Aerospace Dimensions

CYBER SECURITY

MODULE 7

Civil Air Patrol
Maxwell Air Force Base, Alabama

Aerospace Dimensions

CYBER SECURITY

MODULE 7

WRITTEN BY
LACY WICKS
JEFF CARVER, Ph.d.
TRAVIS ATKINSON, Ph.d.

DESIGN
BLAKE ATKINS

ILLUSTRATIONS
LACY WICKS
BLAKE ATKINS

EDITING
JEFF CARVER, Ph.d.
TRAVIS ATKINSON, Ph.d.

NATIONAL ACADEMIC STANDARD ALIGNMENT
SUE MERCER

THE UNIVERSITY OF
ALABAMA

PUBLISHED BY
NATIONAL HEADQUARTERS
CIVIL AIR PATROL
CADET PROGRAMS
MAXWELL AFB, ALABAMA
36112

FIRST EDITION
JANUARY 2022

Introduction

The Aerospace Dimensions module, ***Cyber Security***, is the seventh of seven modules, which combined make up Phases I and II of Civil Air Patrol's Aerospace Education Program for cadets. Each module stands entirely on its own so that each can be taught in any order. This organization of modules enables new cadets coming into the program to study the same module, at the same time, with the other cadets. This arrangement builds cohesiveness and cooperation among the cadets and encourages active group participation. This module is also appropriate for middle school students and can be used by teachers to supplement STEM-related subjects.

Inquiry-based activities are included to enhance the text and provide concept applicability. The activities are designed as group activities, but can be done individually, if desired. The activities for this module are located at the end of each chapter.

Contents

K12 Cybersecurity Learning Standards

Cyber.org
The Academic Initiative of the Cyber Innovation Center
https://cyber.org/sites/default/files/2021-08/K-12%20Cybersecurity%20Learning%20Standards_2.pdf

Computing Systems

Communication and Networking
- 6-8.CS.COMM.1 Compare and contrast network topologies.

Network Components
- 6-8.CS.COMP identify the role of connected network components.

Software Updates
- 6-8.CS.SOFT identify examples of vulnerabilities that exist in software.

Programming and Scripting
- 6-8.CS.PROG Explain the role of scripting in cyber attacks.

Applications
- 6-8.CS.APPS Discuss the role that software plays in the protection of a secure system.

Digital Citizenship

Cyberbullying
- 6-8.DC.CYBL Develop strategies to raise awareness of the effects of, and methods to identify and prevent, cyberbullying.

Digital Footprint
- 6-8.DC.FOOT.1 Recognize the many sources of data that make up a digital footprint.
- 6-8.DC.FOOT.2 Recognize the permanence of a digital footprint.

Public and Private Information
- 6-8.DC.PPI.1 Discuss the risks and benefits of sharing PII.
- 6-8.DC.PPI.2 Examine techniques to detect, correct, and prevent disclosure of PII.

Threat Actors
- 6-8.DC.THRT Describe various types of threat actors.

Ethical Integrity
- 6-8.DC.ETH Distinguish between ethical and malicious hacking.

Intellectual Property
- 6-8.DC.IP Explain how intellectual property and copyright relate to fair use.

Security

Threats and Vulnerabilities
- 6-8.SEC.INFO Analyze threats and vulnerabilities to information security for individuals and organizations.

Securing Network Components
- 6-8.SEC.COMP Describe Defense in Depth strategies to protect simple networks.

Threats and Vulnerabilities
- 6-8.SEC.NET Explain how malicious actions threaten network security.

1 INTRODUCTION TO CYBER SECURITY

Learning Outcomes

- Describe the composition of cyberspace.
- Explain the role of cyber security in cyberspace.
- Define networks.
- Define cyber.
- Describe cybercrime, cyberwarfare, and cyber ethics.

Important Key Terms

Client - a desktop computer or workstation that is capable of obtaining resources from a server

Cyber - describes characteristics of the culture of computers, information technology, and virtual reality

Cybercriminal - a person who conducts illegal activity using computers or other digital technology

Cybercrime - a crime that involves a computer and a network

Cyber ethics - is a set of moral, legal, and social principles that applies to computers relating to the user's behavior

Cyberspace - the environment that allows digital technology of many forms to communicate with one another via the Internet

Cyber security - the collection of security tools, policies, safeguard, and practices that protect the cyberspace environment and its occupants

Cyberwarfare- the use of technology to attack a nation via network communications and computer devices

Internet - a worldwide collection of different networks connecting millions of devices which allows communication between other devices on the network

Network - a channel that links computers, servers, network devices, peripherals, or other devices together to allow the sharing of data

Node - a connection point that relays information along a distributed network

Packet switching - a process of arranging data into small units that can be transmitted over a digital network

Server - a computer program or a device that provides sharable resources

Imagine being the pilot for Flight 321 on your way to the airport. You notice that the Flight Management System (FMS) is not working properly. You glance at the screen and the Global Positioning System (GPS) and Inertial Navigation System (INS) are notifying you to alter the position of the aircraft to an abnormal altitude.

The INS begins to cause an integration drift that incorrectly calculates the acceleration and velocity of the aircraft. You begin to call for help.

This chapter introduces the concepts of cyberspace, cyber security, and the functions of networking systems, like the FMS, which later chapters will explore in more detail.

CYBERSPACE

What is cyberspace? The word "**cyber**" describes the digital environment in which computer networks communicate. The word "**space**", in the cyberspace context, describes an abstract idea of a virtual environment rather than a physical space. Cyberspace is the environment that allows digital technology in many forms to communicate with each other via the Internet. In cyberspace, users can interact with each other, exchange ideas, share information, provide entertainment, conduct business, and also engage in political discussions with a few strokes of their computer keys [4]. Many government and military officials, security professionals, and industry leaders use this term to describe the global technology domain of the web.

Cyberspace consists of two layers: physical and digital. The physical layer is composed of devices with Internet capabilities that can physically be touched, such as laptops, tablets, digital cameras, desktops, or even game consoles. These devices can connect to the Internet and become a part of cyberspace. The digital layer is the part of cyberspace that users cannot physically touch (i.e. the Internet) but can access through devices in the physical layer.

NETWORKS

A **network** links two or more devices. A **node** is a network device that provides a connection through which it relays information to other network devices. To facilitate communication, each network device has a unique address. This address allows the devices to communicate with each other and work together to accomplish a task. These addresses are complex sequences of numbers. But, do not worry, humans do not need to remember these complex numerical addresses, only the network devices do. To make it easier for humans, often these device addresses are represented as human-readable names followed by ".com" or ".net".

A real world analogy may help clarify this addressing concept. If you want to travel to your grandmother's house, you will need to provide your GPS system with some information. While you could provide the GPS with the specific latitude and longitude of her house, you could also provide the street address (i.e. 123 Main Street). Even easier, if you have already programmed your GPS to know where your grandmother's house is located, you can just tell it to take you to "grandmother's house." Similarly, a networked system is able to convert human readable addresses into network locations.

PACKET SWITCHING

Packet switching is the process networks use of splitting a large message into smaller units that can be more easily transmitted over a network. This process helps to prevent network overloading and maintain efficiency. If a communication pathway is unavailable, the network can reroute one or more packets allowing all packets to arrive safely.

As packets travel through networks, they encounter switches and routers that forward the packets to the next point along the route. In route to the final destination, the network tracks each packet to ensure that it arrives on time. Once all of the packets reach the destination, the recipient can extract the information and reconstruct the original message.

An analogy to this process would be when someone wants to send a large document to a friend. If the document is too large, the postal service may charge a fee for excess weight. To save that fee, the sender may divide the document into multiple packages. Because the packages may take different routes and arrive out of order, each package contains a portion of the original document, along with a sequence number to tell the recipient how to reconstruct the overall document.

Figure 1-1 illustrates packet switching using the postal service analogy. Host 1 wants to send a message to Host 2. The message begins at Host 1 (the sender). The network splits the message into three packets that travel through the network to Host 2 (the destination). All of the packets then arrive at Host 2. Host 2 then reconstructs the message. This concept is common in client-server communica-tion, discussed in the next section.

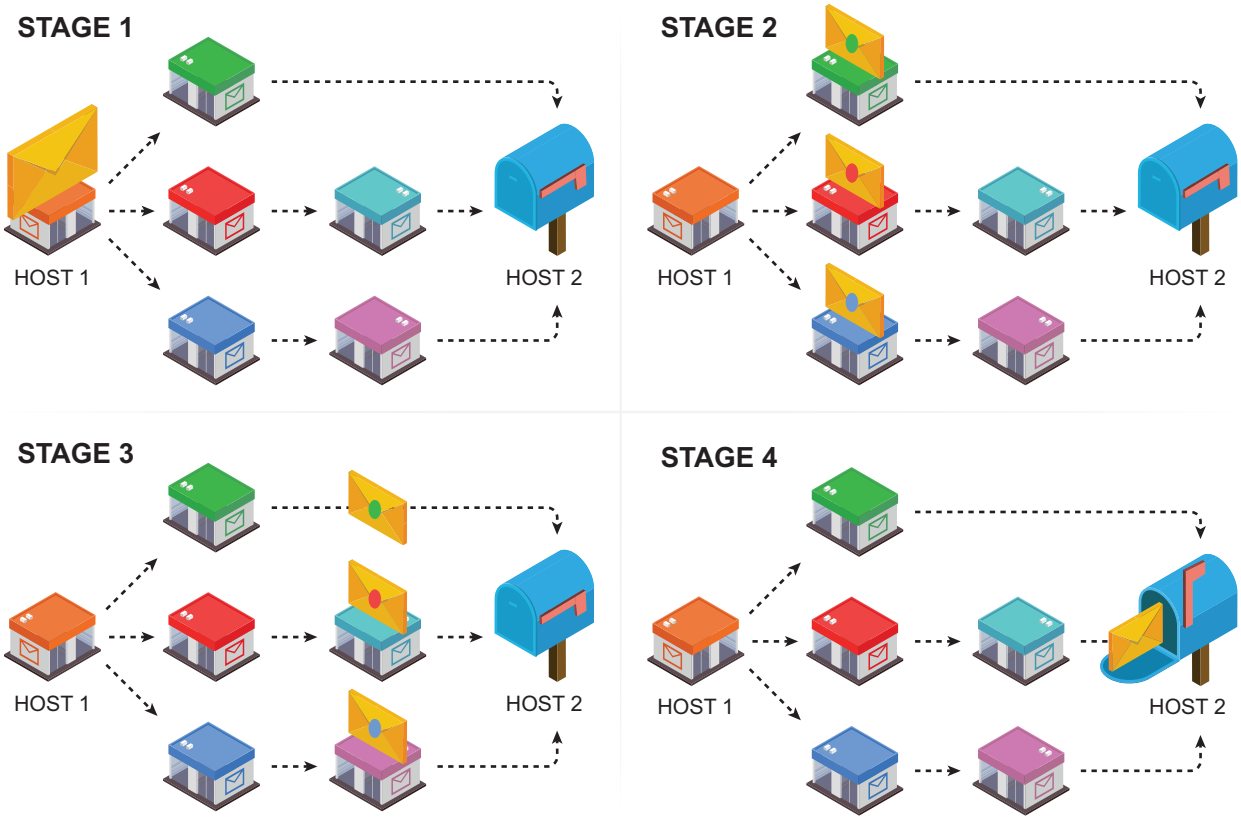


Figure 1-1: Packet Switching Illustration

CLIENT-SERVER NETWORK

In a client-server network, there are two types of nodes: clients and servers. A **client** is a network device that requests access to some type of service to accomplish its task (e.g. requests for data or requests for printing). A **server** is a computer or device that manages access to the centralized resources clients use to complete their tasks (e.g. hard drives, printers, and other sharable resources) [5]. Clients request services provided by servers to help the users complete their tasks.

Figure 1-2 illustrates a computer lab in which all are on the same network and have access to a shared printer. Computers A, B, and C act as clients that help their users can access the shared printer (the server) through communicating over the client-server network. To print, the user chooses the desired printing options on the client. The client communicates this information to the server. The server then sends back a signal giving the client permission to print. This cli-ent-server network reduces the need for each computer to have its own printer

As seen in the previous example, a server may receive multiple requests from clients in a short period. A server can only perform a limited number of tasks at any moment and must prior-itize incoming requests from clients [6]. Also, a server may limit the availability of a resource if the requested workload is too high.

Clients and servers communicate via messages in a real-time request-response pattern. To properly communicate, the clients and the servers must work together so each knows what to expect. The Internet, discussed next, frequently makes use of client-server networks.

