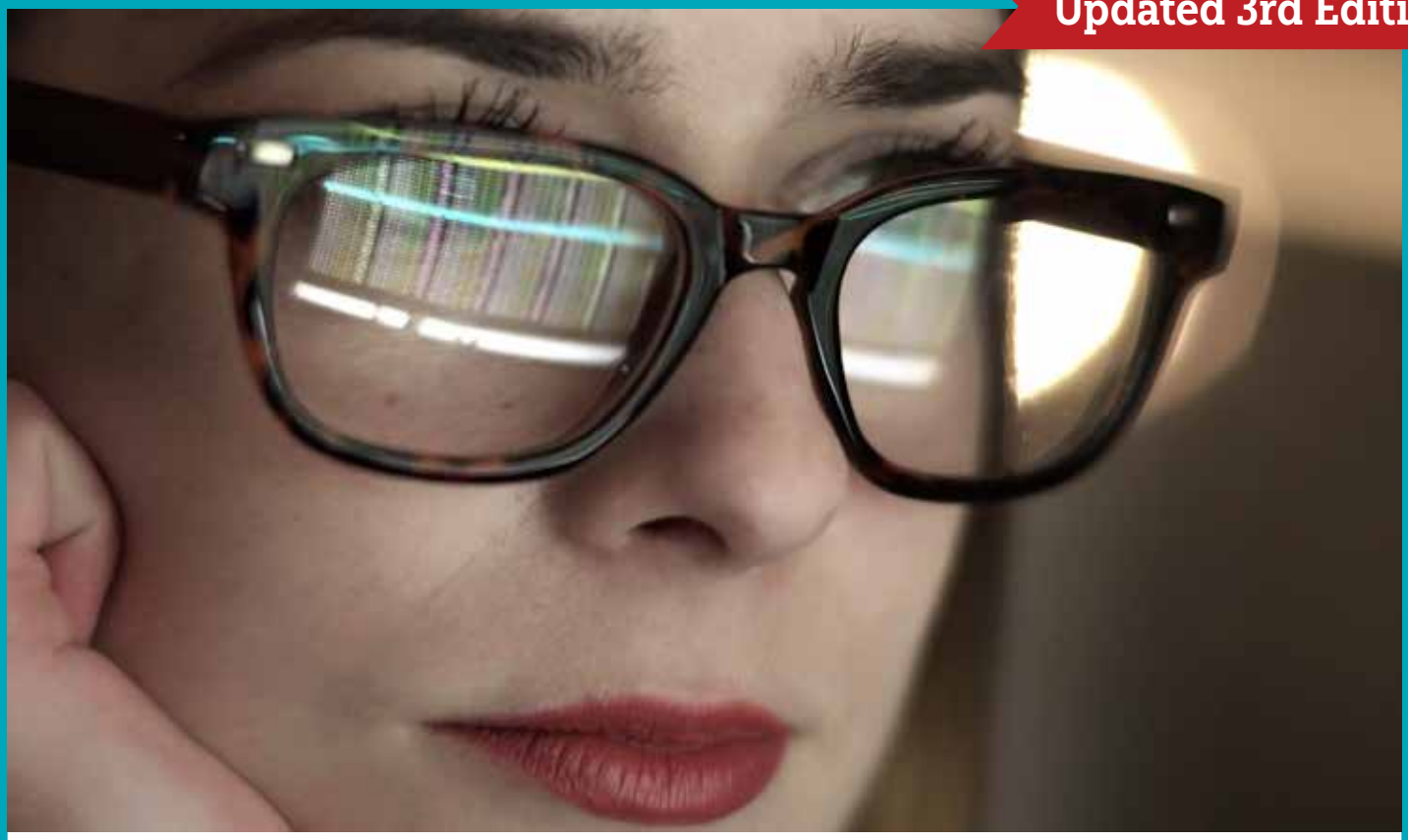
Updated 3rd Edition!



Cyber Career Awareness Program (CyberCAP)

STUDENT WORKBOOK

DISCOVER AND LEARN:

What is cybersecurity and why should I care?

What can I do to stay safer online?

How do I know if I like or can do cybersecurity?

How do I figure out if a career in cybersecurity could be right for me?

Find the answers to these questions — and more! — inside.

Start Engineering

Dear Student,

If you've read the **Start Engineering Cybersecurity Career Guide**, you already know that cybersecurity is one of the hottest career fields around.

Data breaches, phishing scams, and information systems break-ins are almost daily news. Anyone who lives any part of their life online could fall victim to cybercrime. Cybersecurity professionals work every day to protect us and our data from the threats coming out of the dark corners of cyberspace.

Reading the lessons and completing the exercises in this workbook can help you take the first step on your journey towards becoming a cybersecurity professional yourself. You will learn how to better protect yourself and your family online, how your skills and interests line up with needs in the field, and what kinds of cybersecurity jobs might fit you best.

The next steps will be up to you. After finishing the workbook, go back to our **Cybersecurity Career Guide** and take stock of all your options for schooling and degree programs. Look at the kinds of jobs and companies open to people trained in cybersecurity. Flesh out your plans with help from parents, teachers, counselors, and any cybersecurity professionals you can connect with.

As a country, we need people from all kinds of backgrounds with all kinds of skills dedicated to our cybersecurity needs. We hope both our workbook and career guide help you discover how you can make your own, unique contribution to this effort.

Good luck and good learning!

Robert Black
CEO, Start Engineering

CONTENTS

CHAPTER ONE

What Is Cybersecurity and Why Should I Care?

What do you think is worse? Having 1,000's of dollars – or more – of financial crimes attached to your name because of identity theft. Or having revealing pictures of yourself posted online for all the world with an internet connection to see.

If you are a teenager, you might not have to choose.

Every year, cyber criminals steal sensitive, personal data belonging to over 1 million kids and use it to open fake bank accounts and credit cards in the kids' names. In most cases, underage victims of identity theft like this will not even know about these crimes until they try to open up their own, real accounts and find their names attached to acts of fraud they did not commit.

Meanwhile, in 2014, cyber criminals stole almost 100,000 photos and videos delivered through Snapchat. Thousands of these stolen messages contained nudity and explicit messages in-

tended for private sharing only. About half of them came from Snapchat users between the ages of 13 and 17. The fact is that cyber criminals are always looking for new, devious ways to get access to things online they're not supposed to have.

Indeed, the very act of going online opens you up to risks of a totally different kind from those you face in real life. Even if you take every precaution, your data can find its way into the wrong hands, with unpredictable, possibly dire consequences.

In cases of underage identity theft, kids' data can get released into the digital wild via attacks on schools' electronic student records. In 2019, for example, personally identifiable information, or PII, for tens of millions of students was exposed when hackers broke into the online systems of Pearson, a major testing services provider used by thousands of schools across the country. And in the case of the Snapchat leak, hackers broke into the systems of a third-party app that was allowing people to save and store Snapchat messages, even though Snapchat is designed for messages to self-destruct after a short period of time.

ONLINE NETWORKS

As the examples above show, participation in online networks inevitably puts our data at risk of compromise, often because of factors beyond our individual control. Our safety within these networks is a function of two general phenomena, one technical and one behavioral:

1. Online networks need to be built and managed to protect against people getting unauthorized access to network participants and their information.

2. Participants need to make ethical, appropriate use of the network, respecting the privacy and interests of others on the one hand, and on the other, following good security practices.

You might be surprised how many online networks you and your family belong to. Of course, there is Snapchat, along with TikTok, Instagram, email platforms, and other networks that help us communicate with each other.

But what else? If you buy from Amazon, Apple, or other online retailers, you're in their network. Your providers for cell phone, internet, electricity, or water service also count you in their networks, along with any other companies with whom you or your family might have an account.

Complete the activity on the next page about your networks to understand more about how you and your family might be exposed to risks from attacks against online networks.

ACTIVITY 1: Networks

GETTING TO KNOW YOUR NETWORKS

How many online networks do you think you and your family belong to? Try to identify below as many networks as you can that you and your family belong to. Then find out if any of your family's accounts have been compromised by going to www.haveibeenpwned.com. Describe any breaches you discover and what, if anything, you and your family might do about it.

