Updated 2nd Edition!

Start Engineering

CYBERSECURITY 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.

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 you 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

CHAPTER ONE

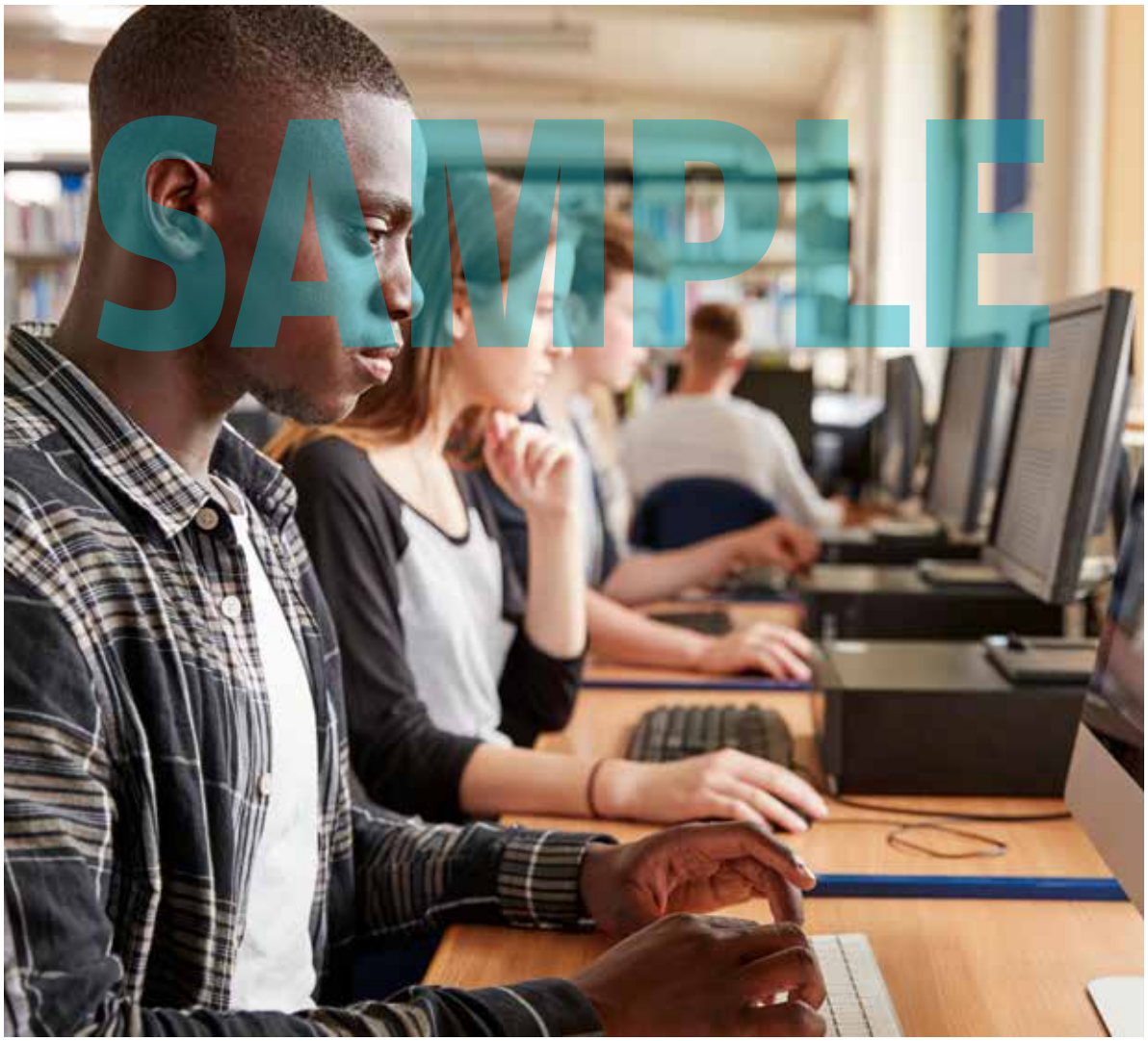
What Is Cybersecurity and Why Should I Care?