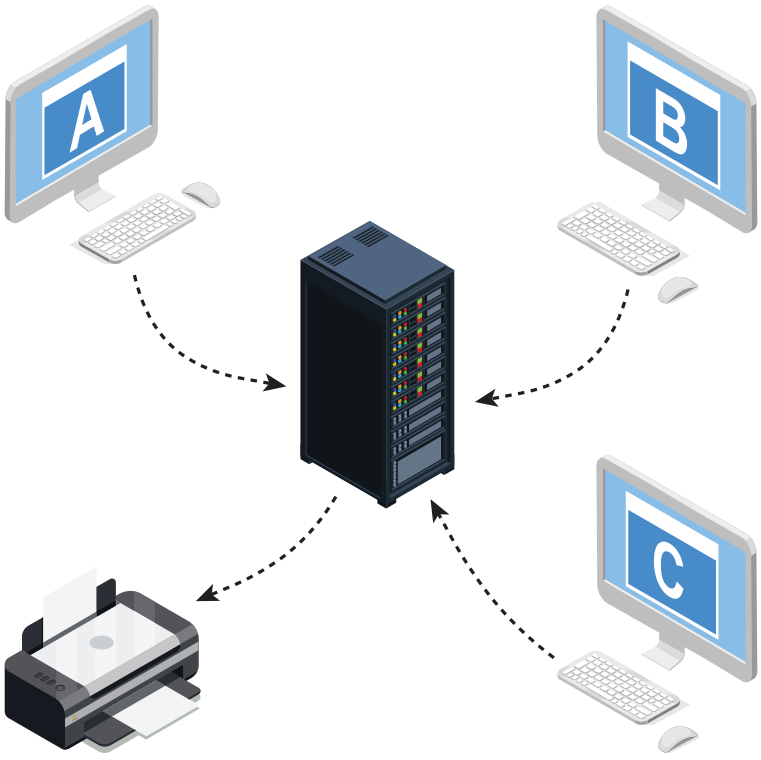
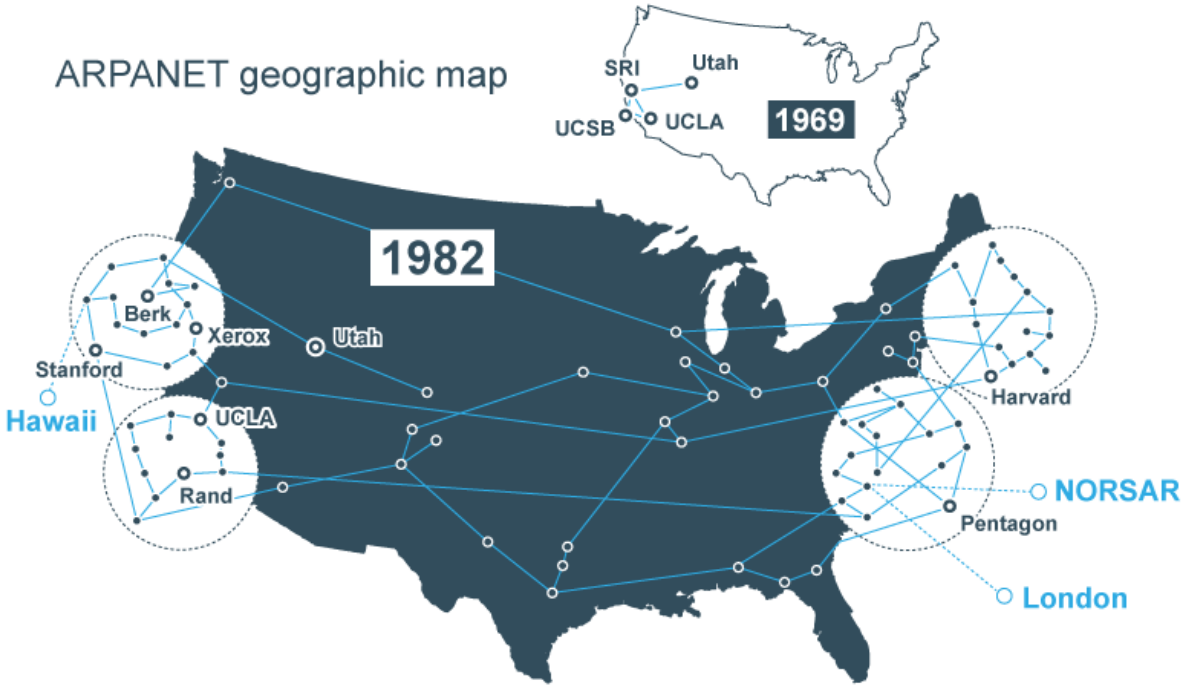


Figure 1-2: Computers sharing a resource over the client-server network.

THE INTERNET

The **Internet** is a worldwide collection of networks that connect millions of devices to allow businesses, government agencies, institutions of higher learning, and individuals to communicate with one another [1].

The Internet, the backbone of cyberspace, started as a networking project of the Pentagon's Advanced Research Projects Agency (ARPA), an agency of the U.S. Department of Defense, with the primary goal to allow scientists to communicate about military and scientific projects [1]. This first iteration of the Internet, called ARPANET, was developed in September 1969 [1]. ARPANET consisted of four computers located at each of the following sites: the University of California at Los Angeles, the University of California at Santa Barbara, the Stanford Research Institute, and the University of Utah to act as a host of the network [1]. It served as a backup communication network for armed forces if other forms of communications were destroyed.



The Internet has evolved to push society to a technological age. People exchange vast amounts of information through the internet every second. Frequent use of the internet increases the chances that a user's confidential information may be compromised by cyberattacks that can compromise the privacy and security of others. For this reason, everyone must take proper security precautions when using the Internet. Cyber security encompasses the various practices for protecting users and their systems.

CYBER SECURITY

To ensure the safety of users in cyberspace, the importance of and the focus on cyber security has increased substantially over the last decade. Cyber security allows users to keep the virtual environment of cyberspace safe from potential threats. Cyber security refers to a collection of technologies, tools, approaches, guidelines, and practices designed to protect networks, devices, and data [2]. Cyber security is a broad and complex field that faces a constant battle between users and malicious attackers [3]. Cybersecurity consists of concepts including:

- **Information security:** protecting access to private information by unauthorized users.
- **Network security:** defending networks to prevent people from gaining access they should not have.
- **Endpoint security:** securing all devices and access points within a network.
- **Website security:** Preventing attacks that will negatively affect a website, causing it to fail or to go offline.
- **Application security:** Reduces the opportunities for people to exploit weaknesses in applications.

When operating in cyberspace, individuals and businesses should take cyber security precautions. Any user can encounter security problems such as clicking on links to malicious sites, fraud, downloading malware, or denial of service. In addition private and public organizations gather, process, and store large amounts of data on internet-connected devices that could be vulnerable to various types of threats if the owners do not use proper cyber security practices.

The increase in the use of social media has led to an increase in the prevalence of cyber security problems. Social media allows users to stay constantly connected with their family and friends across the world. However, this convenience comes with risks. Users' private information can be compromised, old posts can come back to haunt users, or users can become the target of harassment from cyberbullying. It is essential to be careful about your online activities to reduce the chances of becoming a victim of a cybercrime. Chapter 3 discusses this topic in more detail.

CYBERCRIME

Cybercrime is a crime that involves a computer and/or a network. Cybercriminals often target vulnerable computers to gain access to networks and commit crimes. Cybercrime can be a threat to individual people or even to national security. A cybercriminal is a person who commits crimes via the Internet either with a computer as a target or using a computer as a weapon. Some examples of each type of cybercrime include:

Computer as a Target:

- Hacking
- Denial of Service
- Malware
- Botnets

Computer as a Weapon:

- Identity Theft
- Cyberbullying
- Software Piracy
- Cyberstalking
- Cyberwarfare

Chapter 2 discusses the different types of crimes and their effects.

CYBER ETHICS

Cyber ethics is a set of moral, legal, and social principles that apply to user behavior on computers [4]. In other words, cyber ethics is a set of guidelines users should follow to engage in responsible behavior on the Internet. Just as people should act responsibly in everyday lives, people should act responsibly in cyberspace. Some people believe that by deleting or hiding their online behavior, they are able to ignore the effects of unethical behavior. However, because computers, websites, browsers and other internet services log deleted or hidden activity, that activity may lead to legal actions. Remember, unethical behavior in cyberspace may have real world ramifications. Here is a list of some basic guidelines for practicing good cyber ethics:

1. Do not use offensive language or hateful speech.
2. Do not cyberbully.
3. Do not plagiarize.
4. Do not use someone else's password without permission.
5. Do not attempt to infect someone else's computer.
6. Avoid infringing on someone's copyright when downloading material from the Internet, including software, games, movies, or music.

Chapter 3 discusses cyberethics and other good practices for cyber ethics.

Summary: Users must become aware of the dangers of cyberspace and how to keep cyberspace safe. Sometimes when people think of security, they think of law enforcement, government officials, and the military. On a smaller scale, one may think of their parents, teachers, or community leaders. Their primary job is to defend and protect us from any harm to our wellbeing. Conversely, everyone has some responsibility for making, and keeping, cyberspace safe. The first step to achieving this goal is being aware of the obligation to protect cyberspace. Cyber security affects everyone: Be a part of the solution and not the problem.

Chapter 1 Review Questions

1.1. What is cyberspace? What is cyberspace made up of?

1.2. Can anyone be a victim of cybercrime? Why or why not?

1.3. What is cyber security? Why is it important?

1.4. Give an example of a cybercrime.

Discussion Questions

Purpose- Cadets will apply knowledge gained from Chapter 1 to answer the following questions as a group.

Discussion 1: How does cyber security affect schools, hospitals, and government?

Discussion 2: How can you spread awareness within your community about cyber security?

Discussion 3: What does it mean to be ethical in cyberspace?

ACTIVITY 1 SECTION

Activity One - Get Connected!

Purpose: Cadets will demonstrate how networks are connected.

Materials:

- Yarn or string
- Scissors
- Tape

Preparations:

- Cut the yarn into lengths of 8 ft.

Group Member Roles:

- Each group member will represent a device on the network.
- One of the group members represents the server, who manages services and resources on a network.

Note: This activity is similar to the old tin can and string game.

Procedures:

1. Connecting to the Network
Each group member, except for the member who will be acting as the server, will start with a piece of yarn and hold the yarn in their hand. This represents your device connecting to a network.

2. Connecting with a Peer
Each person must now pick another person with whom to connect their yarn. You will connect by tying your yarn together. (This is called a **peer-to-peer network**). You can only send messages to the peer to which you are connected. In order to connect with other peers, repeat the step above with another partner.

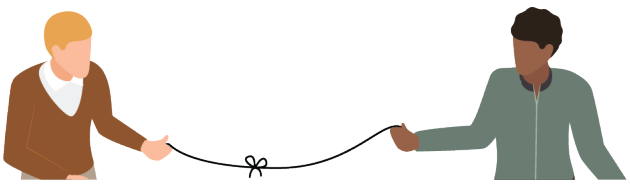


Illustration 1 is an example of the peer–to-peer connection.

3. Connecting to Server

Each pair will now attach their paired yarn to the member designated as the server. (This is an example of the client-server network).

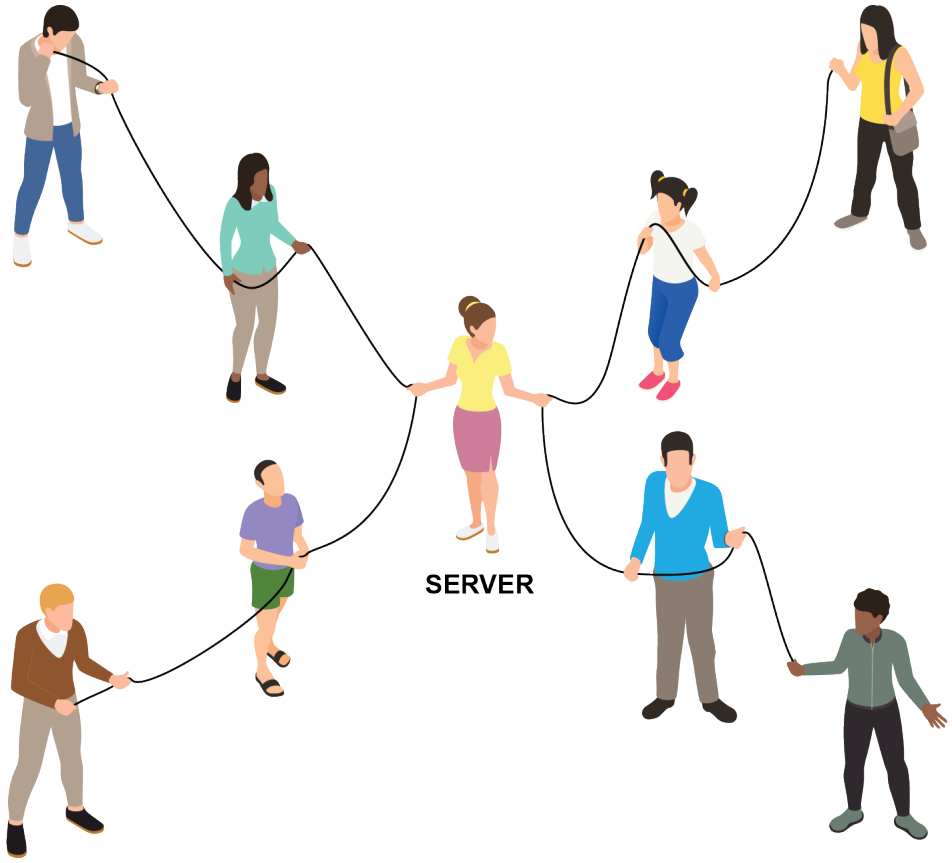


Illustration 2 is an example of the client-server network.

4. Disconnecting from a Peer-To-Peer Network

In order to delete a device, the group members furthest from the server should release the yarn. You are now disconnected from the device.

Note: If too many devices are on a string, this will make the string heavier, which in the computer world means that the data is transferring at a slower rate. You should try to avoid this action.

5. Disconnecting from a Client-Server Network

In order to disconnect from a client-server network, the remaining group members, excluding the server, will release the yarn. You are now disconnected from the server.

Summary: Over the network, there are several ways to communicate and share resources. The goal of this activity is to demonstrate how the devices are connected to peers and servers on the network.

Activity Two - You've Got Mail

Purpose: Cadets will demonstrate how networks communicate.

Materials:

- Envelopes (one per person)
- Yarn or string
- Scissors
- Hole puncher
- One sheet of paper per group
- Pencil or pen
- Clothespins

Group Member Roles:

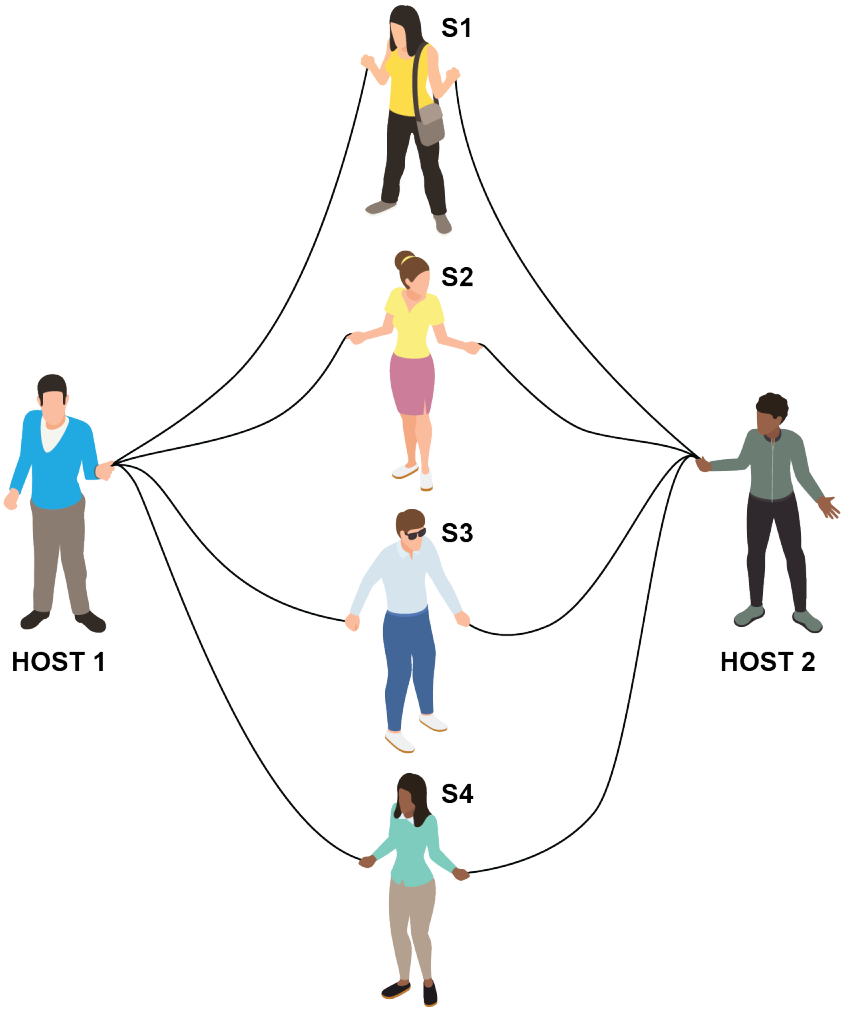
- Group Size: 5 - 7 cadets
- Host 1/Sender - this cadet will be the starting point for all the packets.
- Host 2/Recipient - this cadet will be the destination point for all the packets.
- Routers/Switches - 2-4 cadets. These cadets will help distribute the messages as packets.
- New Router/Switch – 1 cadet. This cadet will step in to help an overloaded connection.

