage, social media, and acceptable use of organizational computers.

Security policies are effective only when employees understand and follow them. Organizations therefore combine policies with training and technical security controls.

15.16: Cybersecurity Training

Because many attacks target people rather than technology, organizations often provide **security awareness training**. Employees may learn how to recognize phishing messages, protect confidential information, use secure authentication, and report suspicious activity.

Some organizations conduct simulated phishing exercises in which employees receive harmless test messages designed to resemble phishing attacks. These exercises can help employees practice identifying suspicious messages.

Incident Response

Despite strong security measures, security incidents can still occur. An **incident response plan** explains what an organization should do when a cyberattack, data breach, malware infection, or other security event is discovered.

Incident response generally involves identifying the problem, containing the damage, removing the threat, recovering systems and data, and determining what can be done to prevent a similar incident in the future. Organizations may also have legal or regulatory responsibilities to notify affected individuals or government agencies after certain types of data breaches.

The Human Factor

Technology such as firewalls, encryption, security software, and monitoring systems provides important protection, but people remain an essential part of cybersecurity. Attackers frequently target employees because convincing one person to reveal information or approve an unauthorized request may be easier than defeating sophisticated security technology.

Creating a strong **security culture** means encouraging employees to think carefully, follow security procedures, and report possible problems quickly. Employees should feel comfortable reporting a mistake or suspicious event because **early reporting can help an organization limit the damage from a cyberattack.**

15.17: Cybercrime and Cybersecurity Careers

As computers and networks have become essential to everyday life, **cybercrime** has become a major concern for individuals, businesses, schools, governments, and other organizations. Cybercrime refers to illegal activities involving computers, networks, or digital information. At the same time, the need to prevent and investigate cybercrime has created many career opportunities in cybersecurity.

What Is Cybercrime?

Cybercrime includes criminal activities in which computers or networks are the target of a crime or are used to commit one. Examples include stealing personal information, gaining unauthorized access to computer systems, distributing malware, conducting ransomware attacks, committing online fraud, and stealing digital information.

Some cybercrimes are committed for financial gain, while others may involve espionage, disruption, harassment, or theft of intellectual property. Cybercrime can affect a single individual or disrupt the operations of a large organization.

Computer Laws

Laws prohibit many forms of unauthorized computer access, fraud, identity theft, and theft of digital information. Cybersecurity professionals need to understand that having the technical ability to access a computer system does not mean they have the legal right to do so.

Authorization is especially important in cybersecurity. Security testing should be performed only on systems for which the individual has been given appropriate permission.

Ethical Hacking

An **ethical hacker** uses hacking techniques with authorization to identify security weaknesses before criminals can exploit them. Ethical hackers may attempt to find vulnerable software, weak passwords, improper permissions, or other security problems.

The key difference between ethical hacking and malicious hacking is **permission and purpose**. Ethical hackers work within an agreed scope and report the weaknesses they discover so they can be corrected.

Cybersecurity Careers

Cybersecurity includes many different career paths, and not every cybersecurity professional performs the same type of work.

Career	What the Person Does
Cybersecurity Analyst	Monitors systems and networks, investigates suspicious activity, and helps protect an organization's information.
Security Engineer	Designs, implements, and maintains systems and tools used to protect networks and data.
Penetration Tester	Conducts authorized tests of systems to identify security weaknesses.
Digital Forensics Investigator	Collects and analyzes digital evidence following cybercrimes or security incidents.
Incident Response Specialist	Investigates security incidents and helps contain attacks and restore systems.
Security Administrator	Manages security settings, user access, permissions, and security technologies.
Security Consultant	Advises organizations about cybersecurity risks, policies, and protection strategies.

Skills for Cybersecurity Careers

Cybersecurity professionals need technical knowledge of computers, operating systems, networks, software, and security technologies. However, technical ability is only part of the job. **Problem-solving, communication, teamwork, attention to detail, and ethical decision-making** are also important.

Cybersecurity professionals frequently work with people outside the IT department. For example, an analyst may need to explain a security risk to managers who do not have a technical background.