In late 2014, hackers stole almost 100,000 photos and videos delivered through Snapchat, teenagers' favorite app for exchanging messages. The blink-and-you-miss-it quality of Snapchat can tempt users to send images more revealing or private than they might otherwise be willing to share. But a third-party app was allowing people to save Snapchat messages permanently. Hackers broke into the app, stole the files, and posted personal, often explicit messages among a group of mostly European users, about half of whom were between 13 and 17 years old.

Still think the internet is safe? Even taking all the safeguards we can think of ourselves, we inevitably rely on other people's systems and behaviors to keep our sensitive materials from falling into the wrong hands. As the news keeps showing, though, these systems and behaviors can and do let us down.

SCHOOLS AT RISK

In the last few years, for example, hundreds of K-12 schools have suffered cyber attacks of one kind or another. The most common attacks involve malicious hackers penetrating storehouses of **personally identifiable information,** or PII, that schools collect about students. These attacks often lead to attempts to extort money from schools in exchange for keeping the data private. However, cyber criminals will also sell the data on black markets or do other bad things with it. Students' grades have been changed, websites have been brought down or damaged, and school operations have been disrupted. The threat to schools has grown so great that the FBI, the Internal Revenue Service, and the Department of Education have all issued recent alerts specifically calling out K-12 schools as vulnerable targets for cyber attacks.



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://www.mediapro.com/blog/free-quiz-phishing-resource/

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

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

https://www.consumer.ftc.gov/media/game-0011-phishing-scams

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 form 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?

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. Beyond viruses and worms are scores of other types of malware, including ransomware, spyware, and Trojan horses. Cyber criminals are constantly developing malware in ever-more devious, damaging forms.

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.

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 improperly sharing passwords to downloading and using software without payment or permission, cybersecurity breaches can vary enormously in scope and severity. But they reflect the failure of people to follow ethical principles meant to preserve the safety, reliability, and privacy of online networks.

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 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 have to 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?

PERSONALLY IDENTIFIABLE INFORMATION

Cyber attacks almost always 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.

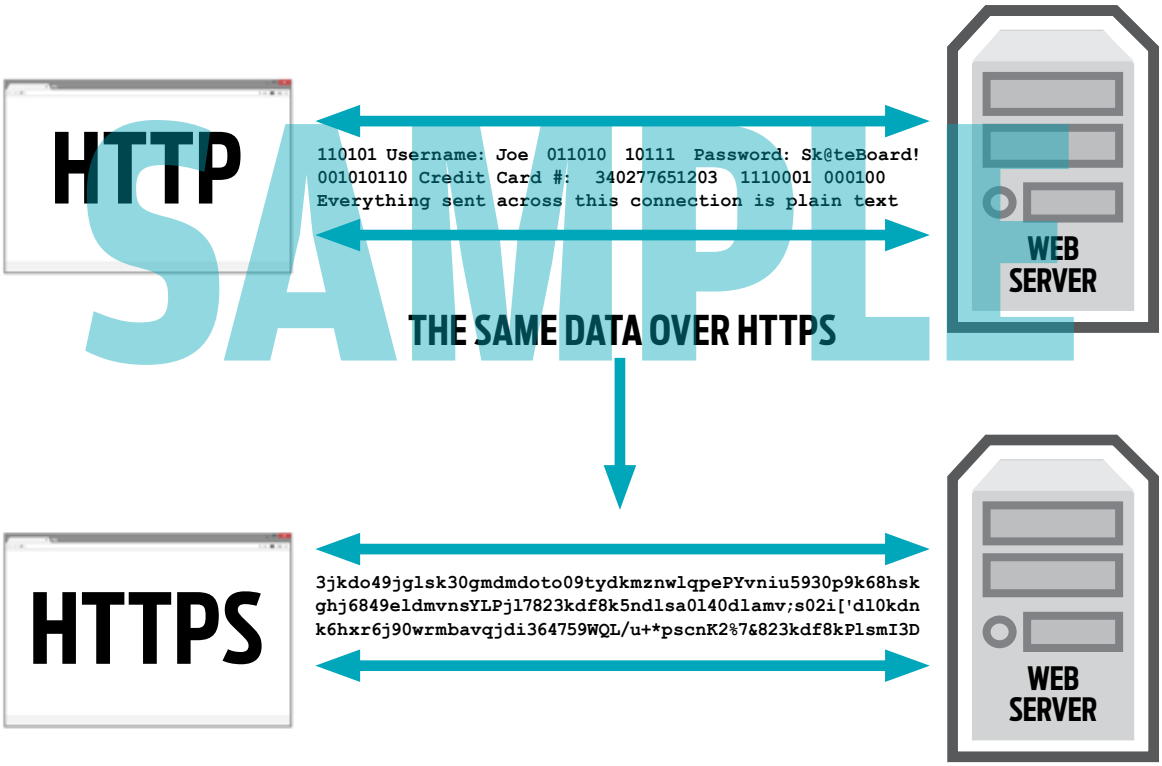
You should treat personally identifiable information, or PII, with extreme care online. PII includes things like your:

- **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 90 percent of cybersecurity breaches start with a user clicking a dangerous URL. 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 ensures that anyone listening in on the conversation can't read anything, such as your ISP, a hacker, snooping governments, or anyone else who manages to position themselves between you and the web server. 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.

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 characters**.

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

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

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.

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

ACTIVITY 1: Numbers, Numbers, Numbers

A. What is the number missing from the last row?

84, 12, 57
29, 11, 65
97, 16, 88
34, _____, 16

B. What is the next number in this sequence?

66, 36, 18, _____

C. What is the next number in this sequence?

2, 12, 1112, 3112, 132112, _____

D. Identify the next two numbers in the sequence below:

202, 122, 232, 425, 262, 728, _____, _____

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 _____

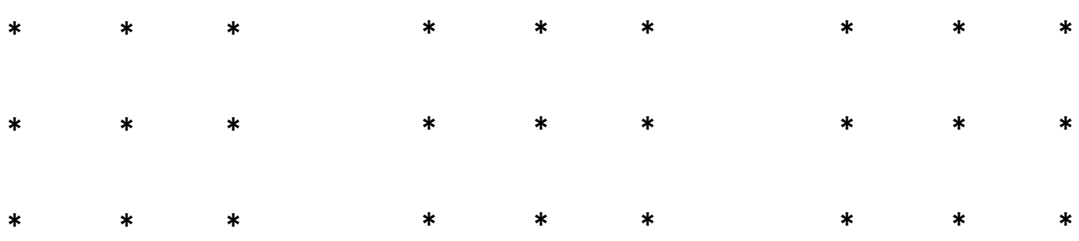
G. Make 80 out of 1, 3, 6, and 9 _____

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

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 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

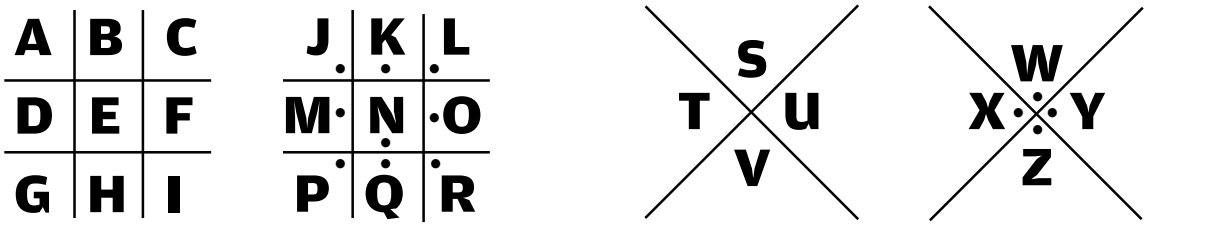
Create your own keyword cipher using the grid below and then write a secret message to a friend!

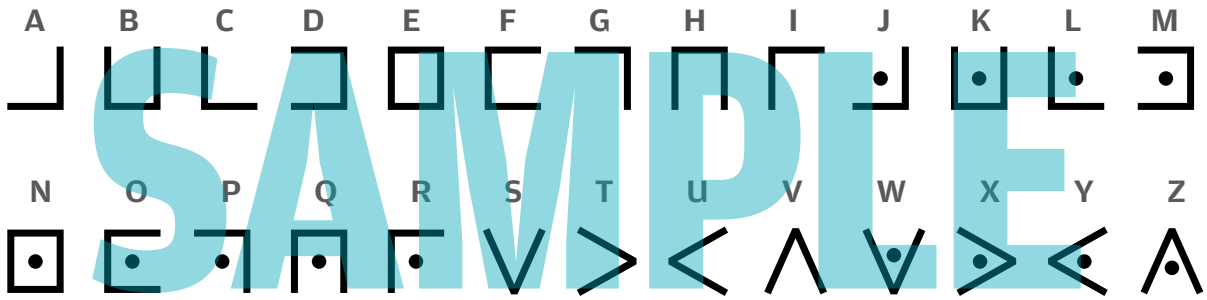
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓

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.