Preparations:

- Cut the yarn into lengths of 8 feet, 2 per each router/switch cadet.
- Punch a hole in the top corner of each envelope, 1 per group member.
- Assign group member roles to cadets as listed above.
- Have Host 1 create a message to send to Host 2 on the sheet of paper.
- Cut the message into as many pieces as you have group members. The pieces will repre sent the message being sent as packets across the network.
- Place one piece of the message inside each envelope.

Procedures:

In this activity, each cadet, except for Host 1 and Host 2, represents routers/switches sending messages on a network. The envelopes represent the packets that were created to send the message from Host 1 to Host 2. The yarn represents the flow of communication.



The yarn represents connections between the hosts and the routers/switches.

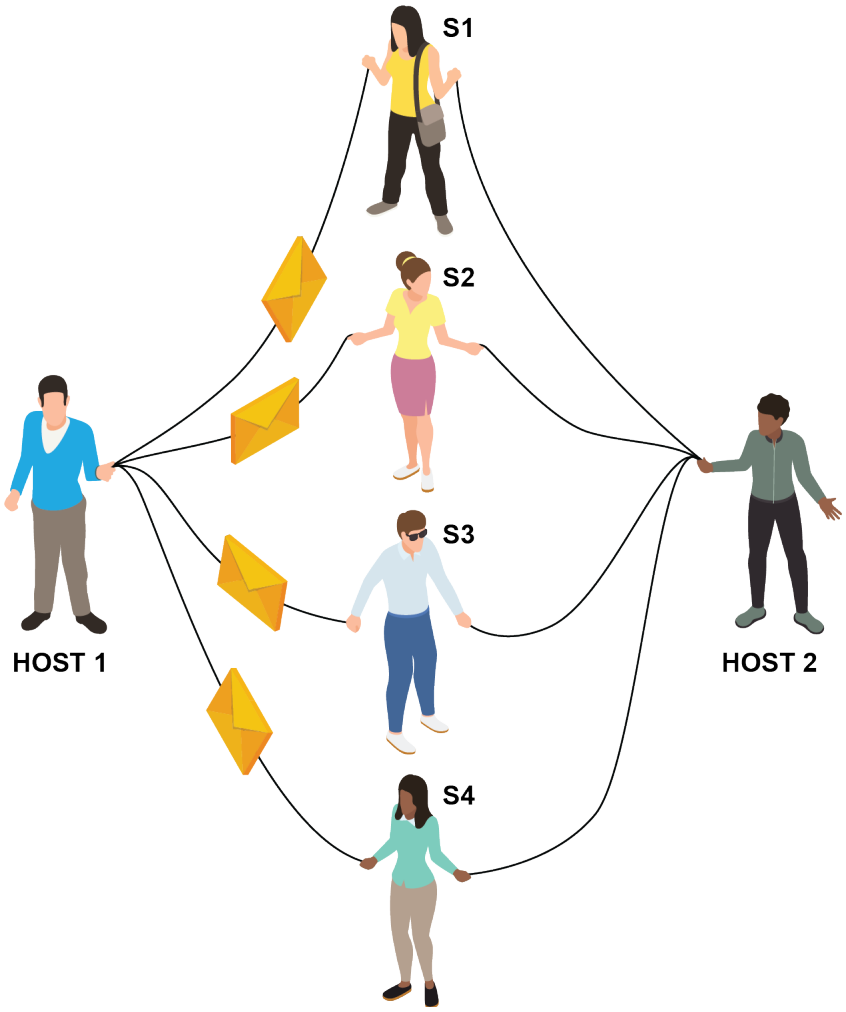
1. Building the Network

The cadet assigned as the new router may observe or act alongside the other router/switch cadets for this part of the exercise.

Host 1 should have all the packets that were made in the preparation stage of this activity.

Each cadet that is acting as a router/switch should have two 8 ft. lengths of yarn.

Each router/switch will share one end of their yarn with Host 1 and the other with Host 2.



The message is sent using packet switching.

2. Send Message

Host 1 will thread each envelope on the yarn. Ensure that the packets are equally distributed among all the pieces of yarn.

> Remember: If you attach all of the envelopes to one yarn this would not be effective and would slow down the retrieval of the messages. Please avoid this action.

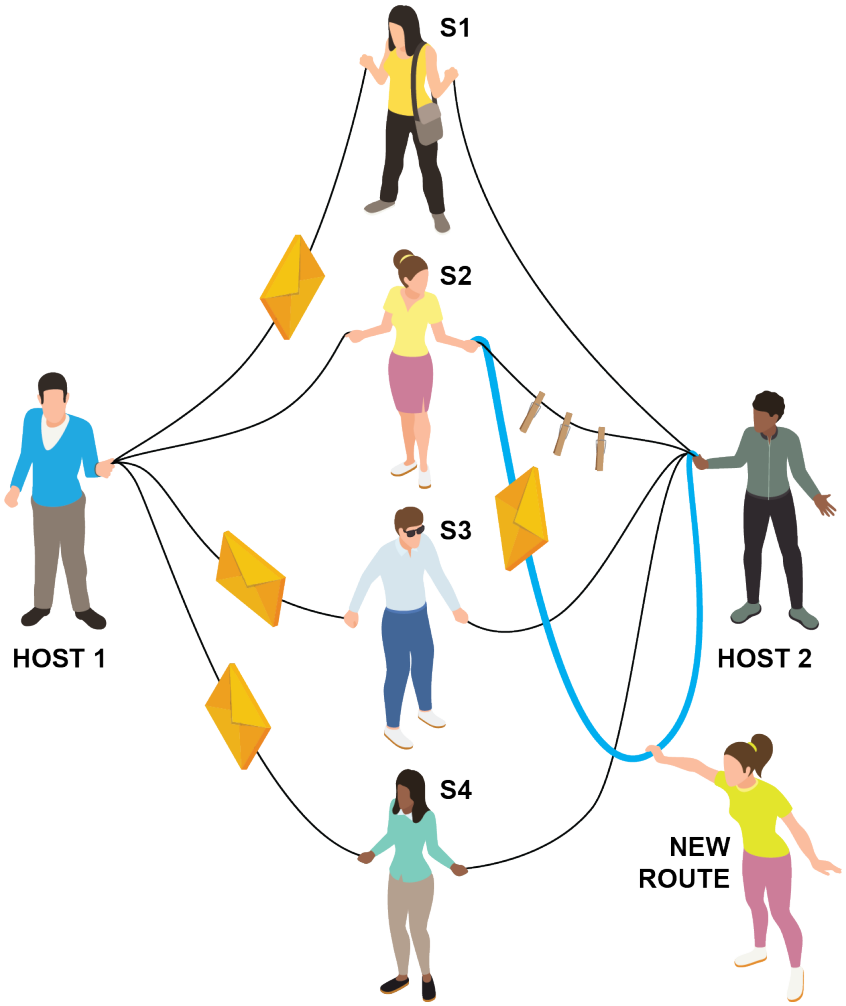
.

The routers/switches will help the packet push along the yarn and pass them between strings until they reach Host 2.

Host 2 must receive all of the packets before reading the message.

Once all the packets have been received by Host 2 they will put the message together and read it aloud. This is how messages are sent using packet switching over the internet.

Break: Did the message arrive at Host 2? What does the message say?



A new route is used when a connection is unavailable.

3. Send Message with Overloaded Router

For this scenario have Host 1 create a new message in the same manner as done before.

The route between one of the original router/switch (S2) and Host 2 is overloaded with work which would delay the arrival of packets. Place clothespins on the string to represent this overload.

Have Host 1 send the envelopes along the yarn as in the first scenario.

When the envelopes reach the string with the clothespins, they'll get stuck. The new router/switch will step in and attach their yarn to the yarn of the router/switch (S2) with the overloaded connection. The other end of the yarn will connect to Host 2.

The packet will now be pushed along the yarn by the new router/switch. This action will allow the packet to travel a new route around the problem connection to arrive on time.

Once all the packets have been received by Host 2 they will put the message together and read it aloud.

Break: Did the message arrive at Host 2? What does the message say?

4. Disconnecting with the Network

Disconnect from the network by removing all hands from the yarn. You are now leaving the network.

Summary: The goal of the activity was to understand better how data is transmitted across the network using packet switching. Packet switching is done to allow communication to happen fast and efficiently.

References:

[1]. Berners-Lee, T., & Fischetti, M. (2004). Weaving the web: the original design and ultimate destiny of the World Wide Web. New York, NY: Harper Business.

[2]. Stallings, W. (2019). Cryptography and network security: principles and practice. Hoboken, NJ: Pearson Education, Inc.

[3]. Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: what everyone needs to know. Oxford: Oxford University Press.

[4]. Kostopoulos, G. K. (2013). Cyberspace and Cybersecurity. Auerbach Publications.

[5]. Robert M. Metcalfe; David R. Boggs (July 1976). "Ethernet: Distributed Packet Switching for Local Computer Networks". Communications of the ACM. 19 (5): 395–404. doi:10.1145/360248.360253. Archived from the original on 2007-08-07.

[6]. Peterson, L.L.; Davie, B.S. (2011). Computer Networks: A Systems Approach (5th Ed.). Elsevier. p. 372. ISBN 978-0-1238-5060-7.

2 COMMON CYBERATTACKS: Beware of the Attack

Learning Outcomes

- Describe the different types of hackers: black, grey, and white.
- Describe ethical hacking.
- Identify current security practices used to protect against cybercriminals.
- Describe the potential gains for cybercriminals.
- List different types of cyberattacks and their techniques.
- Describe how hackers use malware to penetrate computer systems.
- List the characteristics of phishing attacks.

Important Key Terms

Adware - software that automatically displays or downloads advertising material (often unwanted) when a user is online

Black hat hackers - criminals who break into computer networks and systems with malicious intent

Computer virus - software application that disguises itself as an innocent program or file, produces copies of itself and inserts into other software applications, and that when run performs a malicious action such as destroying data or damaging software

Computer worm - a standalone self-replicating software application that invades computers on a network and usually performs a destructive action

Cyberattacks - malicious attempts by hackers to damage, steal, or destroy a computer network or system

Denial of service attack (DoS) - a cyberattack in which the perpetrator seeks to make a machine or network resource unavailable or to disrupt services connected to the Internet

Eavesdropping - occurs when an unauthorized user intercepts a private communication, such as a phone call, instant message, video conference, or email

Ethical hacking - an act of performing penetration tests on a system or network to find loopholes and vulnerabilities that a malicious attacker might use to their advantage to cause loss or damages

Grey hat hackers - an individual who may sometimes violate laws or ethical standards, but does not have the malicious intent typical of a black hat hacker

Hacking - the act of using a computer to gain unauthorized access to data in a system

Hacker - someone who uses a computer to gain unauthorized access to systems or networks

Keylogger - a tool that records or logs every keystroke on a computing device

Malware - malicious software variants that disrupt, damage, or gain unauthorized access to a computer system

Ransomware - a type of malicious software that attackers use to block access to a computer system until the user pays a certain amount of money

Phishing - the practice of sending fraudulent emails or text messages posing as a legitimate source in order to deceive individuals into revealing personal information, such as passwords and credit card numbers

Session hijacking - occurs when an unauthorized user takes over an active communication session without the user's permission

Sniffing - the process of capturing all data packets passing through a given network

Social engineering - the practice of manipulating people into revealing confidential or personal information

Spyware - software that allows an attacker to obtain information about another's computer activities

Trojan - malicious software that looks legitimate but can take control of the computer

Vulnerability scanner - software that detects weaknesses in computers, networks, and applications

THE MORRIS WORM

On November 2, 1988, Robert Tappan Morris, a student at Cornell University, unleashed a malicious computer program onto the Internet. This program infected computer systems at a number of the prestigious colleges and public and private research centers that made up the first national electronic network. The Morris Worm, as it is known, infiltrated an estimated 6,000 of the approximately 60,000 computers on the network [4]. It replicated at a remarkable speed and brought operations to halt in a 24-hour period. While the worm did not damage or destroy files, it still caused havoc on daily operations.

Robert Tappan Morris

As a result of the Morris Worm, vital military and university functions slowed to a crawl [4]. E-mails were delayed for days. The network community labored to figure out how the worm worked and determine the appropriate steps to recover from the attack. Some institutions wiped their systems; others disconnected computers from the network for as long as a week [4]. The Morris Worm was an early and one of the most famous cyberattacks and showed potential hackers what was possible.

Illustration of a Floppy Disk

This chapter introduces the concepts of malicious cyberattacks, like the Morris Worm, cybercriminals, hacking techniques, and defending systems against hacks.

CYBERATTACKS

Cyberattacks are malicious attempts by hackers to damage, steal, or destroy a computer network or system [2]. Cyberattacks happen when an unauthorized user takes advantage of a system by exploiting its vulnerabilities and runs their malicious code to alter the computer's function. While historically these attacks targeted corporations and businesses, they now target individuals that use networked devices, applications, and systems.

There are two categories of cyberattacks: attacks aimed at disabling the target computer and attacks aimed at gaining access to data. Within these categories, there are numerous specific types of attacks. As technology advances, so does the frequency of cyberattacks.

The following subsections discuss malware, phishing, and other cyberattacks that could affect users who are not actively using safe security practices.