Education and Certifications

People enter cybersecurity careers through many paths, including college degrees, technical programs, internships, military experience, industry training, and professional certifications. Entry-level certifications can demonstrate knowledge of basic networking and cybersecurity concepts, while more advanced certifications may focus on areas such as security management, penetration testing, cloud security, or digital forensics.

A Growing Field

Cybersecurity offers opportunities in nearly every industry because almost every organization depends on computers and data. Banks need to protect financial information, hospitals must safeguard patient records, colleges protect student information, retailers secure payment systems, and governments maintain critical systems.

For students interested in **technology, problem-solving, investigation, and protecting others**, cybersecurity can provide a wide range of career possibilities.

15.18: Everyday Cybersecurity: Protecting Yourself

Cybersecurity may seem highly technical, but many of the most effective security practices are simple habits that anyone can use. Every person who owns a smartphone, uses email, shops online, attends school, or uses social media has information worth protecting. Developing good cybersecurity habits can reduce the risk of identity theft, malware, fraud, and unauthorized access to accounts.

Use Strong, Unique Passwords

Use a **different password or passphrase for each important account**. A password manager can create and securely store unique passwords so you do not have to remember all of them. When passkeys are available, they can provide a convenient and phishing-resistant alternative to traditional passwords.

Turn On Multi-Factor Authentication

Enable **multi-factor authentication (MFA)** for important accounts, particularly email, financial, school, and social media accounts. MFA provides an additional layer of protection if someone obtains your password. Never give an unexpected caller or message sender an authentication code.

Keep Your Software Updated

Install updates for your operating system, browser, applications, and mobile devices. Updates frequently contain **security patches** that correct known vulnerabilities. Enabling automatic updates can help ensure that important security fixes are installed promptly.

Think Before You Click

Be cautious with unexpected links, attachments, QR codes, and downloads. A message that appears to come from a bank, employer, college, friend, or government agency could be fraudulent.

Pay particular attention to messages that create urgency: *Act immediately. Your account will be closed. Your payment failed. You have won a prize.* Instead of following the link in the message, contact the organization through a method you already know is legitimate.

Back Up Important Files

Keep backups of important documents, photographs, schoolwork, and other files. Backups can help you recover from hardware failure, theft, accidental deletion, or ransomware. Important information can be backed up to cloud storage, an external storage device, or both.

Protect Your Personal Information

Think carefully before providing personal information online. Do not share passwords, PINs, Social Security numbers, financial information, or authentication codes unless there is a legitimate reason to do so.

Also consider what you reveal through social media. Birthdays, travel plans, locations, photographs, and other seemingly harmless information can sometimes provide useful information to scammers.

Secure Your Devices

Protect smartphones, tablets, and computers with a PIN, password, fingerprint, facial recognition, or another secure authentication method. Configure devices to lock automatically when they are not being used.

Avoid leaving unlocked devices unattended, particularly in public places.

Review Privacy and Security Settings

Periodically review the privacy settings on social media accounts, apps, browsers, and other online services. Check which applications have permission to use your **location, camera, microphone, contacts, and photographs**, and remove permissions that are unnecessary.

Verify Unusual Requests

Artificial intelligence has made it easier to create convincing emails, images, videos, and even cloned voices. Do not rely only on how professional a message looks or whether a caller sounds familiar.

If someone unexpectedly asks for money, sensitive information, a password, or an unusual action, **verify the request using another trusted method**. For example, call the person using a telephone number you already know rather than a number provided in the suspicious message.

Stop, Think, Verify

You do not need to be a cybersecurity expert to protect yourself. Three words summarize one of the most useful habits in cybersecurity:

Stop. Think. Verify.

Before clicking a link, downloading a file, providing personal information, or responding to an unusual request, take a moment to consider whether it makes sense and verify it when necessary. Small security habits practiced consistently can prevent many common cybersecurity problems.

15.19: Chapter Summary

Cybersecurity involves protecting computers, networks, accounts, and personal information from digital threats. Because many attacks rely on human error rather than technical weaknesses, practicing safe online habits is one of the most effective defenses. Strong passwords, multi-factor authentication, software updates, secure browsing, and awareness of scams all contribute to a safer digital experience. Understanding privacy also helps individuals make informed decisions about how their personal information is collected, shared, and protected online.