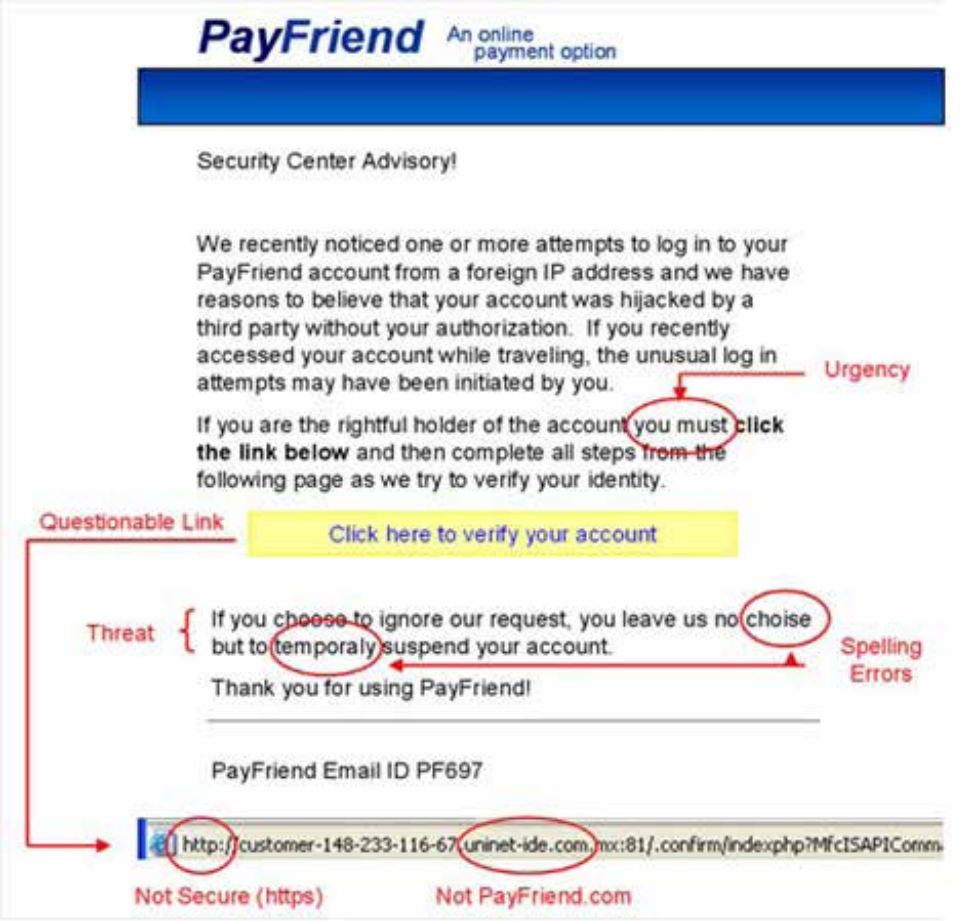
DECEPTIVE ONLINE COMMUNICATIONS

Cybercriminals are constantly testing and developing new ways to separate internet users from their PII. In the Snapchat case above, malicious hackers broke into a third-party network used to capture and store users' personal information and files. In other cases, they target people rather than networks, trying to trick them into divulging the userids, passwords, and other pieces of information needed to get illegal access to others' personal data. Some of the most common, most effective tactics involve emails and other message types that look innocent or familiar but are meant to deceive. "Phishing," and other forms of "social engineering," all seek to trick people into opening attachments or clicking on links that enable cybercriminals to gain access to PII, which they can use for nefarious purposes.

Identifying a bogus email or website can be challenging. Most social engineering scams seek to present their communications as coming from people or online institutions already familiar or trusted, but they also tend to feature some or all of the same give-away traits:

- **They're too good to be true!** Exciting, out-of-the-blue prizes, offers of money for nothing, and so on should tell you not to click on anything and just delete the email.
- **Act now!** When an unexpected email wants you to take urgent action, the only urgent thing to do is delete it.
- **Funky hyperlinks.** If you hover over a hyperlink, you can see the URL. Look for typos, extra-long URL's, or some other indication of trickery.
- **Unexpected attachments.** A dead give-away in almost every case – if you're not expecting an attachment in an email, don't open it. If you have any questions, follow up with the sender before opening it to confirm validity.
- **Unknown sender.** If you don't recognize the name or address of the sender, don't open it.

EXAMPLE OF BOGUS PHISHING EMAIL



DON'T GET HOOKED! HOW TO IDENTIFY PHISHING SCAMS

Identifying phishing scams gets easier with practice. The online phishing quizzes shown below are just some of the options you can find online with a simple keyword search for "phishing quiz."

Phishing quizzes:

https://www.opendns.com/phishing-quiz/

https://www.sonicwall.com/en-us/phishing-iq-test

https://phishingquiz.withgoogle.com/

https://www.phishingbox.com/phishing-test

https://accellis.com/phishing-quiz/

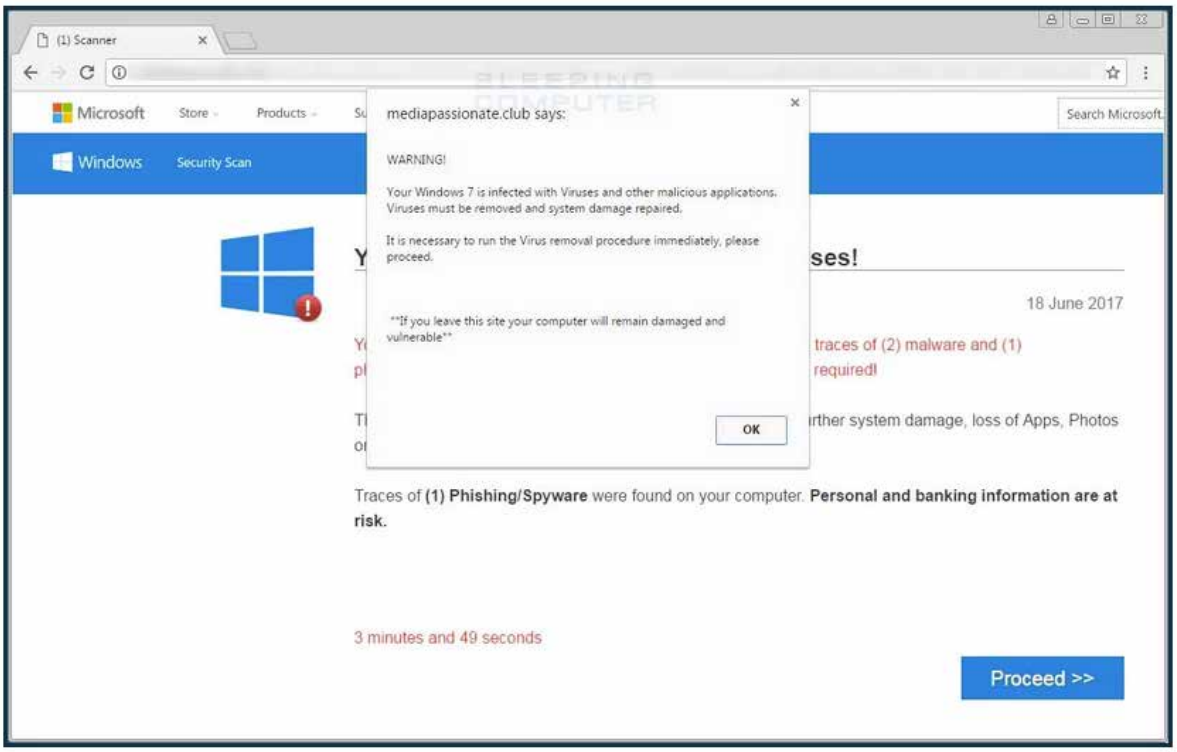
https://www.security.org/resources/something-smells-phishy/

In addition to phishing schemes over email, cybercriminals also use social engineering tactics in other online environments to trick people into compromising behaviors. In these other settings, hackers try to entice users into clicking on links or downloading files that expose their computers or online identities to bad actors' malicious ends.

Sharing apps like Snapchat or Instagram can connect kids with friends and family members but they can also circulate personal information among strangers, especially when privacy settings are not used properly. Even anonymous sharing apps like Whisper or Anomo can become risky when exchanges start to include potentially identifiable information or come with links and attachments designed with malicious intentions.

Social networks like Facebook or YouTube present a host of interactive features that hackers can exploit, like messaging tools, comment entries containing deceptive URL's, and alluring content that entices clicking into dangerous online environments.

Pop-up windows appear all over, from websites to online games to text messages on phones. Threats, urgent calls to action, unfamiliar or strange URL's, and awkward phrasing are just some of the warning signs of a dangerous pop-up message.



ACTIVITY 2: Identify Deceptive Online Communications

From the options on the previous page or others you find on your own, **pick out 3 different online phishing quizzes to take, then come back and complete the exercise below.**

1. What 3 quizzes did you take? Provide the URL's below.

2. How did you do? Write down either the scores you got on all 3 or other forms of feedback you received.

3. Did your performance improve? Why or why not?

4. What was the hardest part about the quizzes? What was the easiest? What was surprising or different from what you'd expected?

5. Have you received phishing emails? Have you or anyone you know ever fallen for a phishing scam? What happened?

ACTIVITY 3: Engineering Your Own Scam

1. How would you design a social engineering scam? Would you use email or perhaps try to lure people to a website by clicking a link or get them to download a file? Describe the steps you would take to build your scam and its ultimate goal.

2. What are three tips for avoiding online scams that you would share with a relative or friend who is not very internet-savvy? Rank your tips based on how feasible and effective they are, and consider tradeoffs they involve between security and accessibility.

MALWARE

Malware is software designed by cyber criminals to gain access to and damage other people's computers or computer networks. It is short for "malicious software," and malware often does its dirty work on your computer without you even knowing it's there. In most cases, malware is spread by emails that entice or trick people into opening attachments, clicking on links, or interacting with pop-ups that provide an entryway into the user's computer or network.

To avoid falling prey to malware, you should ideally verify the trustworthiness and legitimacy of any invitation to click a link or download a file. Airtight verification, though, is rarely possible, so always be vigilant and thoughtful, and take measures to protect the computers you use to go online. That means keeping operating systems up to date, installing antivirus programs, maintaining firewalls, using protections built into web browsers, and generally remaining alert to the risks lurking all over the internet.

Viruses and worms are the most common forms of malware. A virus establishes itself on a user's computer and carries out programmed attacks on the data or operating system. A worm works like a virus, except that it spreads on its own from one computer to the next to cause harm. One of the fastest-growing forms of malware is ransomware, software smuggled into a data network that encrypts files critical to an organization's operations. Cyber criminals follow up with demands for money in exchange for a decryption tool needed to restore files to readable, usable form. The pace of such attacks, by one study, nearly tripled from 2020 to 2021. The calamitous ransomware attack on Colonial Pipeline "highlighted" the trend, forcing the shutdown of all the company's fuel-delivery networks and causing panic buying at gas stations up and down the east coast.