MALWARE

Malware is software designed to disrupt, damage, or gain unauthorized access to a computer system. Different types of malware can infiltrate systems in a number of ways. The following list describes some of the most common types of malware:

• A **computer virus** is a software application that disguises itself as an innocent program or file, produces copies of itself and inserts into other software applications, and that when run performs a malicious action such as destroying data or damaging software [6]. In order to attack the computer, the viruses attach or insert their malicious code into clean code or software. The virus waits for execution by a user or automated process to attack. Computer viruses sometimes are run as a part of other software. For example, when someone is sick with a virus, the virus begins in one part of their body and moves to the next to spread the infection. In addition to copying itself, a computer virus can also execute instructions that cause harm and affect the security of the computer. Computer viruses spread through emails, shared USB drives, and online downloads. For example, a user may insert a USB flash drive in their computer that contains an unexpected virus on it. The virus loads onto the computer and begins to infect files and programs. The software that built the virus halts normal operations of the computer for the user.

• A **computer worm** is a standalone self-replicating software application that invades computers on a network and performs a destructive action [8]. Computer worms get their name from the way that the programs infect computers by searching the network for devices with security vulnerabilities. By connecting to those devices the worm spreads quickly across the network. An example of a computer worm is the Morris Worm described earlier.

• **Spyware** is software that allows a user to obtain information about another's computer activities [13]. Spyware hides in the background on a computer and collects information like passwords, credit card numbers, and other sensitive information without the user's knowledge. For example, a spyware application may collect a list of all websites visited by a user and send that information to an external location. Marketers and malicious users can purchase information collected by spyware. Spyware could even alter the results of Internet searches to redirect users to a web site that may infect their computers with even more spyware.

• **Ransomware** is a type of malicious software that attackers use to block access to a computer system until a payment is made [5]. Ransomware can infect computers through malicious links, files, or downloaded attachments. Once a system is infected, a user will be unable to access its files, data, or software. To regain access to the system, the user must pay the ransom to the cybercriminal, who can then unlock the system.

• A **trojan** is a type of malware that looks legitimate, but, in reality, has malicious intent [14]. Ancient Greek literature tells a story of Greek soldiers who hid in a giant wooden horse given to the city of Troy as a 'present'. Once inside the city walls, the soldiers were able to

launch an attack on the city. Malware trojans act in a similar way. The trojan presents itself as a harmless file or application to trick users into downloading it. Once the trojan is on a system, it can allow cybercriminals to steal information on the system, to install other malware, or to shut down the system itself.

• **Adware** is software that automatically displays or downloads advertising material when a user is online. Adware may appear in a variety of ways, including box display, pop up, video, and banner displays [15]. The software analyzes the user's location and websites frequently visited in order to present legitimate-looking advertisement services or goods near the user's location [15]. The adware will also find personal information about the victim (such as their age, race, and gender). For example, a user casually scrolls through his or her favorite social media site and encounters an ad about a shoe sale. The user clicks on the ad without paying attention to the obscure link. The software begins to collect information about the user in the background to sell.

While each type of malware has a different dissemination method, most require some kind of user interaction. This user interaction is necessary because attackers frequently use links, advertisements, or email attachments, which typically require the user to click on or download something.

The next section discusses how malware disguises itself as a part of a phishing attack.

PHISHING

Phishing occurs when an attacker sends fraudulent emails or text messages to deceive someone into revealing personal information, such as passwords or credit card numbers [11]. As with traditional fishing, the attacker uses ads, emails, or text messages that appear legitimate as a means to 'bait' the target individual.

Preparations:or example, suppose Jane receives an email message that appears to come from a social media website she frequently uses warning her she must update her password immediately. The email instructs her to click a URL embedded in the email. After clicking the URL, Jane enters her old password and her new password in what she thinks is a legitimate site. However, the link in the email has taken her to a fraudulent site owned by the attacker. Now the attacker has her password and can easily access her social media account, change her password, and assume her online identity.

While Jane's story is a made-up example, these situations occur frequently because attack-ers often do a very good job of disguising their phishing attacks to look very real. However, being able to identify characteristics of phishing attacks can prevent users from becoming victims. Some of those characteristics include:

1. The email sounds too good to be true. The email might promise a valuable reward (e.g. money or a trip) for clicking on a link.

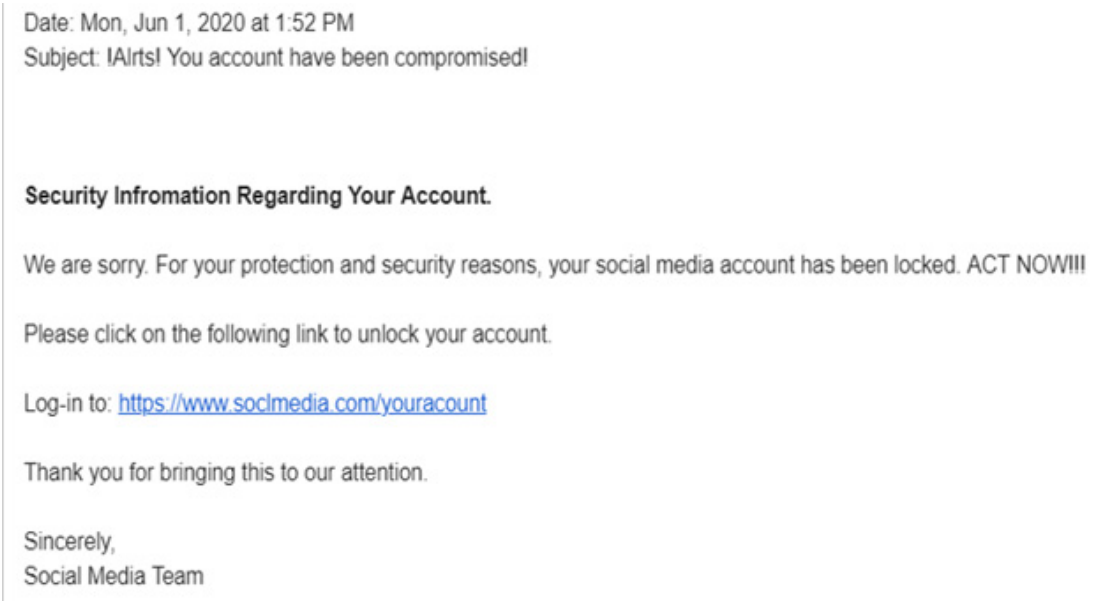
2. You do not recognize the sender.

3. The emails pressure you to react without thinking by including phrases like “Act Now” or “Immediate Action Required.” These types of emails suggest that if the recipient delays, they will face some type of negative consequence, like missing out on a good deal or losing access to an account.

4. The message contains unexpected attachments.

5. The message contains text or URLs that look suspicious, like misspelling a well-known web address, message text, or subject line.

6. The logo of the sending organization does not look exactly right, for example it has a different font or has misspellings.


Date: Mon, Jun 1, 2020 at 1:52 PM
Subject: !Alrts! You account have been compromised!

Security Infromation Regarding Your Account.

We are sorry. For your protection and security reasons, your social media account has been locked. ACT NOW!!!

Please click on the following link to unlock your account.

Log-in to: https://www.socImedia.com/youracount

Thank you for bringing this to our attention.

Sincerely,
Social Media Team

Figure 2-1: A phishing email. The subject line and the first line in the message in Figure 2-1 seems to have some misspelling. The second line says “Act Now” which seems a little scary and too eager. The link listed below also has some misspelling.

Figure 2-1 depicts an example of a phishing email illustrating several of these characteristics. The subject line and the first line in the message have some misspelling. The second line says, “Act Now,” which puts pressure on the recipient to react without thinking. The URL also has some misspelling. If you receive this type of email, you should report it (if possible), delete the email, and instruct your spam filter to filter out similar emails in the future.

Other Types of Attacks

There are many other types of cyber attacks that can also affect users. The following lists provides a few more examples:

• **Social engineering** is when an attacker uses trust or lack of knowledge to manipulate someone into revealing confidential or personal information [16]. To successfully use a social engineering attack, the attacker does not need to possess advanced knowledge of hardware or software. For example, imagine you are in a chatroom with your friends and a stranger enters the chatroom. The stranger engages you in conversation to gain your trust. Then this stranger may begin asking for personal information like where you live or attend school. Unless you are confident that you know someone online, you should not reveal any sensitive information. The stranger could use this information to stalk you at home or school.

• **Denial of Service Attack (DoS)** is a cyber-attack in which an attacker seeks to make a machine or network resource unavailable or to disrupt services connected to the Internet [1]. Hackers accomplish a DoS attack by flooding targeted machines with requests that overload the system and prevent that system from performing its normal operations. For example, a device repeatedly makes requests to a time server. Because the time server is occupied with these requests, it is unable to fulfill any other legitimate requests. Another type of DoS attack is a Distributed Denial of Service (DDoS) attack. In a DDoS attack, the attacker uses multiple devices, instead of only one, to flood the target machine(s) and prevent normal operation.

• **Sniffing** is a process of capturing all data packets passing through a given network [10]. Sniffers can have both legitimate and malicious uses. Network or systems administrators can use sniffers to monitor and troubleshoot network traffic. Attackers can use sniffers to capture data packets containing sensitive information. Sniffers can be either hardware or software.

CYBERCRIMINALS

Chapter 1 identifies a cybercriminal as a person who conducts illegal activity using computers or other digital technology. Cybercriminals use the tools mentioned above, along with several others (new attack mechanisms appear all the time) to attack computer systems and networks. Through these tools, cybercriminals commit various types of crimes, including hacking, identity theft, scams, fraud, malware dissemination, and many others. Cybercriminals use computers either as a tool to commit a crime or as a target of the crime.

Computer as the Target

In this type of attack, the goal of cybercriminals is to cause harm to the computer, or the contents of the computer (e.g. software, files, or data). This type of crime requires the attacker to have some level of computer knowledge and technical skill. The Morris Worm is an example of this type of attack because the primary goal of the worm was to infect other computers. For this worm to work, Morris had to understand how to spread the worm from computer to computer and how to exploit vulnerabilities. Another example of this type of attack is a DoS attack.

Computer as the Tool

When a criminal's target is a person or group of people, the criminal can use the computer as a tool to plan or commit the crime. Some examples of this type of crime include various types of scams, cyberbullying, and theft. These crimes generally exploit human weaknesses. Computers increase the number of victims to attack and the chances the perpetrator is caught. For example, a perpetrator accesses an online gaming account, enters the gaming chatroom and makes harsh remarks about the individuals in the online game.

HACKERS

A **hacker** is someone who uses a computer to gain access to systems or networks. Different types of hackers hack for different reasons. All hackers must have some level of technical skill and knowledge to be successful. Following are three general types of hackers with different goals.

Black hat hackers are the "bad guys" who hack into computer networks and systems with malicious intent [12]. They may use the types of malware described above or perform other malicious acts. Such hackers often have no particular care for the rule of law, or the chaos that they cause. Black hat hackers have cost companies, organizations, and individuals millions of dollars in damages and costs of recovery.

White hat hackers are the "good guys" who use their computing skills for ethical and legal reasons, such as testing a system's vulnerabilities.White hat hackers practice **ethical hacking**, which is the act of performing penetration tests on a system or network to find loopholes and vulnerabilities that a malicious attacker can use to their advantage to cause loss or significant damages [8]. The goal of ethical hacking is to improve the security of networks and systems through testing.

Grey hat hackers are the "neutral guys" who employ their skills to exploit networks and computer systems like black hat hackers, but like white hat hackers they do not have malicious intent. Grey hat hackers hack systems to discover vulnerabilities for their own enjoyment [8]. For

example, a grey hat hacker might attempt to find security vulnerabilities in an email system. The hacker may then exploit the vulnerabilities and notify the system owner of the hack. The grey hat hacker will then ask the system owner to pay a fee to fix the security problem. This type of hacking is illegal because the hacker is not authorized to access the system.

COMMON HACKING TECHNIQUES

Similar to cyberattacks, there are many techniques available to hackers. This section introduces some of the more common ones.

• **Eavesdropping** happens when an unauthorized user intercepts a private communication, such as a phone call, instant message, videoconference, or email. The attackers are usually after sensitive financial or business information to use for criminal purposes. An eavesdropping attack can be challenging to detect because the network transmissions may appear to operate normally. An eavesdropping attack requires an unsecured connection between the parties that the attacker can exploit to reroute network traffic. The attacker installs network monitoring software, on a computer or a server to intercept data as it is transmitted.

• A **keylogger** is a tool that logs and saves every keystroke on a computing device. A keylogger can capture personal messages, banking information, phone numbers, and even passwords.

• **Vulnerability scanner** is software that detects security weaknesses in computers, networks, and applications. Vulnerability scanners help hackers identify vulnerabilities resulting from flaws in firewalls, routers, and web servers [8]. White hat hackers use vulnerability scanners to find vulnerabilities that need to be patched. Black hat hackers use vulnerability scanners to find targets to attack [8].

• **Session hijacking** occurs when an unauthorized user takes over an active communication session [9]. Attackers then can impersonate that user to enjoy their access to resources provided by the session. An individual becomes vulnerable to session hijacking when he or she accesses trusted sites over an unprotected or public Wi-Fi network [9]. Although the username and password for a given site may be encrypted, the session data traveling back and forth may be in plain text. By mimicking a person's session over the same network, a hacker can access sites and perform malicious actions posing as some else.

• A brute force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. Depending on the length and complexity of the password, cracking it can take anywhere from a few seconds to many years. A brute force attack can use a dictionary of common words or common passwords as a source for poten-tial usernames or passwords. Because of the complexity of these attacks, hackers often use tools to more quickly try large numbers of usernames and passwords in hopes of finding a successful combination.

DEFENDING AGAINST HACKERS

Hackers must choose the most appropriate tools for their goals and their target. As technology continues to expand, there will be more tools available both to attack and to defend systems. Because hackers have so many tools at their disposal, by learning about the most common hacking techniques, users can better equip themselves to defend their systems and personal information.

Summary: There are easy, practical steps that users can take to protect their devices and secure accounts from cybercriminals. Here are practical steps that users can follow to defend against hacks:

- Ensure all software, including operating systems and applications, is up-to-date by installing updates as they become available.

- Install antivirus and antimalware software to help defend your system, detect attacks, and remove viruses and malware.

- Disable connections like Bluetooth and Wi-Fi when not in use to prevent hackers from using them for attacks.

- Create strong passwords that do not include any personal information or common dictionary words. Passwords should be a combination of numbers, letters, and characters.

- Only download and install applications from trusted locations.

- Limit use of public Wi-Fi (i.e. Wi-Fi networks you do not own).

- Delete suspicious emails and train spam filters to detect them in the future.