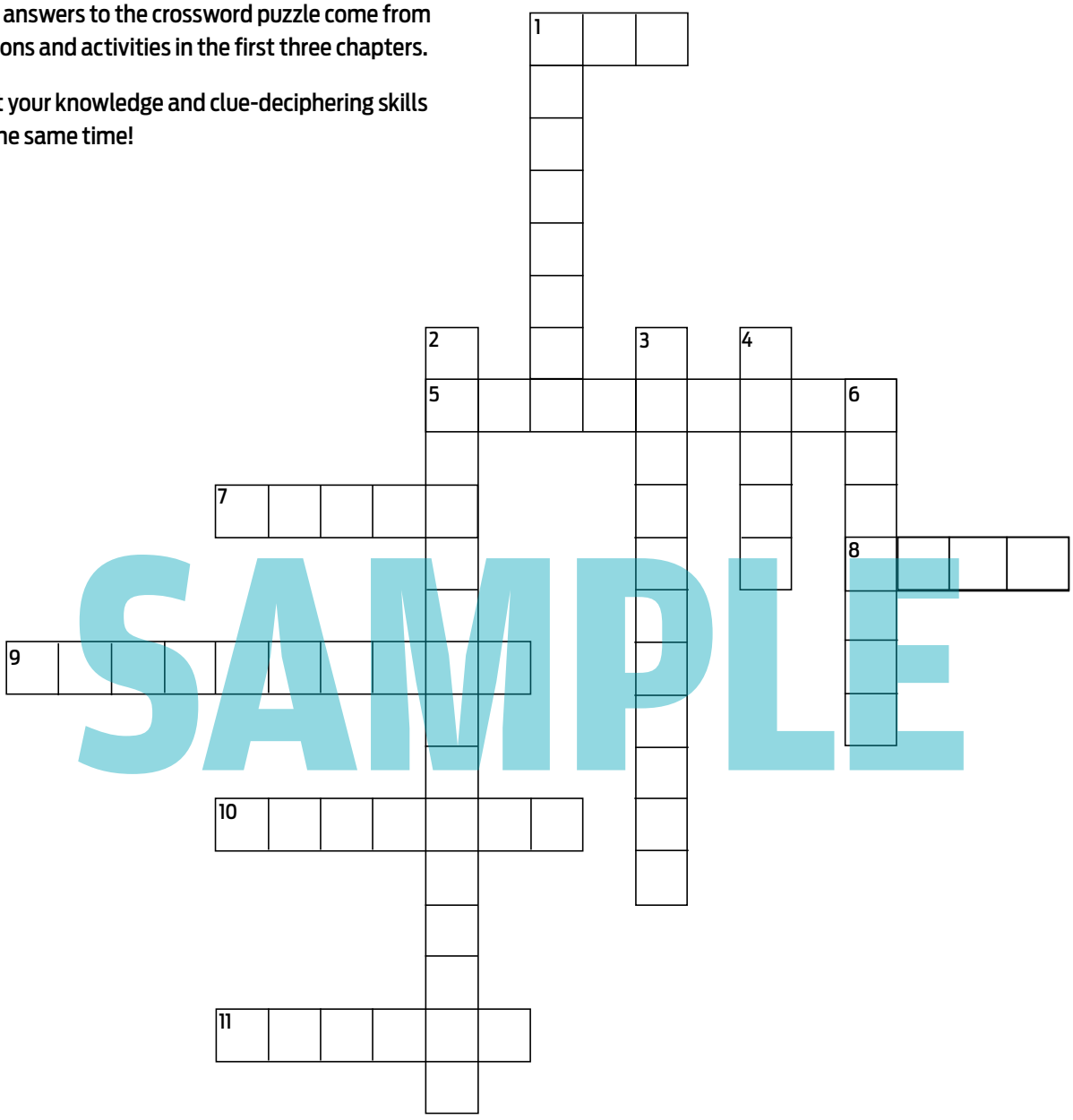
Decode the following message using the pigpen cipher:

Now write your own secret messages!

ACTIVITY 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 4

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. _____

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: _____