TYPES OF MALWARE ATTACKS

Malware that circulates through a device/network:

Virus: Malicious code spread through downloads from websites, email attachments, or portable drives. It reproduces itself in your computer, damaging performance, corrupting data, and harvesting PII, among other nasty things.

Worm: Malware that replicates throughout a network. Unlike viruses, which rely on a user spreading the virus through action, a worm spreads on its own. Worms cause the most damage when they destroy data on a network or allow the attacker remote access.

Malware that collects data:

Adware: Annoying or offensive ad pop-ups, banners, or graphics, adware is usually seen as a "potentially unwanted program" or PUP. It can track online activities or physical locations, and when this kind of information leads to harmful follow-up, adware turns into malware.

Spyware: Tracking software used without the consent of the user to collect data such as keystrokes, browsing habits, location data, or even login information. Spyware data are then harvested and sold, usually to cyber criminals, for them to exploit however they can.

Malware that modifies or deletes data:

Ransomware: Software that encrypts data on a device until the user agrees to pay a fee to unlock it or risk it being deleted.

Backdoor: A piece of code installed without a user's knowledge that allows a malicious user to circumvent system security settings and get illegal access to data in a network.

Logic bomb: Malicious code added to a legitimate program that is triggered by a specific event. Logic bombs can lie dormant for lengthy periods of time.

Malware used to launch attacks:

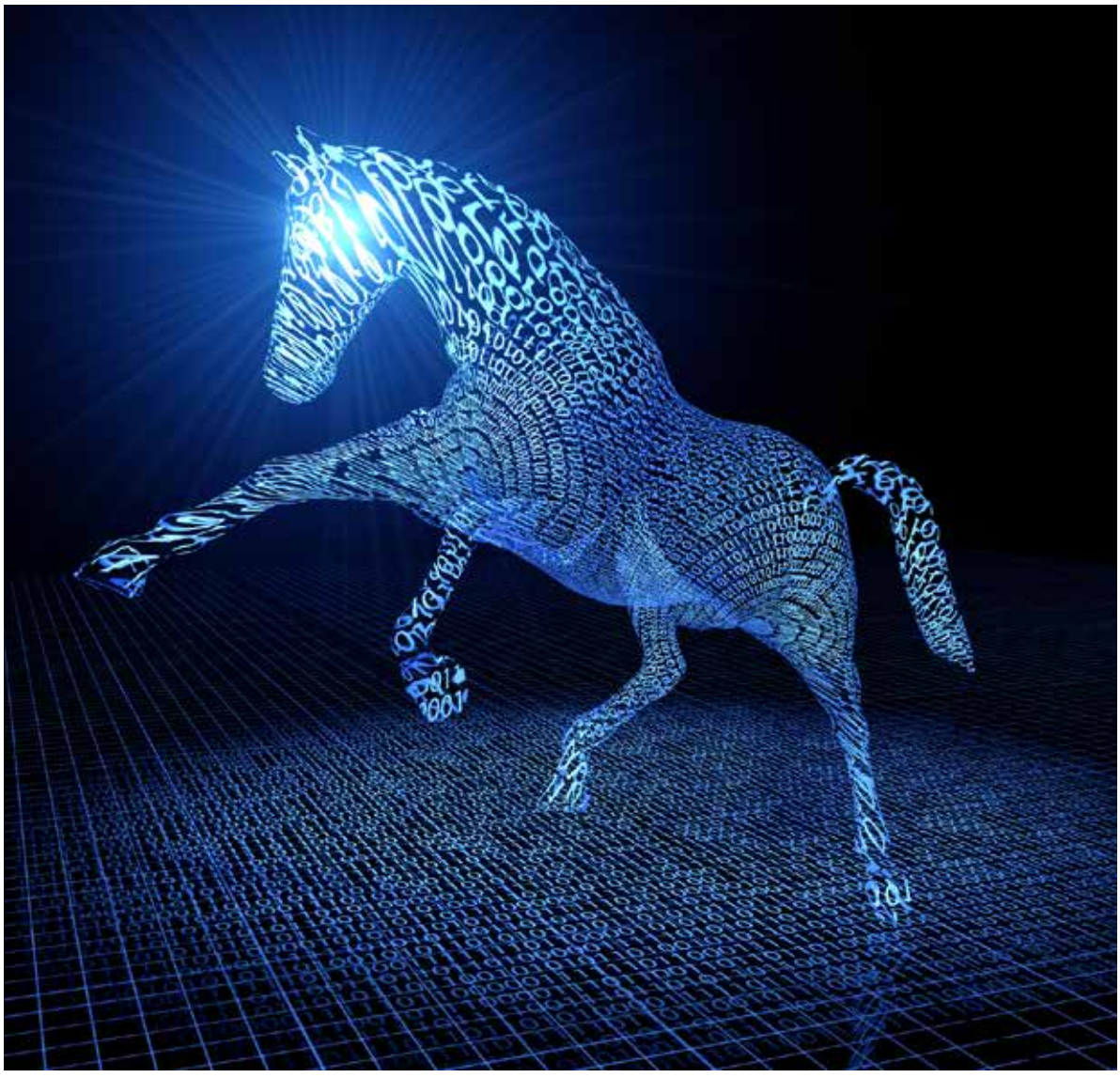
Botnets: Bots (individual computers) that form a network of compromised computers, controlled by a third party and used to transmit malware or spam, launch attacks, steal data, or to spy on user activities.

TYPES OF MALWARE ATTACKS (CONTINUED)

Malware that hides itself in a device/network:

Rootkit: Software that allows remote control of a computer by a third party. Once installed, it allows a remote attacker to steal data or install botware, spyware, spamware, or keystroke loggers.

Trojan horse: A seemingly legitimate program that hides a malicious code/program within. For example, an online game you download might hide a keylogger that records your keystrokes and steals all your passwords.



ACTIVITY 4: Research Malware

Pick out one of the types of malware identified on previous pages. In online research, gather information as described below:

1. What type did you pick? What is it?

2. How does it make its way onto users' machines?

3. Find and describe two examples of real-world incidents in which this malware caused damage or disruption to computer networks.

4. How can people prevent this type of malware from infecting their computers? Identify as many methods of prevention as you can. When you consider preventive measures, assess how feasible they are and what tradeoffs they involve between keeping information secure versus keeping it accessible.

CONCLUSION

In this chapter, you learned about cybercrime and how it can touch you, your family and friends, your school, and really anyone who's anywhere online. Participating in any online network can put all of us at risk of cyber attacks. As you have learned, cybercriminals mount attacks on networks using an ever-changing, ever-growing set of digital weapons.

In the next chapter, you'll learn how you can act to help protect yourself and the networks to which you belong from cyber attacks. From understanding risks to a general grasp of cybereth-ics to building strong passwords, you as an internet user can make choices and do things to help keep the internet safe for yourself and other people, too.

CHAPTER TWO

What Can I Do to Stay Safer Online?

Using the internet is like ... riding a bicycle. Wait, what? You might not remember it, but learning to ride a bike is weird and confusing. Learning to use the internet can feel the same way. But once you get the hang of both, you never forget.

Bicycles are fun, and they help us do things we need and want to get done, like go to school, visit a friend's house, do errands, and so on. The internet can be fun, too, and it has become a necessary part of how we learn, work, play, and live. But in both cases, safety is fundamental. Bicycle owners have to learn how to ride safely in areas where other people walk, drive, and ride their own bikes. They also have to keep their bicycle safe, locked up in a garage or safely chained to a bike rack out in the world. Bicycle safety requires care, planning, and attention.

Using the internet safely takes care, planning, and attention, too. You have to figure out where you want to and can go safely, how to identify risky situations, and how to protect anything you share about yourself online. As we learned in chapter one, many risks await all of us when we put personally identifiable information, or PII, online.

The good news is that you can do a lot to keep you and your PII safer online. Your attitudes and behaviors about using computers have a lot to do with determining how risky your online life ends up being. In this chapter, you will learn various ways to think about and practice online safety — from following broad ethical principles to technical guidance in building strong passwords — that will reduce your risk of falling victim to cybercrime.

ONLINE BEHAVIOR

A cybersecurity incident almost always starts with a choice someone makes to do the wrong thing. From criminal penetrations of guarded networks to sloppy password habits to clicking on virus-infected attachments or bogus website links, cybersecurity breaches result from a myriad of causes. But they almost universally reflect the failure of people to follow ethical principles meant to preserve the safety, reliability, and privacy of online network.

In 1992, the Computer Ethics Institute put forth a set of ten "commandments" for people to follow in the use of computers and information technology:

TEN COMMANDMENTS FOR COMPUTERS AND INFORMATION TECHNOLOGY

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

ACTIVITY 1: Cyberethics

Below you'll find scenarios describing situations and choices people face in using computers for access to digital networks. For each scenario, you'll be asked to decide if a breach of ethics has occurred, which ethical principle is in play, and what other outcomes might have been possible, for either good or bad.

Scenario #1

You found a cool, new online game that requires just an email address for signing up and playing. Winning points allows you to play at higher levels for longer periods of time, and it also increases the visibility of your online avatar in the playspace. Plus, every month, the game company promises $100 Amazon gift cards to the top 10 point-winners. One day, you get an email from the game company offering to double your point total if you provide the email addresses of five friends. You do nothing. The next day, you get another email offering to triple your point total if you also provide your friends' first names, last names, and ages. You decide to provide just your friends' emails, since that's what you did, and nothing bad seems to have happened. Sure enough, your online point total doubles the next day, and you're in the lead for a gift card.

1. Have you broken the code of computer ethics? Why, or why not?

2. Which principle(s) of computer ethics could be relevant to this situation?

3. What are the possible outcomes of your action? Try to imagine at least three different sets of results, ranging from positive to negative.