Chapter 3 discusses other security practices that can help users protect themselves from risk associated with cyber security and how to apply these tips to their own lives.

Chapter 2 Review Questions

2.1 Explain the difference between black hat, grey hat, and white hat hackers.

2.2. Define social engineering?

2.3 List three characteristics of a phishing attack.

2.4 What is a cyberattack?

2.5 How can computers be used as a target? How can computers be used as a tool?

Discussion Questions

Purpose- Cadets will apply knowledge gained from Chapter 2 to answer the following questions as a group.

Discussion 1: What cyberattacks concern you the most and why?

Discussion 2: What can you do to protect yourself from cybercriminals?

Discussion 3: Have you ever been a victim of a cyberattack? What happened?

ACTIVITY 2 SECTION

Activity Three - Let's Go Phishing!

Purpose: Cadets will identify differences between a phishing email and a normal email.

Procedures:

1. Divide cadets into groups of four or five.

2. Give cadets the following emails. As a group, cadets determine which emails are phishing attacks and which are not.

Email 1

From: "Sassy, Dieter" <dsass@uwm.edu>

Subject: You're Dropbox File

Date: Mon, 30 Jan 2017

box

Hello,

You just received a file through Dropbox Share Application.

Please click below and log in to view file.

View file

Need even more space? Upgrade your Dropbox and get 1 TB

(1,000 GB) of space.

Happy Drop boxing.

- The Dropbox Team

Email 2

--------- Forwarded message ---------

Subject: STUDENT PART - TIME JOB

To:

Dear Student,

We got your contact through your school database and I'm happy to inform you that our babysitting service is currently running a student program. This program is to help devoted and hardworking students secure a part time job which does not deter them from their school work, you just need a few hours to do this weekly and with an attractive weekly wages.

KINDLY EMAIL BACK WITH THE BEST WAY TO CONTACT YOU FOR AN INTERVIEW IF INTERESTED IN THIS JOB POSITION.

Best Regards,

Ann Doe

Hiring Lead

Baby Inc.

Email 3

From: Raymond.109@quailtybanking.com

Date: Wed, 24 Aug 2019

Hi,

The monthly financial statement is attached within the email.

Please review it before processing.

King regards,

Pete Richmond

Email 4

Subject: Email Account Upgrade

From: ithelp@ul.edu

Date: 10/28/2016 4:38 PM

Dear User,

Someone else was trying to access your email account.

Date and Time: 28 October 2016, 1:38 PM

Browser: Firefox

Operating System: Windows

Location: Australia

If the information above looks familiar, disregard this email.

If you have not recently and believe someone may be trying to access your account, you should ACT NOW

Sincerely,

Technical Support Team

Email 5

From: chrismark.edu@gmail.com

Subject: URGENT REQUEST

To: davidchristensen@uwl.edu

Are you available?

No calls text only 356-703-9390

I'm in a meeting and need help getting some Amazon Gift Card.

Please text all of the gift card information to the number listed above.

BEST REGARDS

Chris Mark

Chancellor

University of West Louisiana

Email 6

From: Library Account

Date: Sat, Apr 1, 2017 at 2:09 PM

Subject: Library Account

To: jmicheal@librarysystems.gov

Dear Student,

Your access to your library account is expiring soon due to inactivity. To continue to have access to the library services, you must reactivate your account. Download the software from the website below:

https://recoveryyourlib.net/download

Sincerely,

J. Micheal

City Library

3. Cadets discuss their decisions and the reasons behind them. The group should choose one member to take notes about the discussion and prepare a short report of the findings.

4. Each group's reporter should read their group report aloud.

Summary: Protecting yourself against phishing is never an easy task. Being able to identify the characteristics of phishing is the first step in defense against the attack.

Activity Four - Think Like a Hacker

Purpose: Cadets examine their social media platforms and identify what personal information can be used by hackers to attack.

Materials:

Computing Devices (cell phones or computers)

Procedures:

1. Pair cadets up.

2. Each cadet will have 5 minutes to use their own device to see how much of the following information they can find about their partner.

Full Name: _____

Related To: _____

Close Friends' Names: _____

Phone Number: _____

Email Address: _____

Location: _____

Education: _____

Associated Groups: _____

Place visited: _____

Shared Locations: _____

3. Have cadets swap results with their partner to see how much of the information is correct.

Closing Discussion: Cadets will discuss why this information would be useful to hackers and what information should be removed after doing this activity.

Summary: The Internet is a great place to learn, shop, play, and chat with family and friends. Unfortunately, there are also cybercriminals who may try to harm you by stealing your information. In order to be safe online, it's important to limit the amount of sensitive information about yourself online to keep the “bad guys” away.

Activity Five - The Guessing Game

Purpose: Distinguish the characteristics of different cyberattacks and cybercriminals.

Materials:

- Notepad to keep score
- Marker or other writing material
- Timer
- Notecards

Preparations:

Write the following terms on notecards (one term per card):

Trojan	Adware	Black Hat Hacker	Phishing
Spyware	Ransomware	Computer Virus	Malware
Keylogger	Hacker	Computer Worm	Grey Hat Hacker
White Hat Hacker	Eavesdropping	Cyberattacks	Denial of Service

Group Member Roles:

- Time Keeper - ensure each team has two minutes per round.
- Score Keeper- ensure each team receives a point per correct guess.

Note: These individuals will not be a part of a team.

Procedure:

1. Divide the cadets into two teams.

2. Shuffle the notecards and split them between the teams. The notecards should be given out face down so no one is able to see the word on each card.

3. Team 1 chooses a member to go first. That person, who becomes the actor, looks at the word on the first notecard. Then, the actor uses the information in this module to describe the term, attempting to get his or her teammates to guess it within 2 minutes. Cadets cannot use the book, online resources, or any other aid. This process repeats with Team 2. Teams alternate, choosing a different actor each time, until all terms have been revealed.

4. Keep score. The team earns 1 point if they guess the term within 2 minutes. If the actor uses the term on the card, then the team loses 1 point.

Closing Discussion: As a group, answer the following question:

1. What challenges did you face describing or recognizing the terms?

Summary: By learning about cybersecurity basics, individuals can prepare themselves for the risks that they might face in the future. If the risks are encountered, we will know what to do and how to prevent them going forward. By having a strong foundation in preventative practices, individuals can enhance their cybersecurity knowledge and help keep everyone safe.

References:

1. Us-cert.cisa.gov. 2020. Understanding Denial-Of-Service Attacks | CISA. [online] Available at: <https://us-cert.cisa.gov/ncas/tips/ST04-015> .

2. Definition of WORM. (2020).
Retrieved 17 July 2020, from https://www.merriam-webster.com/dictionary/worm

3. Ethical Hacking. (2019). CEH v10 Certified Ethical Hacker Study Guide, 1–8. DOI: 10.1002/9781119533245.ch1ransom

4. Morris Worm. (2019, July 17).
Retrieved from https://www.fbi.gov/history/famous-cases/morris-worm

5. Ransomware: Definition of Ransomware by Lexico. (n.d.).
Retrieved from https://www.lexico.com/en/definition/ransomware

6. Definition of VIRUS. (2020).
Retrieved 17 July 2020, from https://www.merriam-webster.com/dictionary/virus?utm_campaign=sd&utm_medium=serp&utm_source=jsonld.

7. Grebennikov, N., Grebennikov, N., Racy, E., Cody, Cody, Angie, … Dia. (n.d.). Keyloggers: How they work and how to detect them (Part 1).

8. Y. Wang and J. Yang, "Ethical Hacking and Network Defense: Choose Your Best Network Vulnerability Scanning Tool," 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA), Taipei, 2017, pp.110-113, DOI: 10.1109/WAINA.2017.39.

9. Burgers, Willem; Roel Verdult; Marko van Eekelen (2013). "Prevent Session Hijacking by Binding the Session to the Cryptographic Network Credentials".

10. "Types of attacks - Sniffer Attack". Omnisecu.com. OmniSecu.

11. Phishing: Definition of Phishing by Oxford Dictionary on Lexico.com also the meaning of Phishing. (n.d.). Retrieved from https://www.lexico.com/en/definition/phishing

12. Black Hat Hacker. (n.d.).
Retrieved from https://www.sciencedirect.com/topics/computer-science/black-hat-hacker

13. Spyware: Definition of Spyware by Oxford Dictionary on Lexico.com also the meaning of Spyware. (n.d.). Retrieved from https://www.lexico.com/en/definition/spyware

14. Trojan: Definition of Trojan by Oxford Dictionary on Lexico.com also the meaning of Trojan. (n.d.). Retrieved from https://www.lexico.com/en/definition/trojan

15. "Malware from A to Z". Lavasoft. Retrieved 4 December 2012. [Adware] delivers advertising content potentially in a manner or context that may be unexpected and unwanted by users.

16. What is Social Engineering? Examples and. (n.d.).
Retrieved from https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering

3 IMPROVING YOUR PERSONAL SECURITY

Learning Outcomes

- Define privacy.
- Define online privacy.
- Explain cookies and the different types of cookies on the web.
- Explain the importance of online privacy.
- Explain how to protect your online privacy.

Important Key Terms

Computer cookies - small text files created by a web browser that store information

End-to-end encryption - a communication method that prevents unauthorized access to data while it is in transit between systems

First-party cookies - computer cookies created by a website visited by a user

Incognito mode - web browser privacy feature that prevents browsing history from being stored on the user's device

Session cookies - allow a website to store information across pages within the site so the user does not have to repeatedly enter the same information

Third-party cookies - computer cookies created by websites not directly visited by a user

Privacy - the right to be free from being observed or disturbed by other people

Virtual private network (VPN) - internet connection that encrypts traffic from a device to a private network

Weak password - a password that is easily guessed by a human or computer

Web browser - a software application used to access websites

PRIVACY

Imagine that Ashley is browsing online for a gaming system. After finding the right one, she buys it and continues with her day. Later, when Ashley returns to her computer to browse the internet, she begins seeing advertisements for the gaming systems she viewed earlier. Ashley wonders why she is seeing these advertisements on websites that are unrelated to gaming.

When users like Ashley browse the internet, websites capture and share information with marketers. The easiest way for businesses to identify Ashley's interests and habits is by watching her online behavior and internet searches. The developers of websites believe they can optimize a user's experience if they better understand the user's interests. However, websites that track, monitor, and share user information raise privacy concerns.

Privacy is the right to be free from being observed or disturbed by other people. Privacy concerns often arise related to sensitive information. Whether you are worried about a security camera tracking your movements in a store or a computer sharing information about the websites you visit, privacy is a concern both in the physical world and in the digital world. Also, when you are present in cyberspace, there are new opportunities for criminals to gather your sensitive information. As the scope of activities we conduct online continues to increase, so do the related risks to our privacy.

This chapter discusses the trade-off between the convenience of the internet and the loss of privacy that comes with it. This chapter also introduces the concepts of online privacy, cookies, strong passwords, and other precautions to aid in privacy protection.

ONLINE PRIVACY

Internet privacy is the ability of individuals to control what information is accessible to others online. Internet privacy is a part of the larger concept of data privacy, which ensures companies use customer information only for its intended purpose. An essential aspect of data privacy is **personally identifiable information (PII)**. PII can identify an individual either alone or in combination with other personal information. PII includes information like phone number, address, social security number, email address, and photographs.

As an example, while Bob is visiting a social media website, a survey appears. Bob decides to complete the survey because it promises a chance to win a prize. The survey asks Bob to enter his username and password along with other sensitive

information like his address, social security number, and bank information in case he wins the prize. Not long after Bob completes the survey, he begins receiving calls from his bank about unusual activity on his account. It turns out the survey was a scam used by cybercriminals to perform a PII harvesting attack and obtain Bob's sensitive information. The cybercriminals have stolen Bob's information and sold it on the dark web.

To understand how internet privacy works, users must consider privacy risks. Privacy risks occur when events allow attackers to compromise user privacy. The events include, but not limited to:

- Browsing - A web browser is a software application used to access websites. In short, a browser retrieves information from the internet and displays it on a computing device. Browsers share various types of information with the sites the user visits, including the browser type, computer system type, display resolution, and battery level of the device. All browsers allow users to adjust their privacy settings. While these settings provide users with some level of control over whether their private information is stored or shared, the amount of privacy protection varies from browser to browser.

- Emailing - Malicious users gain access to sensitive information by hijacking emails. Hijacking occurs when an intruder intercepts communications while in transit. For example, a user may send an email containing private information. As that email travels through the network, it can pass through untrustworthy nodes before reaching its destination. There is the potential that an unauthorized can intercept the communication and access confidential information. Unfortunately, there is no way to verify that an un authorized party accessed the email; therefore, an invasion of users' privacy occurs without the user's knowledge.

- Online shopping - To make an online purchase, a user typically has to enter their credit card number, expiration date, and security code. The user can choose to allow the website to store this information for later use. However, this convenience comes with a risk. If a cybercriminal can break into the database that houses this financial information, they will then be able to make unauthorized purchases or sell the information on the darknet.

COMPUTER COOKIES

Computer cookies are small text files created by a web browser that store information. The cookies pass information between the web browser and the web servers. The primary purpose of computer cookies is to track a user's activity on a website. When a user visits a website, the browser saves a cookie file that stores information about the user's identity and activities. Each time the user returns to the website, the browser can pass this information back to the server to facilitate the browsing session.

Online stores use cookies to record information about a customer, including items the user browses. This information prevents the customer from having to perform the same search again.

For example, users may see advertisements for products that are similar to those from their previous searches. These types of cookies help companies better target their marketing to a particular audience. There are different types of cookies:

- **First-party cookies** are created by the website the user visits. First-party cookies help the website provide a good user experience by remembering user preferences and session information. Companies share this information with advertising agencies to target their marketing to a particular audience. Each website has a separate first-party cookie.

- **Third-party cookies** are created by websites not directly visited by the user. Often an advertising site may place a cookie on a user's device to track behavior so they canbetter target advertisements. In our earlier example of Ashley, as she browsed for gaming systems, a third-party cookie from an advertiser stored information about that search. This information then helps the advertiser know to show Ashley advertisements for gaming systems the next time she is online. Unlike a first-party cookie, the third-party cookie can track information from multiple sites.

- **Session cookies** allow the website to temporarily store information throughout one session of visiting a website. A session may include visits to multiple pages. For example, a session cookie can store login information so the user does not have to enter it repeatedly on each page. Session cookies are temporary and are stored only for the session.

- Persistent cookies exist for more than one session to provide websites with user preferences or settings on future visits. For example, users can personalize their settings for their school website to show the types of information of most interest to them first. Persistent cookies stay on the user's browser for an extended time but may have an expiration date.

Computer cookies store personal information. A common misconception is that by deleting cookies, users are protecting their internet privacy. While deleting cookies can preserve some level of privacy, protecting internet privacy involves more than deleting cookies.

PROTECTING INTERNET PRIVACY

With the increase in websites and services, users can store their information in more places, which increases their exposure to privacy threats. To ensure internet privacy, users must safeguard information they share online. As discussed above, cookies monitor behavior to enhance the user's experience. However, malicious entities can also monitor behavior to exploit users.

To reduce the threats from malicious actors, users must implement security practices to protect their personal information. Users must also take the time to understand how websites handle users' personal information. If users are not responsible for protecting their personal information, they leave themselves open to cyberattacks. Users can protect their privacy by implementing the following security practices:

1. Check the company's privacy settings - Many online services help users protect their information by providing privacy settings, including blocking who can see certain content, limiting access to photos and videos, and restricting account access. Users should enable these privacy features to reduce the chances of malicious users obtaining private information.

2. Take care when storing private information in a cloud storage location - Sites that store and share information provide convenience for a user. For example, a user can use these services to easily share photos from a trip with their friends. However, users should avoid storing sensitive information, like potentially embarrassing photos, in a public cloud. If a cloud service is hacked, the risk of vacation photos falling into the wrong hands is much less severe than the risk of embarrassing photos being stolen.

3. Avoid online tracking on shared devices - When a user browses the internet on a shared computer, they have the potential of revealing confidential information. For example, when Emily surfs the web on a public computer, the browser saves information in a cookie. Other users of the same device can potentially access those cookies. Emily can prevent the shared device from storing her information by using the incognito mode on the browser. **Incognito mode** is a web browser privacy feature that prevents browsing history from being stored on the user's device.

4. Use a secondary email address to sign-up for websites - By using a separate "junk" email address to interact with websites, users can reduce the amount of unwanted emails that arrive in their primary account. If the user does not expect to have ongoing communication with the site, using the "junk" email address will route all the communication, and associated spam from the email address being shared with other sites, to this separate account where it can be ignored.

5. Use messaging apps with end-to-end encryption - End-to-end encryption is a communication method that prevents unauthorized access to data while it is in transit between systems. When sending confidential or sensitive information, individuals want to ensure that no one tampers with or accesses the communication. Messaging applications that use end-to-end encryption, encrypt (or make unreadable) the message on the sender's device, transmit the message over the network in an unreadable format, and decode the message on the recipient's device. Even if a malicious user intercepts the message, it is unreadable.

6. Use secure passwords - A weak password is a short, commonly used word or phrase easily guessable by a human or computer (e.g., "123456" or "abcdef"). Use of a weak password makes it easier for malicious users to gain unauthorized access to a user's accounts or information. The simpler the password, the easier it is to detect. Use of strong passwords reduce the chances of unauthorized access to accounts, information, or devices. In addition, using a unique password for each site will also reduce the chances of unauthorized access. Below are suggestions for creating and using strong passwords:

• Do not share passwords across multiple sites.
• Do not write your passwords down in a place where others can find them.
• Use passwords of at least eight (8) characters.
• Use combinations of uppercase letters, lowercase letters, numbers, and special characters.
• Do not use someone's name, birth date, or words found in the dictionary.
• Substitute characters for letters or numbers. Instead of using "a" use "@."
• Update passwords frequently.
• Use a secure password manager to store complex passwords so you do not have to remember them.

7. Review permissions for mobile apps and websites - Sometimes, excited mobile app users do not fully review terms and service agreements, which may give the app permissions to access more information than necessary. For example, an app used for audio recording might ask for permission to access a user's contact list. The user must decide whether the permissions requested are really necessary. Sometimes apps need permission to access specific functions to operate correctly. However, other apps may use this access for less legitimate purposes. In many cases, the user will not be able to install an app without granting the requested permissions. The user should carefully consider whether the risk is worth it. In any case, the user should restrict permission to use device features to only the times the app is in use.

8. Use a VPN when accessing public Wi-Fi networks - Use of public Wi-Fi, while convenient, may introduce unnecessary privacy risks. If the Wi-Fi is unencrypted (which is the typical case), a malicious user can spy on the network traffic. Therefore, users should avoid transmitting sensitive data over a public Wi-Fi. Users may also employ a virtual private network (VPN), which encrypts traffic from the device to a private network over the internet. For example, Michael may access the public Wi-Fi at a coffee shop and then use a VPN to connect to the private network at his school. Then, when Michael sends information between his device and his school's network, that information is encrypted. Even if a malicious user intercepts the information in transmission, that information is unreadable.

Summary: Protecting confidential and sensitive information when using the internet may seem like a daunting task. However, it is possible for a user to greatly reduce the chances of exposing this information. When a user goes online, advertisers, merchants, and even cybercriminals track every action. Therefore, users must be proactive to ensure their private information does not fall into the wrong hands. By putting into practice the recommendations in this chapter, a user can greatly reduce the likelihood of a privacy invasion.

Chapter 3 Review Questions

2.1 Define internet privacy.

2.2. List the different types of cookies and explain their purpose.

2.3 List three ways that your privacy can be invaded.

2.4 What is a VPN? How does it protect privacy?

2.5 What is end-to-end encryption?

2.6 List five ways that users can protect their privacy.

Discussion Questions

Purpose- Cadets will apply knowledge gained from Chapter 3 to answer the following questions as a group.

Discussion 1: Do you think people have the right to online privacy?

Discussion 2: Is maintaining access to technology and online content more important than having privacy? Is there a way to have both?

Discussion 3: Who or what is the greatest threat to online privacy?

Activity Six - Passing Encrypted Notes

Purpose: To demonstrate the risks of sharing information over an unsecured network and how encrypting information can reduce those risks.

Materials:

- Notecards
- Writing utensil
- Yarn or string
- Scissors
- Hole puncher

Preparations:

- Cut the yarn into lengths of 8 ft.
- Use the hole puncher to create a hole in the top corner of each notecard.

Procedures:

1. Divide cadets into groups of 3.

- Cadet A is the sender, Cadet B is the malicious user, and Cadet C is the recipient.
- Cadet A and Cadet C will stand an equal distance apart. Each cadet will have one end of the string.

2. Cadet A will write something on the notecard and send it to Cadet C by sliding it along the string. Cadet C will then write something on the notecard and pass the message back to Cadet A. Cadet B will intercept the note before it reaches Cadet A, he or she will read the note aloud.

Note: *This depicts the way unsecured networks work: malicious users (Cadet B) can intercept communications on unsecured networks and decipher two-way conversations, exposing Cadet A and Cadet C's private information.*

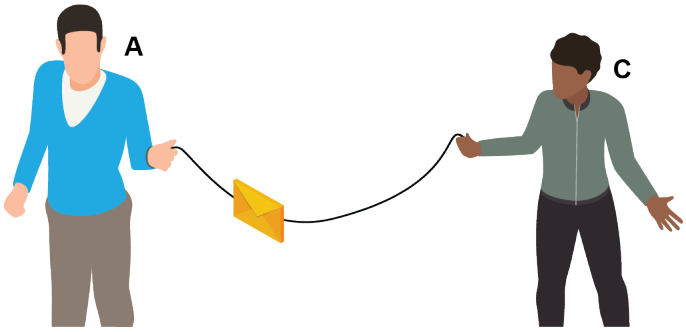


Figure 3-1: Activity Set-Up

3. Cadet A and Cadet C will develop an encryption code on a sheet of paper. To develop an encryption code, the cadets should assign a different letter or other symbols to each letter in the alphabet. Cadet B should not see the code Cadet A and Cadet C are developing. However, Cadet B may be allowed to eavesdrop and strategize about breaking the code. The eavesdropping represents a type of attack on end-to-end encryption.

4. Cadet A and Cadet C will return to their positions and repeat Step 1, this time with an encrypted note. Before passing along the note each time, Cadet B will copy it (either by taking a photograph with a smartphone or manually copy it down). Ask Cadet B if they can decipher what the encrypted message says.

Note: *This is an example of how to ensure information when communicating online by using encryption!*

Summary: End-to-end encryption can provide security in terms of integrity and privacy for users if implemented correctly. There are many online end-to-end encryption tools available to help users maintain their privacy and integrity.

Activity Seven - Privacy Policies

Purpose: To demonstrate how privacy policies work on social media websites or applications.

Materials:

- Computer or mobile devices
- Pen
- Paper

Procedures: Divide cadets into groups of three or four. Each group will pick a social media website or app used by a majority of the group. The cadets will look up the privacy policy for the selected site or app and answer the following questions:

1. What data is collected by the social media website or app?

2. How can your data be used?

3. With whom will the social media company share your data?

4. Does the site disclose personal information to third parties?

5. How can third parties use your data?

6. Do you have to explicitly say you agree to the website's privacy policy before sharing your information?

7. Can the users change their privacy settings and preferences on their accounts?

8. Does the user have the option of deleting their account?

9. Who is responsible for liability in the event of a security breach?

10. Does the site notify users if and when it changes its privacy policy?

Summary: Users should carefully read the privacy policies before using an app, site, or service to ensure that their privacy rights are not violated.

Activity Eight - Where Did Your Data Go?

Purpose: To demonstrate the problems with sharing information online.

Materials:

- Paper, poster, or whiteboard
- Writing utensil

Group Member Roles:

- The sharer - writes some information about a fictional character on the board or a poster.
- The re-sharers (other cadets) - copies what the sharer writes on the board.

Procedures:

1. The “sharer” writes information about herself or himself on the board. The information should not be sensitive and can even be made up. The “sharer” then leaves the room.

2. The “re-sharer(s)” have 30 seconds to copy the information written on the board to pieces of paper and hide those pieces of paper in the room.

3. The “sharer” returns and has 3 minutes to find every copy of the information created by the “re-sharer(s)."

Note: *It is unlikely that the sharer will find every slip of paper; this activity highlights how difficult it is to take back information once shared on a social media site or application. Even if the sharer successfully recovered every slip of paper，the “re-sharers” will still know what the note said.*

Summary: Once a user posts vital information online, there is no turning back. Your data can end up in the wrong hands. If it's too personal, then keep it to yourself.

4 PROTECTING YOUR DIGITAL FOOTPRINT

Learning Outcomes

- Define digital footprint.
- Discuss online usage and online reputation.
- Describe the characteristics of a healthy digital footprint.
- Identify cyberbullying and cyber predators and how to protect/report these attacks.

Important Key Terms

Active footprint - a trail of data intentionally left behind by a user who is deliberately sharing information about themselves on websites

Cyber bullying - a form of harassment using electronic communication, with the intent of intimidating or threatening a person or group of people

Cyber predator - an individual who exploits people via the internet intending to cause psychological, emotional, sexual, physical, or emotional harm

Cyber stalking - the use of electronic communications to harass or stalk someone

Cyber trolling - harassment targeted at an individual, relies on the engagement of other users to provide the potential victim

Digital footprint - a trail of data created by a user through online activity

Metadata - descriptive data that contains information about other data

Passive footprint - a trail of data unintentionally left behind by a user without that user's knowledge

Jake is applying for an internship with a local aviation company. Jake notices the application requires his social media information. Prior to completing the application, Jake goes to his social media accounts and deletes information he thinks might cost him his internship opportunity. Jake then completes the application and waits for the company to contact him.

The potential employer receives Jake's application and begins the review process. The company uses Jake's social media account information and his name to search online for information that can provide insight into his behavior. During the search, the potential employer finds old posts from Jake describing behavior the potential employer finds inappropriate. The potential employer then sends Jake a letter explaining that he is not the best fit for the company.

This chapter discusses how users, like Jake, can damage their digital footprint by practicing unethical behaviors online, the consequences of having an unhealthy digital footprint, and online safety practices.

DIGITAL FOOTPRINT

A **digital footprint** is a trail of data created by a user through online activity. Online activities include social media posts, online purchases, visiting websites, and communicating with others. There are two types of digital footprints. An **active footprint** is a trail of data intentionally left behind by a user who is deliberately sharing information about themselves on websites. For example, an active digital footprint results from a logged-in user making comments in an online forum or social media site. Because the user's name or profile can be linked to these posts, it is surprisingly easy to find out a lot about a person from the trails they leave behind. A **passive footprint** is a trail of data unintentionally left behind by a user without that user's knowledge. For example, a passive footprint occurs when a website collects and stores information about how many times a user visits.

Whether someone leaves behind information intentionally or unintentionally, other people can access that data. Depending on the amount of data someone leaves behind, other people can find a large variety of data through a simple search engine. In the example above, Jake unintentionally left data online that the potential employer found. By searching Jake's name, the employer was able to locate various information about his behavior.

How is a digital footprint used?

Digital footprints contain metadata and other sensitive information that can affect the security and privacy of users. **Metadata** is descriptive data that contains information about other data, for example, date, time, or location. Cybercriminals can use metadata to locate a user at a specific date and time. In addition to metadata, a digital footprint can contain sensitive information like demographics, religion, medical conditions, or interests. A cybercriminal can use this information to identify a target for burglary, fraud, or identity theft. For example, Mike lists his birthday on the public version of his social media account. Recently, Mike made a public social media post of a picture from a visit to his hometown. If a cybercriminal knows (or can guess) where Mike banks (for example based on 'likes' on Mike's social media), the cybercriminal has the information he or she could potentially use to answer security challenge questions to gain unauthorized access to Mike's bank account. This example is a reminder to be careful not to post sensitive information where it is publicly accessible.

It is important for users to consider how they share information online and how that information is stored. Content shared on the internet can remain accessible even after the user thinks he or she has deleted it. Companies often maintain records of posted information for legal purposes, if needed in the future. For example, the victim of a crime may subpoena the records from a social media site or other online organizations to support his or her course case.

Because of the uncertainty of how long data remains available online and the ownership of shared content, it is important to have a healthy digital footprint. If a user's digital footprint

exhibits unhealthy, or even illegal, behavior, that footprint can be detrimental to the user's future job prospects. There are two main factors that contribute to a digital footprint: online usage and online reputation.

ONLINE USAGE

Online usage is data flowing between a user's computer and the internet. Data flows from the user's computer to the internet (upload) and from the internet to the user's computer (download). Whether it's browsing the internet, chatting with friends, playing online games, or sharing photos online, any online activity users engage in generates information. Online usage can affect a user's digital footprint depending upon the type of content they engage with or share. Terrorist or hate groups often use online platforms to post content and promote their ideas. If a user associates himself or herself with one of these groups online, it could have a potentially negative impact on their digital footprint. User's should be careful about their online affiliations as they can have either a negative or a positive effect on future social and professional opportunities.