ACTIVITY 1: Cyberethics continued

Scenario #2

Your school is in an uproar. A student has hacked into the school's grading system and erased the results of an important math test everyone in your grade just took. The test results are a big part of final grades and thus have an impact on college application packages. The principal is threatening to give everyone a failing grade on the test if nobody comes forward with information about who did it. If the school finds the culprit, then that student will be expelled for the rest of the school year and must start the same grade over in the fall. Everyone else will have to take the test again.

One day at lunch, you overhear some other students in your computer class talking about who they think did it; shockingly, it's you and your lab partner. You know you didn't do it, but you're not sure about your lab partner. Your lab partner has been acing the class, could definitely have hacked the school's computer system, and he is kind of a troublemaker. You make up a fake email account for yourself and leave an anonymous message for the principal, describing your suspicions and how you came by them.

1. Have you broken the code of computer ethics? Why, or why not?

2. Which principle(s) of computer ethics could be relevant to this situation?

3. What are the possible outcomes of your action? Try to imagine at least three different sets of results, ranging from positive to negative.

ACTIVITY 1: Cyberethics continued

Scenario #3

Your friend's sister works at a software company. Like you and your friend, she and her colleagues can't wait for the release of "Captain FearFace 4," the latest movie in a series that has earned over $1 billion worldwide. One day, your friend brings over the exciting news that the sister has figured out how to see the movie before it's released! You have to use a peer-to-peer file sharing app, go to an un-searchable website she found out about at work, and then download the movie to watch on a computer. Your friend's sister says it's okay, since her company got the information from someone at the studio itself. But it must be now, since the file will be available for just one day. Your friend says you have to do it on your computer, since your friend's is too slow to complete the download in time. And besides, it's not like the movie isn't going to make millions of dollars when it comes out for real. You go ahead and load the file-sharing app, download the movie, and watch it that evening. As you lie in bed that night, you do wonder what you might find on your hard drive the next time you boot up your computer.

1. Have you broken the code of computer ethics? Why, or why not?

2. Which principle(s) of computer ethics could be relevant to this situation?

3. What are the possible outcomes of your action? Try to imagine at least three different sets of results, ranging from positive to negative.

PERSONALLY IDENTIFIABLE INFORMATION

Cyber attacks of most concern to individuals are those that target personally identifiable information, or PII. This is the online asset that all users have and all cybercriminals want. Keeping it safe allows us to go where we want to go online and do what we want to do, just as a bicycle helps us move around town on our desired rounds. And just as bicycle owners put behaviors and protective devices to work keeping their property safe and accessible only to them, internet users have many ways to do the same with their sensitive data. Not only is learning how to stay safe online in our personal lives a fundamental requirement in this internet age, it is also a good way to start building the skills and knowledge that could lead to a career in cybersecurity.

Here's a generally safe assumption: **everything you do online, any information you post, could be made public or visible to someone else**. With any luck, not in a way that harms you. But it's always a possibility. For this reason, it's important to take steps to make sure you keep important personal information protected or offline altogether, and practice sound safety with anything you do put online.

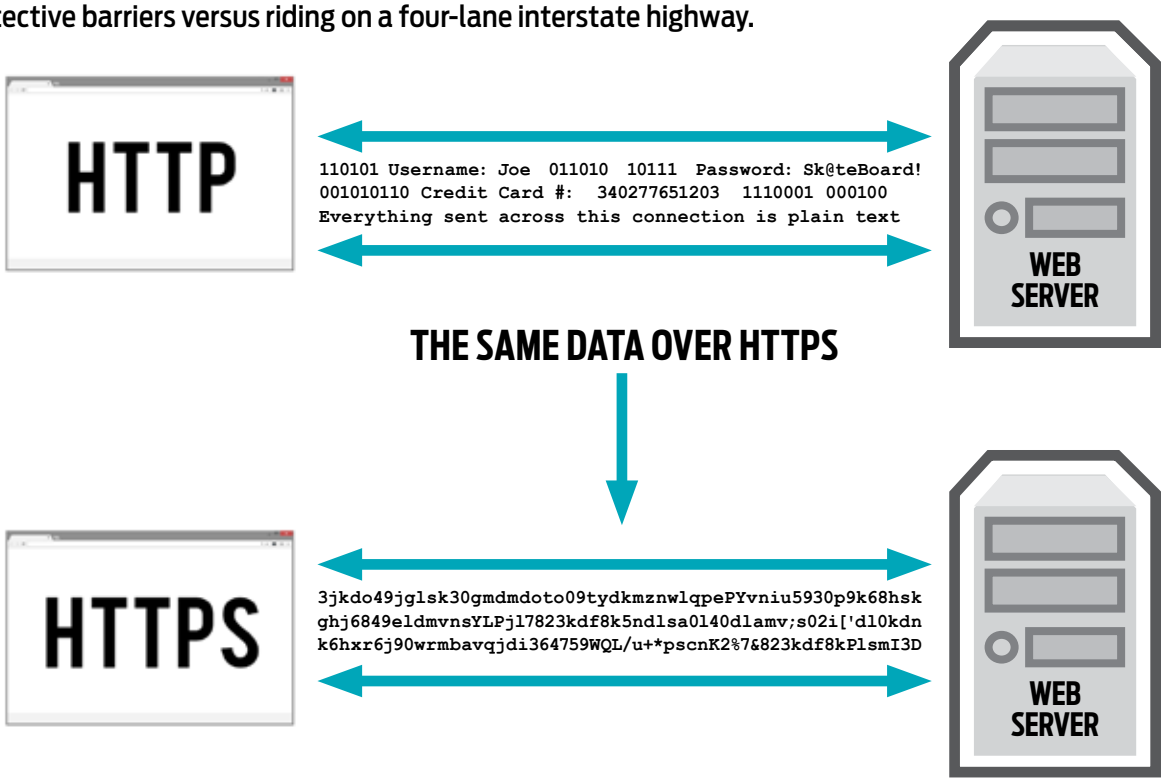
You should treat personally identifiable information, or PII, with extreme care online. PII includes things like your:

- **Social Security Number**
- **student identification data**
- **passwords**
- **financial account information**
- **address information**
- **any other data that could allow people to connect your online activities to you and things you value in the physical world**

SMART CONNECTING

Research shows that 95 percent of cybersecurity breaches start with users falling for a phishing attack, downloading an infected attachment, clicking a dangerous URL or doing something else to allow hackers into a data network. Any time you encounter a website asking for information, PII or otherwise, make sure it's secure and legitimate. The URL should be accurate, show an "s" after the "http," and feature a small padlock image in the address bar.

HTTPS keeps your data secret by encrypting it as it moves between your browser and the website's server. This level of security makes the information going between you and the website inaccessible to anyone trying to spy on the exchange, such as your ISP, a hacker, snooping governments, or anyone else. It's like the difference between riding in a bike lane marked off with protective barriers versus riding on a four-lane interstate highway.



BUILT-IN SAFETY FEATURES

It's also worth using the built-in safety features of whatever internet browser you're using, such as pop-up blockers, anti-virus and -spyware tools, and other similar options. Social media and shopping sites present the most risk for PII or other revealing information to spread. Use them, by all means, but with caution and awareness. It's safe to assume that everything you post about yourself is permanent, visible to future schools, employers, acquaintances, and anyone else interested in your personal life.

ONLINE SAFETY 101

1. **Change your password regularly.** Don't re-use old passwords or use the same passwords for multiple accounts. Figure out a system to remember your passwords. Write them down and hide the list. Use a password manager.

2. U**se strong passwords.** Use passphrases or abbreviations and avoid words found in the dictionary. Use random special characters and numbers to avoid being the victim of a brute force attack. Passphrases should be at least 8 characters long. Don't share passwords; if you wouldn't give the person the key to your most valuable possessions, don't give them your passwords.

3. **Use two/multi-factor authentication, if available.** This adds another layer of protection. It may take slightly more time but is becoming more and more common to avoid compromise.

4. **Beware of phishing attempts.** If an offer seems too good to be true, it is. Be a skeptic. Don't give personal information out over the phone without verifying identity of the caller. Do not click or open emails that appear suspicious. Slow down!

5. **Cover up your webcam and practice basic safety.** Close or at least lock your device when you leave it. Never leave a device alone in public and avoid unknown devices such as random thumb drives or other plug-ins.

6. **Be aware of location settings on your device.** Turn off location settings and bluetooth when not in use. Do not allow apps access to data if they do not need access to function. Turn off location settings on your camera. Do not post while on vacation. In general, do not overshare on social media.

7. **Run antivirus software.** Be sure to use valid software and keep it updated.