Users also need to take care about what information they share online. Doing something as seemingly simple and innocent as sharing a funny video or photo could unknowingly provide information a criminal needs to commit identity theft. For example, Adam Savage, one of the hosts of the "MythBusters" show, posted a picture of his vehicle in front of his house. The photo contained metadata that included the latitude and longitude of the photo's location. People who saw the post were able to identify exactly where he lived. The picture also had a caption that read "Now it's off to work." These two pieces of information together told potential thieves the location of his residence and that its occupant was currently at work, making it a prime target for a crime.

ONLINE REPUTATION

An **online reputation** is a collection of data that describes an entity (that is, a company, person, product, or service). Once information about an entity is available online, it is available to the public and should no longer be considered private. If a user searches for the entity, they may find posts, articles, photos, videos, social media profiles, and public records data. As the user continues their search, they might find additional information posted by other users that contributes to the online reputation of the entity. The way that the user interprets this information produces the entity's online reputation.

An individual's online reputation can affect their potential jobs and social relationships. As in the example earlier in this module, many employers commonly use online background checks. Potential employers can use the information about an applicant's online reputation to help decide whether they are a good candidate for the job. A person's online reputation can provide a potential employer with information to estimate how the applicant may interact with clients and other employees.

Online reputations can also be impacted by false information. When someone posts or shares information about an entity that is not true, it can damage the online reputation of that entity. Once this type of false information is available online, preventing its dissemination is difficult. A user can post false information either innocently (that is, they are unaware that it is false) or

maliciously (that is, knowingly posting false information with the intent to harm). Maliciously spreading false information about an entity with the goal of harming their online reputation can result in cyberbullying.

CYBERBULLYING

Cyberbullying is a form of online harassment that uses electronic communication to intimidate or threaten a person or group of people. This bullying behavior includes actions like posting rumors, threats, sexual remarks, hate speech, or sensitive information about someone else. Cyberbullying can occur through text, apps, email, social media, gaming platforms, and chatrooms. Cyberbullying can damage relationships because bullies can cause psychological or emotional harm to victims. As a result, cyberbullying victims may experience anxiety, depression, low self-esteem, and even suicidal thoughts.

Unlike traditional bullying, victims of cyberbullying may not know the identity of their bully or why the bully is targeting them. Cyberbullying has wide-reaching effects because of the large number of users that can see, share, and spread the negative content once it is available. Some cyberbullying activities are unlawful. Cyberbullying tactics include cyberstalking and trolling.

CYBERSTALKING

Cyberstalking is the use of electronic communications to harass or stalk another user. This cyberbullying tactic can threaten the victim's safety. Cyberstalkers repeatedly send threatening messages with the intent of causing harm. They can also encourage other people to participate in these activities. Cyberstalking is more than just the annoyance of receiving unsolicited email. Cyberstalking is considered an extension of physical stalking.

Due to the large amount of online data, a cyberstalker can easily locate sensitive information about a potential victim. To prey on their victims, a cyberstalker may create a web page that contains fake or fictitious information about their victim. The cyberstalker could also assume their victim’s identity to discredit the victim’s reputation, post embarrassing details about the victim, or solicit unwanted attention from other users. Cyberstalking includes several actions over time that cause distress to the targeted victim. Due to the rapid advancement of technology, anyone can be a victim of cyberstalking. Victims of cyberstalking can experience a large range of physical, emotional, and psychological distress including trouble sleeping, increased stress, eating disorders, and the loss of personal safety.

A **cyber predator** is someone who uses the internet to cause psychological, emotional, sexual, physical, or emotional harm to a victim. Cyber predators use cyber stalking to monitor or find their victims. Many cyber predators gain the trust of potential victims and lure them in by assuming a false identity or by lying about their details of their identity. Once a cyber predator has gained the trust of the potential victim, he or she usually begins communicating with the potential victim and monitoring their online behavior to identify ways to exploit the potential victim. These actions are illegal. Authorities can take legal action against cyber predators if they are caught and convicted. Here are some tips for fighting cyber predators and other criminals online:

1. Avoid revealing sensitive information such as your full name, address, or other identifying information.

2. Do not communicate with strangers or suspicious users.

3. Never agree to meet someone you do not know in person.

4. Report inappropriate or odd behavior or actions that make you uncomfortable to the website owners or other authorities.

5. Avoid using suggestive usernames or photos in your profile that could attract unwanted attention.

CYBER TROLLING

Cyber trolling, another form of cyber bullying, is harassment targeted toward an individual that relies on the engagement of other users to provoke the victim. Internet trolls provoke their victim to elicit a reaction. Trolls exist on several digital platforms, from group chats to social media. Trolls have varying goals: some engage in cyberbullying while others are just up to mischief. It can be difficult for users to distinguish between a troll and a legitimate user who just wants to dialogue about a topic. Some characteristics of a troll include a condescending tone, unrelated images, a dismissive attitude, and off-topic offensive remarks.

Cyberbullying, cyber trolling, and cyberstalking, can damage your online reputation and result in criminal action. States have varying ways of handling users who engage in these harmful activities, including fines, community service, and even jail time. In some cases, academic institutions can become involved, resulting in suspension or expulsion from academic programs and activities. A good way to ensure you are not engaging in these activities is to treat others the way you want to be treated, even online. If you begin to have moral or ethical doubts when sharing or posting information about other users, then you should reconsider whether this behavior is appropriate.

PREVENTING CYBERBULLYING

The following practices can help users prevent or fight against cyberbullying:

1. Do not share passwords or other account information - This will limit the possibility of bullies gaining access to accounts to post false, sensitive, or embarrassing information or pictures.

2. Only post photos that are deemed appropriate - If you would not want your family to see the photo, then you should not post it.

3. Think before posting - Avoid posting anything that can negatively impact your online reputation.

4. Set up privacy controls - Restrict who can see your online activities and profiles.

5. Check your digital footprint by performing a search - Search for yourself in major search engines and monitor the accessibility of personal information or photos online.

6. Never open messages from unknown users - Delete or flag messages from unknown users without reading them, as they could contain viruses and infect your computer.

7. Report the incident to the authorities - If there is an immediate risk of harm, then contact the police or other authority figures. If someone is experiencing distress, contact the National Suicide Prevention Lifeline.

Cyberbullying can happen to anyone. It is everyone's responsibility to report it and not engage in cyberbullying. One way to help prevent cyberbullying is by controlling the content available online. Users should create a healthy online reputation that will help positively shape their digital footprint.

CREATING A HEALTHY DIGITAL FOOTPRINT

Users can create a healthy digital footprint by minimizing the amount of information available online because once information is available online, removing it is nearly impossible. Users must be cautious about what they post. Digital footprints are like tattoos, permanent and in some cases very costly to remove. A user controls their digital footprint, which means the user is responsible for the positive or negative content that makes up the footprint. To create a healthy digital footprint, the first step is to avoid posting anything that would be considered unethical, illegal, or threatening to others. If a user believes that a post may haunt them or cause negative consequences, then the user should not make that post.

In the opening example, Jake's negative footprint cost him an employment opportunity. If Jake thought about how his digital footprint could affect future opportunities, he might have made better digital decisions. Employers and universities use digital footprints to better understand their applicants. A healthy digital footprint should highlight a user's skills and interest in a positive way. To begin managing a digital footprint, users can use the checklist below:

1. Delete inactive accounts - List all online accounts. Delete any accounts that are unnecessary. If you cannot delete an account, at least edit the available information.

2. Think before posting - Before sending or posting, think about how the content will affect your online persona. If the content does not positively represent who you are, then do not post it. If your previous posts no longer reflect your views or opinions, delete the comment or contact the site owner directly. While site owners are often not obligated to remove your information, some will do it for you.

3. Use privacy settings - Only post or share information that paints a positive public image of you. If you post personal information, use privacy settings to restrict this information to friends and family. Privacy settings help you monitor who sees your content on your social media streams. You should frequently check and update your social media privacy settings.

4. Keep all software up to date - Many malicious programs and viruses are designed explicitly to mine digital fingerprints. To help protect yourself, make sure you keep antivirus software and other software up to date.

5. Build your footprint through positive behavior - Ensure everything you post complements or positively impacts your online reputation. Avoid negative posts, untag yourself from questionable content, and keep critical comments to yourself. Consider building a positive reputation by starting a blog or website that showcases your skills or your interests.

Summary: A digital footprint can have a positive or negative effect on a user. The digital footprint is an extension of a user's thoughts and feelings. Its effects depend on your values, beliefs, priorities, school, and family expectations. A digital footprint is a self-portrait that users paint when they are online. It is important that this information is accurate and portrays who users truly are.

Chapter 4 Review Questions

1. What is cyberbullying?

2. How can a user create a healthy digital footprint?

3. What is the difference between a passive and active digital footprint?

4. How can a digital footprint be used?

5. What should a user do if they encounter a cyber predator?

Discussion Questions

Purpose- Cadets will apply knowledge gained from Chapter 4 to answer the following questions as a group.

Discussion 1: Do Internet Service Providers (ISPs) and social media companies have a duty to stop cyberbullying?

Discussion 2: What would you do if your friend or another classmate was demonstrating poor digital choices?

Discussion 3: What is the best way to take away a cyber bully's power? What is the worst way to react to cyberbullying? Is it okay to be a bystander of cyber bullying?

ACTIVITY 4 SECTION

Activity Nine - Leave Your Digital Footprint

Purpose: Cadets will illustrate their digital footprint.

Materials:

- Computer or Computing devices
- Markers
- Scissors
- Glue
- Magazines

Procedures:

1. Cadets will use their favorite celebrity's name to perform a search on three different search engines. Cadets will use the following variations of their celebrity's name:
- First name Last name
- First name Middle name Last Name
- First name Last name, City, State that the celebrity lives in

2. Cadets draw a footprint and fill the footprint with pictures or words from the magazine. The pictures and words should reflect the information found in Step 1. The size of the footprint depends on how much information is available online about their celebrity. Figure 4-1 is an example of the final product.

Figure 4-1: Example of a digital footprint collage

3. Exchange your digital footprint with other cadets. Repeat Step 1 using your partner's celebrity choice. Did you find information about your partner's celebrity that is different from what they found? How would you describe their digital footprint?

4. Present your findings to the squadron.

Summary: A digital footprint is a record of online activities and behaviors. It may include the recording of activities such as system login, visits to webpages, shared files, or online communications. The digital footprint allows interested parties to access this data for data mining, or profiling purposes. Having a healthy digital footprint can help market you to future colleges and employers!

Activity Ten - Who Are Your Real Friends?

Purpose: Cadets will examine their social media profiles and eliminate potential threats from cyberstalkers.

Materials:

- Computer or Computing devices with access to a social media website.
- Paper
- Pens/Pencils

Procedures:

1. Cadets will use their computing devices to open the social media site of their choice. Cadets will write down the number of friends, followers, or contacts they have on that site or service.

2. Cadets will browse through their lists and see if they know everyone on these lists. On the paper from the previous step, cadets will create a list of usernames of any follower they don't know personally or are unsure of.

3. Cadets will go to their profile and open the feature that allows them to view their page as another person. Select one of the people from the list in Step 2 and view their profiles from the perspective of this person. Make a list of information that this person would be able to gather (locations, birth date, vacation spots, etc.).

4. As a squadron, the cadets will discuss with the different ways in which the users from their list in Step 2, might use or abuse this information.

Note: *If there are cadets who don't use social media sites, this can be a partner activity.*

Summary: It is important that you only befriend other users you know in real life to avoid a potential attack by a cybercriminal. Monitoring who can see your profile by using your privacy settings can keep malicious users (i.e. cyber predators) away.

Activity Eleven - Say No to Cyberbullying

Purpose: Cadets will identify cyberbullying and provide solutions to combat it.

Materials:

- Writing utensil
- Paper

Procedures:

Divide cadets into 6 groups. Assign each group a cyberbullying scenario. The groups each prepare a presentation answering the questions below. Each cadet will be responsible for at least one of the questions during the presentation.

1. What kind of cyberbullying was it?

2. How do you predict being cyberbullied makes the victim feel? What are some of the physical, social, and emotional effects of this kind of cyberbullying?

3. How should the victim handle the situation?

4. What should be the consequences for the cyberbully/bullies?

Scenarios:

Scenario 1: Amber is getting ready to travel with the debate team to a competition. To look her very best, she tries out a new skin care cream the night before the trip. Amber has an allergic reaction that causes her face to swell. While traveling on the bus to the competition, another student takes an embarrassing photo of Amber. He then posts the photo on social media with a caption mocking her allergic reaction and sends the photo to all the other teammates without her permission.

Scenario 2: Michael constantly bullies a player on his hockey team. One afternoon, Michael apologizes to the player and asks him to join an online game later that day. Joe, the bullied player, is relieved, but little does he know Michael purposely asked other players to join the game so they can humiliate Joe. During the game, Michael also engages in aggressive behavior, including sending threatening and harassing messages. Joe begins to feel even worse and he no longer wants to be part of the hockey team.

Scenario 3: A group of cheerleaders does not like the new coach's policy of rotating cheer captains. They create a plan to try to have the coach removed. They record the coach at school and practice then digitally alter the video. They create a website in the coach's name and post the digitally enhanced video showing the coach using profanity and hate speech. The coach is so upset, she quits.

Scenario 4: Two students tease each other during school. The students are punished and the teacher thinks that the fighting has stopped. Rather than fight at school, the students start an online fight. Student A creates a web page embarrassing student B. Student B starts an online group spreading horrible rumors about student A's family.

Scenario 5: Ashley broke up with Jake a few months ago. Jake says he is really upset and can't get over her. Ashley requests that he gives her some space, but he continues to send her direct messages on social media. Jake embarrasses Ashley by sending a humiliating picture of her to the student body.

Scenario 6: Lauren was attacked when an anonymous poster started a thread on a message board making fun of her. The cyberbully teased Lauren about her weight. The cyberbully also made horrible comments about Lauren's living conditions. However, the bullying didn't stop there. Someone egged Lauren's car and vandalized her house. Lauren's friends decide to defend her by reporting the message board and asking other users if they knew any information about the cyberbully.

Summary: Cyberbullying is never ok and could negatively affect someone's life. If you or someone you know is experiencing cyberbullying, please seek help immediately.

5 THE FUTURE OF CYBER SECURITY

Learning Outcomes

- Discuss different professional paths to future cyber security jobs.
- Discuss different certifications for cyber security.
- Discuss the role of cyber security professionals in companies when attacks happen.

Important Key Terms

Computer Science - the study of computing systems and their functionality

Amy is starting her daily work routine when she receives an email from her company's headquarters that all operations have been shut down for the day. Amy notices concern in her coworkers. Amy's manager then calls an emergency meeting. During the meeting, the manager explains the company is experiencing a ransomware cyber attack. The manager states that the cyber security department is working around the clock to mitigate the attack. Amy will not be able to assist any of her clients, conduct business meetings, or bring in any revenue until the ransomware attack is over. While cybercriminals are attacking companies like Amy's at an alarming rate, cyber security professionals work diligently to prevent and defend the system from these attacks.

Cybercriminals do not need specialized training to perform malicious activities. They can find numerous attack scripts and tutorials readily available on the Internet. As a result, the number of cybercriminals has increased. However, skilled cyber security professionals possess the security knowledge and talent needed to fight against these attackers. Cyber security professionals must stay current with the techniques and strategies necessary to defend systems against cybercriminals.

While cyber security professionals do not often make the news headlines for their hard work, their work is of national importance. These cyber security professionals are responsible for protecting information and assets from criminals whose attacks could cripple the country's technological infrastructure and compromise national safety. A cyber security career is both a means of public service and a way to make a living.

This chapter discusses pathways into cyber security careers, the roles of cyber security professionals, cyber security certifications, and cyber security jobs.

CYBER SECURITY CAREER PATHWAYS

Today's smartphone contains more advanced technologies than the computers that sent the first man to the moon. The mobile applications currently in use were only the subjects of science fiction movies and novels just a couple of decades ago. With the rapid technological advancement, it is difficult to predict what will happen next or the source of the next threat.

A key problem is the lack of cyber security professionals to meet cyber security needs and to fill vacant positions. The number of cyberattacks will continue to rise, which places the national technological infrastructure at risk. There are many opportunities for careers in cyber security due to the increasing demand for cyber security talent. Many organizations, including those in the health care, government, finance, and retail domains, hire cyber security professionals to protect their IT infrastructures. There are different types of cyber security professionals who contribute to an organization's overall cyber security. Understanding the responsibilities of these different cyber security roles can help someone decide whether a career path in cyber security is right for them. There are two approaches for pursuing a career in cyber security: a cyber security degree or a cyber security certification.

DEGREE PROGRAMS

Aspiring cyber security professionals can enroll in a degree program at a college or university. There are many reasons why individuals should consider pursuing a cyber security degree. In addition to the formal training and experience one can gain, there is also the urgent demand for educated and qualified cyber security professionals to meet the demands of companies willing to pay high salaries to protect their digital assets.

With increasing concerns over the cyber threats facing organizations, governments, and individuals, institutions of higher learning, such as the University of Alabama, offer Bachelor of Science in Cyber Security degrees. Some institutions even offer courses online, making it more convenient for students who may be working full-time or who are located in a different city. To properly prepare students with the appropriate knowledge and skills, educators design the curricula for these programs based upon input from cyber security practitioners, stakeholders, and leaders. Through these programs, students also gain leadership, time management, and communication skills that will benefit them in the workforce. Graduates of these programs often find lucrative employment in the cyber security profession.

Universities and colleges that do not offer a dedicated cyber security program, may have a Computer Science degree that can provide similar knowledge and skills. Computer science is a broader field that encompasses aspects of cyber security along with other topics. Computer Science degree programs provide students with fundamental knowledge about computing systems and how they operate. These programs often include cyber security courses. While a degree in Cyber Security will provide a student with more depth in cyber security than a traditional computer science program will, a degree in Computer Science can still open the door to numerous cyber security career options.

CYBER SECURITY CERTIFICATIONS

While a formal degree in Cyber Security or Computer Science can help ensure an individual has the appropriate background, certifications are another path into a cyber security career. With the current shortage of qualified professionals, many organizations will hire individuals, who do not have a degree, for entry-level cyber security positions as long as they possess appropriate cyber security certifications.

It can be less expensive and more convenient for an individual to earn a certification than to complete a full degree program. Cyber security certifications are beneficial as a supplement to other qualifications. These certifications can provide a solid foundation of security fundamentals necessary for someone to be successful in cyber security. There are multiple online resources that provide training, study material, and courses for specific certifications. To obtain a certification, an individual typically must study relevant material, pay a fee, and then pass a rigorous exam on the concepts related to the certification. If successful, the individual can use the certification to make their resume more appealing to potential employers.

Many companies view certifications as a differentiator between applicants. Certificates can be valuable even if someone has a degree in Cyber Security or Computer Science. These certifications make them more marketable to employers. In addition, some institutions of higher learning will accept certifications for credit to a degree. Individuals can obtain certifications that cover the following topics, and many more:

- **Introductory Cyber Security Skills** - These certifications help IT professionals who are new to cyber security and are looking to gain a basic foundation. The certifications cover basic IT security concepts, including network attacks and defenses, security policies, business continuity, disaster recovery, encryption, and cryptography. These certifications aim to help an individual establish the core knowledge required for most cyber security roles. This type of certification can help an individual pursue entry-level cyber security positions.

- **Ethical Hacking** - These certifications ensure individuals can assess the security of a system and understand how to identify system vulnerabilities, which cyber criminals can exploit to gain access. The certifications focus on the skills necessary for someone to think and act like a cyber criminal, including topics like hacking technologies, malware and viruses, mobile platforms and operating systems, security laws, and standards.

- **Information System Security** - System security certifications focus on the technical aspect of securing information assets. More advanced cyber security specialists often pursue certifications focused on information system security as evidence of their expertise with information security. These certifications include risk management, security operations, access control, networking, cryptography, and telecommunications.

- **Penetration Testing** - Penetration testing is the process of testing a system to identify vulnerabilities through simulated attacks. People with the ability to perform penetration testing are in high demand. Penetration testing certifications include vulnerability scanning, web application attacks, buffer overflows, antivirus, and privilege escalation.

In addition to these examples, there are a number of other cyber security certificates available. Each certification can open different doors into a cyber security career. Each person should choose the certificate(s) that best fits their interests.

CAREERS IN CYBER SECURITY

A cyber security career can be both rewarding and challenging. Cyber security professionals are well compensated, have opportunities for advancement, and enjoy job security. In addition, the intangible benefits of a cyber security career can be equally fulfilling, including preventing cyber criminals from gaining access to sensitive systems and protecting the secret information in an organization, business, or even the federal government.

Cyber security careers are also challenging because of the evolving nature of cyber security and cyber criminals. As attackers become more sophisticated, cyber security professionals must adapt to protect against new types of attacks. The cyber security field is ideal for individuals who have a love for technology and security. Cyber security professionals who work for the government may be responsible for protecting top-secret information and other national security secrets. Similarly, private sector cyber security professionals protect databases, websites, and devices that are critical to the success of a business or organization. Cyber security professionals can progress through several phases in their careers based on their education and experience.

- **Entry-Level Positions:** Ideal for individuals who are looking to gain experience in the cyber security field. Some positions require a degree, while others require certification and experience. Examples of entry-level positions include security specialists, technicians, and investigators.

- **Intermediate-Level Positions:** Ideal for individuals with three to five years of cyber security experience. Examples of intermediate-level positions include cyber security analysts, security consultants, and penetration testers.

- **Advanced Positions:** Ideal for individuals with more than five years of cyber security experience. Examples of advanced positions include cyber security engineers, security architects, and chief information security officers.

Table 1 depicts some of the most in-demand jobs at different levels in cyber security.

Table 1: Cyber Security Careers and Responsibilities

CYBER SECURITY CAREERS AND RESPONSIBILITIES		
Entry Level		
Security Specialist • Conduct security inspections for an organization's IT infrastructure • Search for security vulnerabilities • Manage and monitor systems for attacks and intrusions	**Cyber Security Investigator** • Identify security issues within an organization and reporting them in real-time • Analyze potential security vulnerabilities and solutions • Protect computer system by defining access privileges, security standards, and system controls	
Intermediate Level		
Cyber Security Analyst • Perform security assessments by conducting security audits • Protect hardware, software, and networks from cybercriminals • Ensure that all security standards are met	**Cyber Security Consultant** • Develop security strategies to prevent threats • Perform threat analysis on systems • Maintain standard cyber security procedures	**Penetration Tester** • Perform penetration tests on an organization's systems, networks and applications • Probe existing security measures to identify security weaknesses • Document and report security issues
Advanced Level		
Cyber Security Engineer • Manage and monitor security measures • Troubleshoot security problems through testing and analysis • Engineer secure, trusted systems	**Cyber Security Architect** • Implement security strategies • Build security architecture elements to mitigate potential risk • Identify gaps that exist in current security architectures	**Chief Information Security Officer** • Implement a strategic security programs • Work directly with other management personnel to facilitate risk assessment • Provide leadership within an organization's IT department

Summary: Cyber security professionals are the modern-day heroes of cyberspace. Their work protects sensitive and important systems and information by keeping malicious hackers away. By earning a certification or degree, an individual can be a part of the fight against cyber criminals and enjoy a rewarding career.

Chapter 5 Review Questions

1. Give some examples of the types of skills covered by cyber security certificates.

2. What are the different career pathways for cyber security?

3. What is the difference between an entry level and intermediate level position?

4. Name four cyber security jobs and their duties.

Discussion Questions

Purpose: Cadets will apply knowledge gained from Chapter 5 to answer the following questions as a group.

Discussion 1: What are some benefits of pursuing a degree or certification in Cyber Security or Computer Science?

Discussion 2: Would you rather have a boring job that just allows you to make a living or a rewarding and enjoyable career?

Discussion 3: Why are cyber security professionals important in healthcare, education, or government agencies?

ACTIVITY 5 SECTION

Activity Twelve - Career Profile

Purpose: To explore different career pathways in cyber security.

Materials:

- Computer or mobile devices
- Pen or pencil
- Poster board

Procedures:

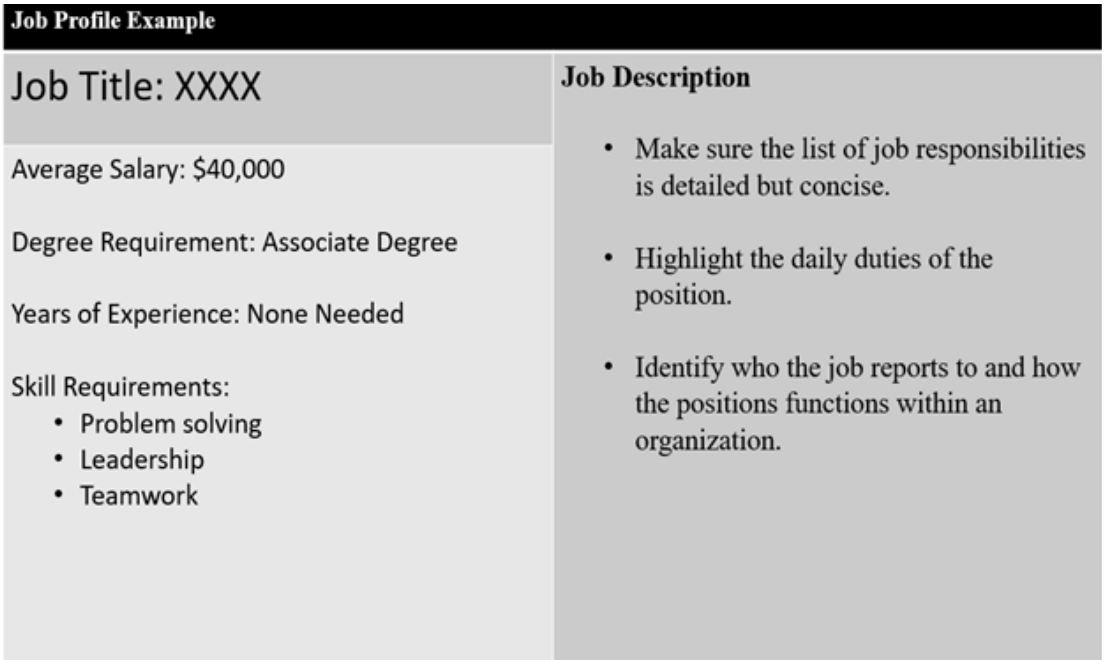
1. Cadets will use their desired search engine to research a cyber security profession of interest. Once the research is complete, each cadet will create a career profile using the poster board.

2. Each profile should contain the following information:

- Job Title
- Job Description
- Average Salary
- Degree Requirements
- Skill Requirements

Figure 5-1 is an example of a job profile posterboard.

Figure 5-1: Job Profile Example



3. After the profile has been created, cadets will present their profile to the squadron and discuss the similarities or differences between jobs.

Summary: Career exploration can help cadets better understand the different career options in cyber security.

Activity Thirteen - Lightning Speed

Purpose: Cadets will practice formulating proper responses to interview questions.

Materials:

- Timer
- Lighting Speed Interview Worksheet
- Writing utensils

Group Member Roles:

- Observer - watches, rates, and notes their observations of the interview on their worksheet.
- Interviewer - asks the questions provided by the worksheet and rates their interviewee's response.
- Interviewee - answers the questions to the best of their abilities.

Procedures:

1. Cadets will be divided into groups of three. Cadets will prepare to participate in a brief mock interview by conducting online research about typical cyber security interview questions. Cadets should treat this activity as an actual interview as much as possible.

2. Set the timer for four minutes and start the interview. Cadets should complete the Lightning Speed worksheets and conduct their interviews during this time.

3. When the four minutes have passed, stop the interview. The observer and interviewer will have two minutes to offer feedback to the interviewee. Repeat this process until everyone has had a chance to be the interviewee.

4. Lastly, cadets will discuss lessons learned and observations made during the interview to help the entire group.

Summary: Interviews are essential because they allow potential employers and employees to determine whether skills and character align with their needs. Interviews also allow potential employees the chance to market themselves outside a resume.

Name _____ Date _____

LIGHTNING SPEED INTERVIEW WORKSHEET

Complete the following worksheet by providing your interviewee rates.

Rating values: 1-poor; 2-fair; 3-neutral; 4-good; 5-excellent

Tell me about yourself. Notes:	1	2	3	4	5
How would your teachers describe you? Notes:	1	2	3	4	5
What are your strengths? Notes:	1	2	3	4	5
What are your weaknesses? Notes:	1	2	3	4	5
Why should I hire you? Notes:	1	2	3	4	5
Do you have any questions? Notes:	1	2	3	4	5
Rate the candidate's body language. Notes:	1	2	3	4	5
Rate your overall impression of the candidate. Notes:	1	2	3	4	5

THE UNIVERSITY OF

ALABAMA