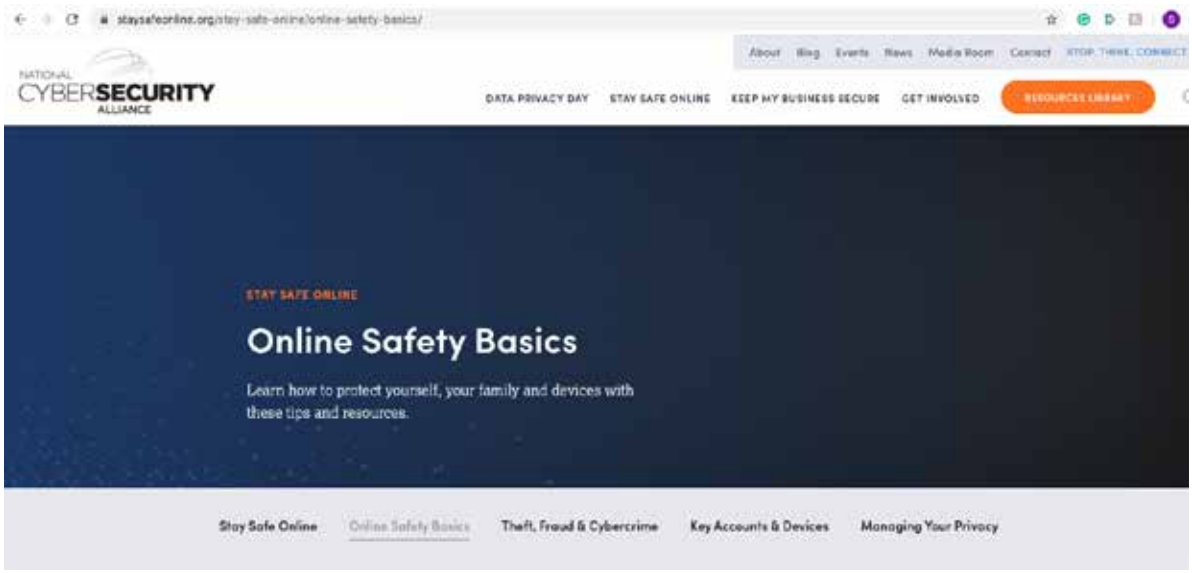
8. **Avoid public WiFi.** At the very least run a good VPN to add another layer of protection. Be conscious of the websites you visit while on public WiFi. Be especially careful in areas of high traffic (coffee shops, airports, hotels, etc.).

9. **Back up your data.** Then back it up again. Use an external hard drive, even if you use cloud storage.

10. **Update/patch your devices.** Yes, it might be annoying. However, it's necessary. Run the updates. If you question the validity of the update, be sure to run it straight from the source.

ACTIVITY 2: Staying Safer Online

StaySafeOnline.org is a reliable source of guidance for best online safety practices. Go to the website and pick a topic from the Online Safety Basics section under the Stay Safe Online tab. The options are: **Spam and Phishing**; **Online Shopping**; **Back it Up**; and **Malware, Botnets, and Ransomware**. Study the topic you've chosen — if you're in a group, discuss your topic with other group members — and boil down your thoughts into a set of recommendations to share with others in a presentation, using the title "Five Tips for [your topic]."



PASSWORDS

Passwords do enormous work online to keep our information and activities visible only to those who should be able to see them. Well-built passwords, carefully kept only to yourself, will protect your personal information in almost every case. To build and manage passwords effectively, it will help to have a fuller grasp of what they are and how they work.

A password is the primary tool for people to authenticate their identity in an online data environment. In effect, a password proves that "you are you" to a computer. You present yourself to a computer with a user identification, in many cases an email or online tag that is made visible to other users of the system. The password, though, is meant to remain secret and hidden, and online systems use advanced, mathematically complex tools to "hash" or encrypt passwords and keep them out of sight inside the system. Outside the system, it's up to you to keep your passwords out of sight.

Once your identity is authenticated, you are authorized to access, change, review, or otherwise manipulate data inside the system, according to the privileges attached to your user account. In most cases, these privileges extend just to PII, but depending on a user's status or needs, privileges might be wider.

In theory, then, online security should be as simple as having a strong password known only to a single user and recorded in sufficiently encrypted form to prevent malicious hackers from bringing it to light, even if they do gain access to an online database of passwords.

However, most people let down their guard in building and managing passwords. They use the same, weak password(s) for multiple accounts, share or reveal passwords among friends, family members, or co-workers, fall prey to malicious hackers' tricks to acquire passwords, or do some combination of all these things. In events such as these, a password breach is the result of the password owner's poor choices.

In other events, cybercriminals hack into other people's accounts by cracking their passwords. Malicious hackers have powerful tools to decipher passwords, once they home in on a user account that is accessible online.

Check it out:

- Passwords composed of eight letters can be cracked in about **five seconds**.
- Add numbers to that password, it can be cracked in about **a minute**.

If you, as most people do, use your email address as user identification, a hacker could rifle through your online assets in a very short period of time, indeed.

The lesson:

Build strong passwords, keep them private, and be wary of any requests people make for your login information, even if they come from apparently familiar sources.

STRONG PASSWORDS

A strong password system should use complex constructions — involving numbers, lower- and upper-case letters, and symbols — be unique to each account you have online, and always and entirely be known only to you. It's also useful to keep a hard-copy directory of passwords (in a safe place!) or a list of passwords encrypted on a secure device.

The 25 most common passwords make up about 10 percent of all passwords in use. Common passwords include these below and similarly constructed variations:

- 123456
- password
- qwerty
- admin
- abc123
- letmein
- iloveyou
- football
- welcome

YOU CAN BUILD STRONG PASSWORDS IN VARIOUS WAYS:

- **Make them long and impersonal, with different types of characters.**

  Longer passwords are better, especially to protect sensitive data to do with money or health. Mix up different kinds of characters, including upper- and lower-case letters, numbers, and special symbols.

  Use words, numbers, or letter combinations with no personal connection – hackers often mine publicly available pieces of information to try and guess passwords.

- **Devise a method or formula for building passwords that are both unique and memorable.**

  Choose a personally meaningful phrase, a book title, a song lyric – anything you'll easily remember – and then contort it in some non-intuitive form: "We went to Disney when I was 12" then becomes wW2dwEYEwas12.

- **Start with a combination of repeated, meaningful characters you can remember as a base and then add unique characters that correspond to the particular website.**

  For example, nFl41pHi33 would work as a base for a fan of the Philadelphia Eagles, who won the NFL's Super Bowl by a score of 41-33. For an account at the Bank of America, adding Boa! to this base would yield a very strong password of: nFl41pHi33Boa!

Avoid writing down passwords, or if you do write them down, record them in an encrypted file labeled something other than "passwords." You could also write down hints instead of the passwords themselves. Alternatively, a password manager can help keep track of all the different passwords you develop. Be sure to use a strong "master" password to unlock access to those stored in the management system. A quick internet search on "password manager" will lead you to several examples of the tool as well as reviews that can help you identify the one that works best for you.

ACTIVITY 3: Building Passwords

In this exercise, you will build several passwords of different lengths, estimate how long it would take to crack them, and then test them online to find out how long it would actually take to crack them.

Fill out the table below with 3 sets of 3 passwords each, running 6, 9, and 12 characters.

For the first password in each set, use only **letters.**
For the second, use **letters and numbers.**
For the third, use **letters, numbers, and special character**s.

For each password, guess how long it would take a hacker to crack it.

PASSWORD	ESTIMATED CRACKING TIME	ACTUAL CRACKING TIME
_ _ _ _ _ _		
_ _ _ _ _ _		
_ _ _ _ _ _		
_ _ _ _ _ _ _ _ _		
_ _ _ _ _ _ _ _ _		
_ _ _ _ _ _ _ _ _		
_ _ _ _ _ _ _ _ _ _ _ _		
_ _ _ _ _ _ _ _ _ _ _ _		
_ _ _ _ _ _ _ _ _ _ _ _		

ACTIVITY 3: Building Passwords (continued)

Once you've built your passwords and estimated cracking time, go to this website: **https://www.security.org/how-secure-is-my-password/.**

Enter all 9 of your passwords in the box and record the results for how long it would actually take to crack them.

1. How different were your estimates from actual times?

2. Which estimate of yours was closest to the actual time?

3. Which was farthest away?

4. Does this exercise change the way you think about the passwords you are using in your own online life? In what ways?

ACTIVITY 4: A Personal Password Management System

With the lessons of this chapter in mind, you should be able to develop your own personal password management system.

Keep in mind that a strong password is

- **Hard to crack.**
- **Used just once.**
- **Possible to remember without being written down.**

1. What type of password-building approach would work best for you?

2. For each of the approaches described above, what do you think are some advantages and disadvantages to each?

3. Now develop a system that will work for you. But DON'T write it down here; remember, your system is for you and you alone to know.

ACTIVITY 5: Password Cracking Challenge

Read the paragraph below describing the private life of an imaginary character. Then follow the directions below with a partner to create and then try to crack possible online passwords this character might use.

Andy Davis has a problem. He's about to leave his childhood home at 234 Elm St. and go off to college at UCLA. He knows he'll still be able to play his favorite sports – baseball and soccer – but he can't decide which of his old, favorite toys to bring with him. How to choose among Buzz, Woody, Jessie, Bullseye, Slinky Dog, and the rest? A young girl named Bonnie has recently moved into the neighborhood, and she seems lonely. Andy decides to leave his toys with Bonnie. He brings them over to her house in a box, along with a note that says, "Enjoy these toys. They brought me a lot of happiness. So long, partner! Andy. P.S. Call me if you ever want to talk, my number is 203-555-0112."

Directions:

In college, Andy will have to create several passwords to manage all the new accounts he will be using as a student. He knows he should use a unique password for each of these new accounts, but he is not very good at building them. Your job is to help Andy learn what makes a weak versus a strong password. With a partner or in a group, **use the information from Andy's story to take turns building passwords you think would range in strength from weak to medium to strong**. Then your partner or group will try to guess the passwords, based on information included in the story. Keep track of how many attempts it takes to guess passwords, or at least get close to them. When you've got some strong passwords at hand for Andy to use, give him a call to let him know!

CONCLUSION

By now, you should understand some of the many ways you can act to keep yourself safer online. From considering the ethical implications of choices you make about using computers to building and using strong passwords, individuals can do much to reduce exposure to the consequences of cybercrime.

Now it's time to think about cybersecurity as an option for further education and possible work. If you have found yourself interested in the topics of these first two chapters, you should know they form the basis of work that many people do in cybersecurity. In the next chapter, you will learn more about careers in the field and begin to discover if a future in cybersecurity might be right for you.

CHAPTER THREE

How Do I Know if I Like or Can Do Cybersecurity?

"Cybersecurity requires 'insatiable' problem-solving skills; technical skills can be taught."

That was a headline in *The Wall Street Journal*, describing the views of high-level cybersecurity executives at a May 2018 forum on the cybersecurity workforce. As one of the participants said, "Cognitive diversity is more important than anything for a cybersecurity person." That means creativity, a willingness to learn, an ability to incorporate new information and conflicting views into innovative solutions. Cybersecurity professionals succeed by finding patterns, making connections, and collaborating widely. They can understand both the task they

are focused on and the larger system it is part of. In both speech and writing, they can translate complex technical issues into terms that help people stay safe online and practice proper data security practices. People who are good at these kinds of things excel in deductive reasoning, critical and flexible thinking, and solving complex problems.

To help you explore your own abilities along these lines, we've gathered some activities that might help you understand if you have some of the basic cognitive skills that can lead to success in cybersecurity. The exercises are basic and accessible, involving numbers, words, and logic challenges. They take creativity and imagination, plus logic and reasoning. If they're fun for you, and you can make your way to some of the answers, you might have the makings of a future cybersecurity professional.

ACTIVITY 1: Numbers, Numbers, Numbers

To solve these problems, you'll have to look at and think about numbers in imaginative, unfamiliar ways. Sometimes numbers might not be what they seem, and sometimes the answer might be "hidden" in plain sight.

A. What is the answer to the last equation?

12 x 21 = 9

13 x 31 = 16

14 x 41 = ?

Hint: Sometimes a number shows up whole, sometimes it shows up in parts.

B. What is the next number in this sequence?

3, 6, 10, 15, 21, _____

Hint: Remember, it's the differences among us that make life interesting.

C. What is the next number in this sequence?

2, 12, 1112, 3112, 132112, _____

Hint: Each successive number will point you back to the number just before it, if you can read it in the singular way required and take one thing at a time.

D. A credit card has 16 numbers on it. Look for a pattern to figure out the last two digits on a card with these numbers:

1248 1632 6412 82 ____ ____

Hint: Numbers don't always belong together, even if they're right next to each other.

In the next exercises, use addition, subtraction, multiplication, and division to construct the given number out of the others presented. Use each operation and each number only once. For example, making 6 out of 3, 2, and 1 could be (3 x 2) / 1 = 6.

E. Make 43 out of 2, 5, 7, and 8 _____

F. Make 4 out of 1, 1, 6, and 7 _____

G. Make 80 out of 1, 3, 6, and 9 _____

H. Make 32 out of 4, 7, 7, and 9 _____

In the next exercises, use the equations and the grid to identify the numbers represented by letters. All letters correspond to a unique whole number up to the number of squares in a row.

I.

	1	2	3	4	5
A					
B					
C					
D					
E					

B + A = 6

E + B = C

E + C + B = 8

J.

	1	2	3	4	5
A					
B					
C					
D					
E					

D – 2 = C

E + C = D

A + E = C

K.

	1	2	3	4	5
A					
B					
C					
D					
E					

A + D = 6

DA = E + A

A + C = B

ACTIVITY 2: Words, Words, Words

A. Find the four-letter word that overlaps the end of one word and the beginning of the next word. The order of letters may not be changed.

The pirate ship sank, and all the survivors fled overland before regrouping. _____

Frozen icecaps are often found north of Canada. _____

Each year my school tests the alarm system to make sure it works. _____

Kevin ended the conversation right away. _____

Their biggest problem was the neighbors playing loud music. _____

B. Find pairs of rhyming words that match the definitions appearing below:

Paperback thief: _____ _____

Lengthy tune: _____ _____

Formal dance with very few people: _____ _____

Buzzing insect at the top of a tree: _____ _____

Wind that you feel only below the waist: _____ _____

C. What word is pronounced differently when the first letter is capitalized?

_____

D. Punctuate the following so that it makes sense, and rewrite it below.

That that is is that that is not is not is not that it it is.

_____

ACTIVITY 3: Reasoning

These puzzles can all be figured out using just the information presented. Using logic and attention to detail, can you solve them?

A. Your parents have six daughters, including you. Each daughter has one brother. How many people are in your family?

_____

B. If 3 cats can catch 3 mice in 3 minutes, how long will it take 30 cats to catch 30 mice?

_____

C. Rearrange the letters of NEW DOOR to make one word out of them.

_____

D. A farmer had nine sheep, and all but seven died. How many did he have left?

_____

E. If a doctor gave you three pills and told you to take one every half hour, how long would they last?

_____

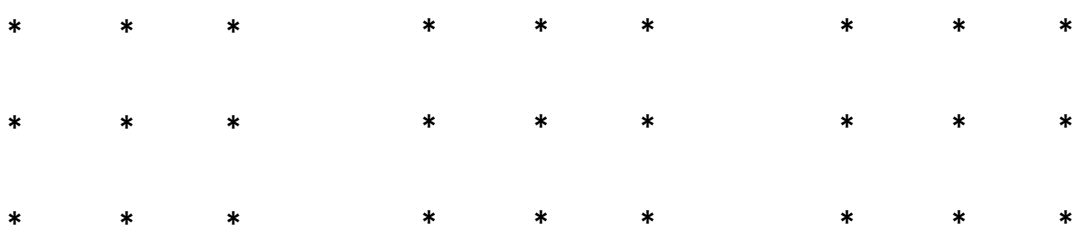
F. You are standing in front of three boxes of fruit, labeled “apples,” “oranges,” and “apples and oranges.” The boxes do contain these fruits divided up in this way, but all the labels are on the wrong boxes. To label the boxes correctly, you need to pick only one piece of fruit from one box. Which box do you pick the fruit from? And how do you label the boxes correctly?

G. A man is the owner of a winery who recently passed away. In his will, he left 21 barrels (seven of which are filled with wine, seven of which are half full, and seven of which are empty) to his three sons. However, the wine and barrels must be split so that each son has the same number of full barrels, the same number of half-full barrels, and the same number of empty barrels. Note that there are no measuring devices handy. How can the barrels and wine be evenly divided?

H. At a family reunion were the following people: one grandfather, one grandmother, two fathers, two mothers, four children, three grandchildren, one brother, two sisters, two sons, two daughters, one father-in-law, one mother-in-law, and one daughter-in-law. But not as many people attended as it sounds. How many were there, and who were they?

I. You have two slow-burning fuses, each of which will burn up in exactly one hour. They are not necessarily of the same length and width as each other, nor even necessarily of uniform width, so you can't measure a half hour by noting when one fuse is half burned. Using these two fuses, how can you measure 45 minutes?

J. Nine dots are arranged in a three-by-three square. Connect each of the nine dots using only four straight lines and without lifting your pen from the paper. (We gave you 3 tries.)



ACTIVITY 4: Algorithms

What is an algorithm? It's a complicated-sounding word, but think of it simply as **a series of steps to accomplish a task**. You perform algorithms everyday while washing your hands, making your lunch, or getting to school. In computer language, an algorithm is a series of steps for a computer program to accomplish a task. For example, how does Google Maps figure out how to get to a particular location? They use a route-finding algorithm that computer scientists wrote. This algorithm is more complicated than the one you use to wash your hands, obviously, but it's still a series of steps. So what makes a good algorithm? It should both solve the problem and do so efficiently.

Now it's your turn. Write down the steps below for a seemingly simple task, like washing your hands or tying your shoes. You may be suprised how many steps it takes!

TASK: _____

STEP 1 _____

STEP 2 _____

STEP 3 _____

STEP 4 _____

STEP 5 _____

STEP 6 _____

STEP 7 _____

STEP 8 _____

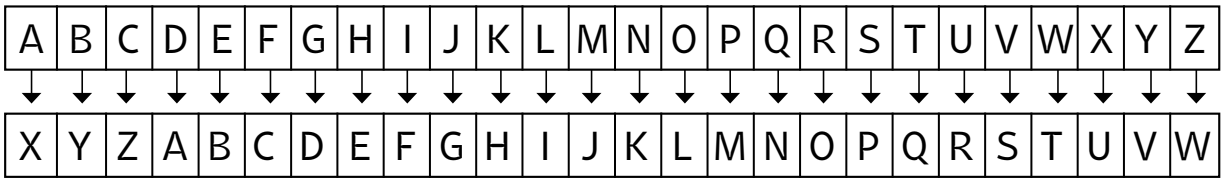
STEP 9 _____

ACTIVITY 5: Cryptography — Caesar Cipher

A mastery of cryptography enables people to send all kinds of information from one party to another without being comprehensible to anyone in between. The actual practice of cryptography has developed in mind-bendingly complicated directions, thanks to the combination of advanced mathematics and high-powered computers. Even so, the principles are simple, and people have employed cryptographic systems for thousands of years.

A cipher is like a code, a secret or disguised way of writing. To encrypt a message—and to decode it—requires following a set of well-defined steps. Another way of saying this is to say that a cipher is an algorithm for performing encryption or decryption. (You may have heard the word algorithm associated with online coding and it works in a similar way. See previous page for more.)

In cryptography, a Caesar cipher, also known as the shift cipher, is one of the simplest and most widely known encryption techniques. (The method is named after Julius Caesar, who used it in his private correspondence.) It is a type of substitution cipher in which each letter in the text is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on as shown below:



Use the cipher key to decode this phrase, then write your own message.

MXOQV XQ KXQBP ELRPB QLKFDEQ XQ BFDEQ

WRITE YOUR MESSAGE HERE (with translation):

What do you think would be the drawbacks of this kind of cipher?

ACTIVITY 6: Cryptography — Keyword Cipher

The Keyword cipher is identical to the Caesar cipher with the exception that the coded alphabet is shifted by using a keyword. To create a substitution alphabet from a keyword, you first write down the alphabet. Below this you write down the keyword (omitting duplicate letters if the word contains two or more of any letter) followed by the remaining unused letters of the alphabet.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
K	E	Y	W	O	R	D	A	B	C	F	G	H	I	J	L	M	N	P	Q	S	T	U	V	X	Z

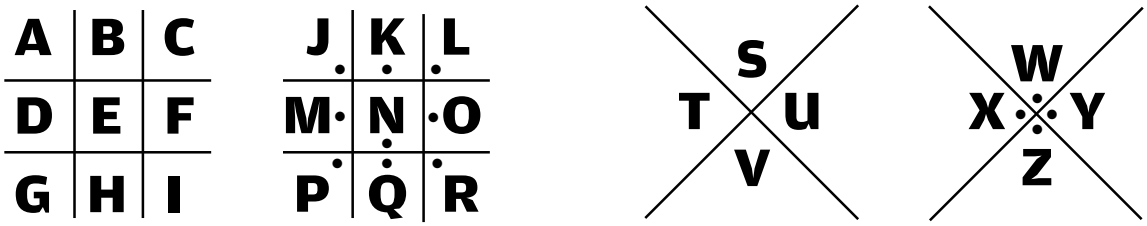
Create your own keyword cipher using the grid below and then write a secret message to a friend!

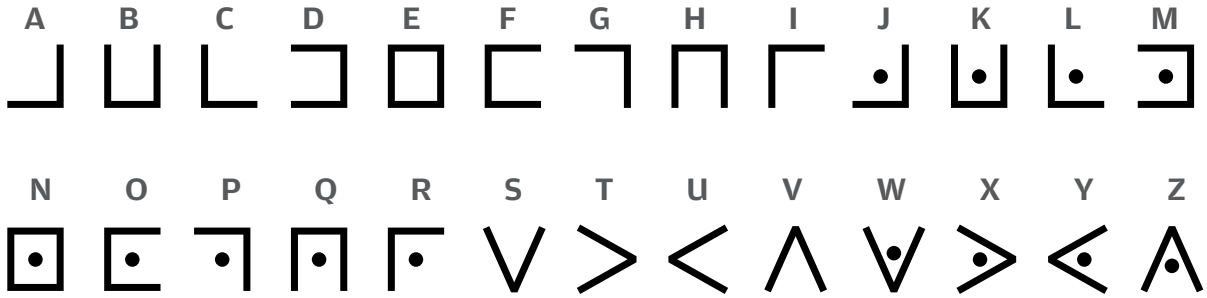
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓

How would a keyword cipher be more secure than a Caesar cipher? How would it be less secure?

ACTIVITY 7: Cryptography — Pigpen Cipher

The Pigpen cipher (also referred to as the masonic cipher, Napoleon cipher, and tic-tac-toe cipher) does not substitute one letter for another; rather it substitutes each letter for a symbol. The alphabet is written in the grids shown, and then each letter is enciphered by replacing it with a symbol that corresponds to the portion of the pigpen grid that contains the letter.





Decode the following message using the pigpen cipher:

Now write your own secret messages!

ACTIVITY 8: Cryptography — Crack the Binary Code

All letters of the alphabet, numbers, and symbols are converted to 8-character binary numbers as you work with them in software on your computer. The code is made up exclusively with ones and zeros. For example, the letter A is represented by the eight character binary number 01000001. Computers transport, calculate, and translate binary numbers because computer hardware circuits only have two electrical states, on or off. Zero is off, one is on. Use the binary code table below to translate the answers to the following riddles. Notice a pattern in the table? See if you can fill in the last blanks.

1. What 7-letter word is spelled the same way backwards and forwards?

_____ _____ _____ _____ _____ _____ _____

01010010 01000001 01000011 01000101 01000011 01000001 01010010

2. What travels around the world but stays in one spot?

_____ _____ _____ _____ _____

01010011 01010100 01000001 01001101 01010000

3. I have cities, but no houses. I have mountains but no trees. I have water, but no fish. What am I?

_____ _____ _____

01001101 01000001 01010000

4. What word does the following? The first two letters signify a man, the first three letters signify a female, the first four letters signify a great person, while the entire word signifies a great woman. What is the word?

_____ _____ _____ _____ _____ _____ _____

01001000 01000101 01010010 01001111 01001001 01001110 01000101

5. What gets wet while drying?

_____ _____ _____ _____ _____

01010100 01001111 01010111 01000101 01001100

6. The more you take, the more you leave behind. What am I?

_____ _____ _____ _____ _____ _____ _____ _____ _____

01000110 01001111 01001111 01010100 01010011 01010100 01000101 01010000 01010011

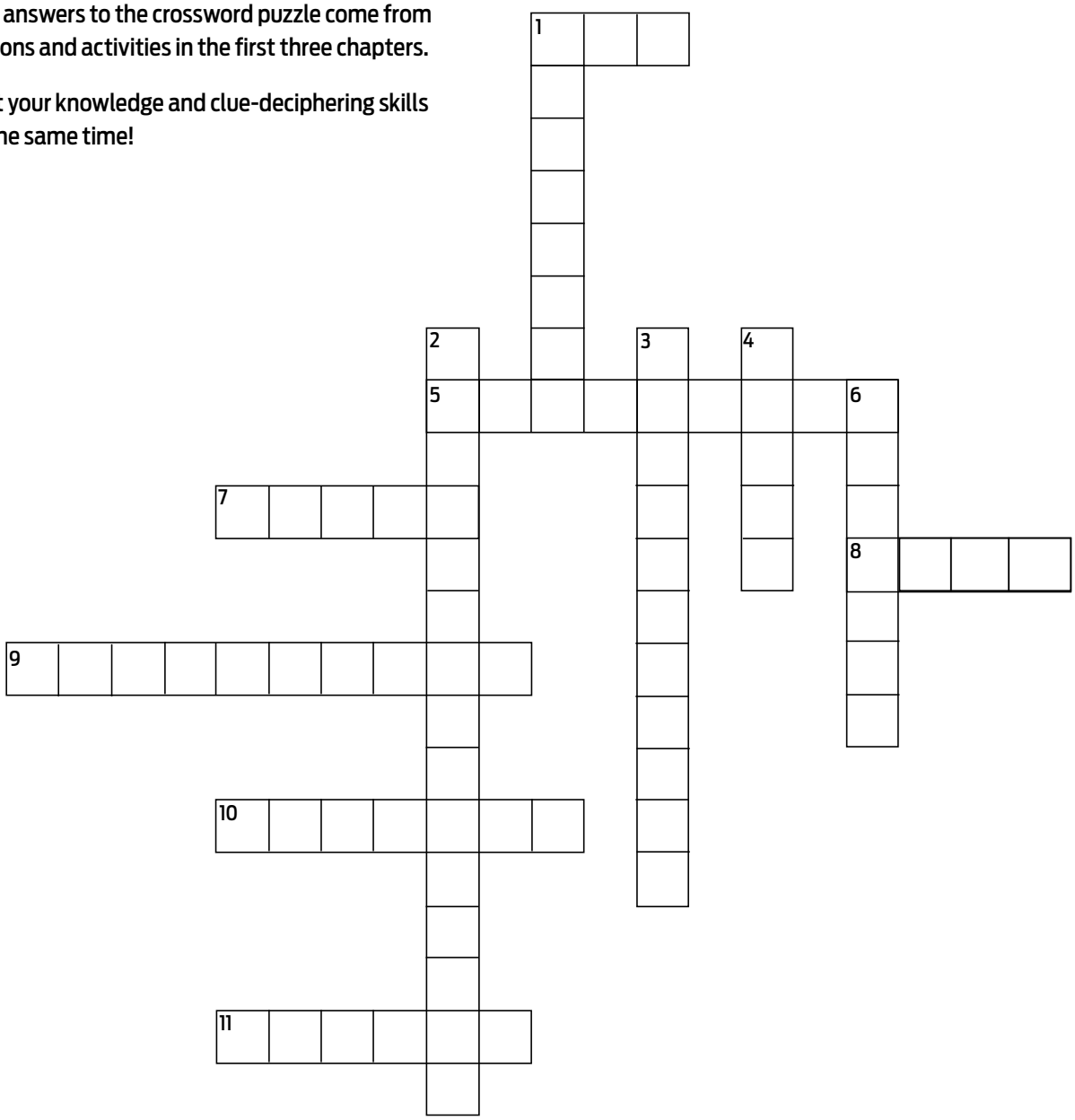
BINARY TABLE

A	01000001
B	01000010
C	01000011
D	01000100
E	01000101
F	01000110
G	01000111
H	01001000
I	01001001
J	01001010
K	01001011
L	01001100
M	01001101
N	01001110
O	01001111
P	01010000
Q	01010001
R	01010010
S	01010011
T	01010100
U	01010101
V	01010110
W	01010111
X	
Y	
Z	

ACTIVITY 9: Crossword Puzzle — Vocabulary Review

The answers to the crossword puzzle come from lessons and activities in the first three chapters.

Test your knowledge and clue-deciphering skills at the same time!



ACROSS

1. Valuable data troves of individuals, abbreviated.
5. Linear sequence of steps, to go from A to B to ...
7. Makes a computer "sick".
8. Makes a computer "sick," then another, then another.
9. A tool of extortion, it takes data hostage and locks it up.
10. Secret resident of a hard drive that watches your every move.
11. Actually makes sense, once you know how to read it.

DOWN

1. Tries to "hook" you into trouble.
2. Something to lean on for help with access to online accounts.
3. Could be bearing "gifts" you don't want to live with.
4. Says, "Feel safe, all ye who enter here."
6. Poison software pills that let the bad people into your data.

CONCLUSION

What did you think of these exercises? Were they fun? Or boring? Easy or hard? Did they engage you in ways you like to think or learn?

In the next chapter, you'll analyze some examples of real-world cybercrimes. And you'll learn about how the field of cybersecurity is shaped.

As you continue your cybersecurity learning journey, pay close attention to how problems and topics strike you. The ones that stick in your head are worth exploring further, since they could serve to point you in the direction of further study and work in the field.

CHAPTER FOUR

How Do I Figure Out if a Career in Cybersecurity Could Be Right for Me?

Cyber attacks can hit anyone, anywhere, at any time. Individuals, companies, governments, schools, and more – any person or group with an online presence is vulnerable, and everyone should be careful about protecting themselves and their data. That means cybersecurity professionals are needed everywhere.

When cyber criminals steal stashes of PII or phish their way into protected networks, cybersecurity professionals get in gear. They work to identify and close down breaches in compromised systems. They conduct forensic investigations to track down digital intruders. And they study attacks in the present to learn how to build stronger defenses in the future.

Cybersecurity is one of the fastest-growing, most important fields of study and work in America. And it could be the right field for you.

ACTIVITY 1: Cybersecurity in Action

If you have a copy of the **Start Engineering Cybersecurity Career Guide**, go to the front section of the book called "Cybersecurity is ...," on pages 4-11, to answer the questions below. If you don't have a copy of the book, go to the **same material on our website**, or search "cyber attack" online.

Pick out 3 scenarios from this front section of the book or from your internet search and name them below. Answer the following questions as part of an exercise to become familiar with what real-world cyber attacks look like.

SCENARIO A: _____

SCENARIO B: _____

SCENARIO C: _____

1. Who do you think is carrying out the cyber attack being described? A government? Individuals? Groups of criminals? Military? Companies? A combination of actors? Who else?

A. _____

B. _____

C. _____

2. Who or what is the target of the attack?

A. _____

B. _____

C. _____

3. What was the goal of the attacker(s)? What are they trying to accomplish?

A. _____

B. _____

C. _____

ACTIVITY 1: Cybersecurity in Action continued

4. Why did the attacker(s) pick that particular target?

A. _____

B. _____

C. _____

5. What is the worst-case result of the attack, if completely successful?

A. _____

B. _____

C. _____

6. What kinds of prevention measures can you imagine? Think about what behaviors people can change, technologies that might be useful, laws that might be made, and other possible responses.

A. _____

B. _____

C. _____

7. What kind of response would be required to recover from the attack? Money? New behaviors? New technologies? What else?

A. _____

B. _____

C. _____

ACTIVITY 1: Cybersecurity in Action continued

8. Rank the attacks in order of seriousness or threat. Think about how many people are affected, what damage might result and to whom, what kinds of effort and money it might take to recover from the attack, and other possible criteria for assessing the threat level.

9. Pick out one attack scenario and imagine you are the leader of the country, company, or group under attack. You need to make a speech to your followers, explaining the attack, how and why it happened, what the damage has been, and how you're going to prevent attacks from happening in the future. What will you say to your audience? Make an outline or set of bullet points addressing these questions and for use in your speech.

ACTIVITY 1: Cybersecurity in Action continued

10. For each scenario, do some research online to determine if there have been more recent cyber attacks in that field, either in the United States or overseas. In each case, what happened?

WORKING IN CYBERSECURITY

Now that you've delved into the details of specific cyber attacks, let's take a step back and consider more generally what professionals in the field of cybersecurity actually do.

THE "CYBER DOMAIN"

Cybersecurity professionals work in the "cyber domain," meaning the actual and virtual space in which cybersecurity-related activities occur, both for bad and good. That means everything from online network break-ins to phishing and social engineering scams to network administration, digital forensics, and legal, political, and educational measures.

The United States Army defines the cyber domain as a system composed of **three** interrelated layers: the **physical layer**, the **logical layer**, and the **social layer.**

1. The **physical layer** consists of the hardware and infrastructure that comprise networks as well as the actual building sites where hardware is located.

2. The **logical layer i**ncludes all the programmable devices that can connect to a computer network, as well as the programming itself that is required to make these connections work.

3. The **social layer** means the human factors, both the virtual and actual selves that people bring to their online actions and exchanges.

Cybersecurity professionals fill jobs that involve roles and responsibilities in some or all of these layers. Different skills and aptitudes equip people to succeed in different kinds of jobs across all three layers. Knowledge of technical, computer, and engineering topics is the starting point for work in the physical layer, while programming and system design skills make for success in the logical layer. These two layers are, of course, closely connected. Hardware and software mesh in countless, complex ways to make up the systems we use for online activities. You can think of these layers, taken together, as the "territory" or "homeland" of the cyber domain. Large numbers of cybersecurity professionals work in many different capacities to make this territory as resistant to attack and as resilient in recovery as is possible.

In the social layer, cybersecurity professionals bring knowledge of fields like law, psychology, politics, business, or international relations, especially as related to how people live and work in the cyber "territory." You might think of these jobs as making up the "border" of the cyber domain. In some of these jobs, people work in organizational or governmental capacities, crafting legal or policy safeguards, studying and guiding people's online behaviors and habits, or developing and implementing cybersecurity procedures for individuals and organizations to follow. In other jobs, people work closer to the "front lines," monitoring systems, implementing defensive measures, analyzing threats, or investigating attacks and tracking down criminals.

Across all three layers, cybersecurity professionals need the underlying cognitive skills highlighted in chapter three: **problem-solving**, **imagination, teamwork**, and **communications**.

Cybersecurity is such a complex, multi-dimensional, fast-changing field that individuals can never keep up on their own; it takes teams, working across organizational boundaries, focused on a common goal and always alert to surprise, risk, and threat.

FINDING YOUR PLACE IN THE FIELD

To get a fix on finding your place in cybersecurity, you can learn more about particular functions or roles people fill in the field. The National Initiative for Cybersecurity Education (NICE) has developed a framework for cybersecurity careers that defines seven basic categories encompassing the different kinds of work people do. Delving into these functions and using them as a filter for your own interests and abilities can help identify the educational and career pathway into cybersecurity that would work best for you.

These seven categories are:

1. **Securely Provision:** Design and build secure IT systems.
2. **Operate and Maintain:** Administer systems and manage the data they house.
3. **Oversee and Govern:** Manage teams; develop elements of the legal, policy, and education environment.
4. **Protect and Defend:** Identify and understand threats, defend networks against attack.
5. **Analyze:** Gather information and translate into usable, accessible intelligence.
6. **Collect and Operate:** Gather information inside and outside systems; execute defensive countermeasures.
7. **Investigate:** Collect and analyze forensic and other data associated with events or crimes directed at IT systems.

These categories can overlap, depending on a person's individual skill set or an organization's structure and needs. Cybersecurity professionals often move in and out of jobs with responsibilities spread across two or more of these categories. The chances for learning and variety can be many, throughout the length of any career in the field.

ACTIVITY 2: Career Exploration

Based on the thumbnail descriptions of the seven NICE framework categories above, rank all seven in order of career preferences for you.

1. _____

2. _____

3. _____

4. _____

5. _____

6. _____

7. _____

Go to the **NICE framework page** (https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework) and read more deeply into the definitions of the seven categories.

For each category, note two or three things that appeal AND do not appeal to you about the work described.

Securely Provision

Pro's: _____

Con's: _____

Operate and Maintain

Pro's: _____

Con's: _____

ACTIVITY 2: Career Exploration continued

Oversee and Govern

Pro's: _____

Con's: _____

Protect and Defend

Pro's: _____

Con's: _____

Analyze

Pro's: _____

Con's: _____

Collect and Operate

Pro's: _____

Con's: _____

Investigate

Pro's: _____

Con's: _____

Now that you've explored career roles in some detail, go back and review your ranked order of career preferences. Would you change your original ranking in any way? In what ways, and why?

_____

_____

_____

_____

ACTIVITY 2: Career Exploration continued

CYBERSECURITY WORK ROLES

Look at the tab called "work roles," at https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework/workroles.

Now scroll down the pull-down menu and pick out three that seem interesting to you and **write them below, along with the category of the work role.** (Just ignore the Work Role ID.)

1._____

2._____

3._____

Is the category of each work role above one of your highly ranked career preferences?
Add a Y or N to each line.

For each of the Work Roles you've chosen, pick out 3-5 items from the Abilities/Knowledge/Skills/Tasks lists that seem interesting or appealing to you and write them below.

1._____

2._____

3._____

What classes or subjects do you think you would take in school to learn more about these items? Try to come up with 5-8 possible classes or subjects.

1._____ 5._____

2._____ 6._____

3._____ 7._____

4._____ 8._____

CONCLUSION

Congratulations! You now have a starting point for picking a college major and identifying a school that could fit your academic and professional interests. Your parents, your school's guidance counselor, and professionals in the field can help you home in even further on a plan for finding a college and a career path that work for you.

The exercises in this workbook have been designed to give you hands-on experience and practical knowledge about cybersecurity, both as a personal exercise as well as a potential career path. The next step is up to you. If you think cybersecurity might be work you want to explore, go back to our **Cybersecurity Career Guide** and read about the different kinds of training you can get, what schools offer programs, and the different kinds of jobs that might be available to you.