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 from 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 let us down.

From elections to the power grid to consumer credit data, online information environments of all kinds have turned out to be vulnerable.

HACKING IN SCHOOLS

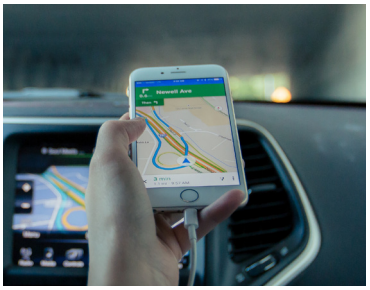
In the last few years, for example, **hundreds of K-12 schools have suffered cyber attacks of one kind or another**. The most common attacks involve malicious hackers penetrating storehouses of personally identifying information, or PII, that schools collect about students. These attacks often lead to 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 a vulnerable target for cyber attacks.

ONLINE NETWORKS

A common thread in the risks of cyber attacks that we face is participation in **online networks**. 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 Facebook, 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.

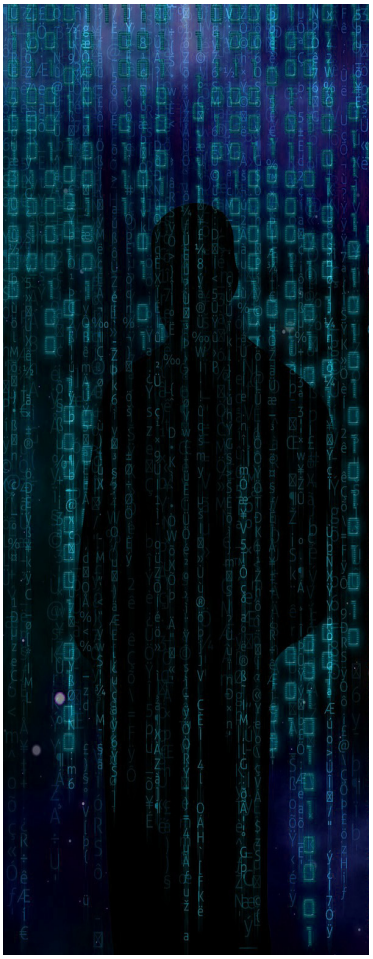
Complete the activity on the next page about your networks to understand more about how you and your family might be exposed to risks from attacks against online networks.

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

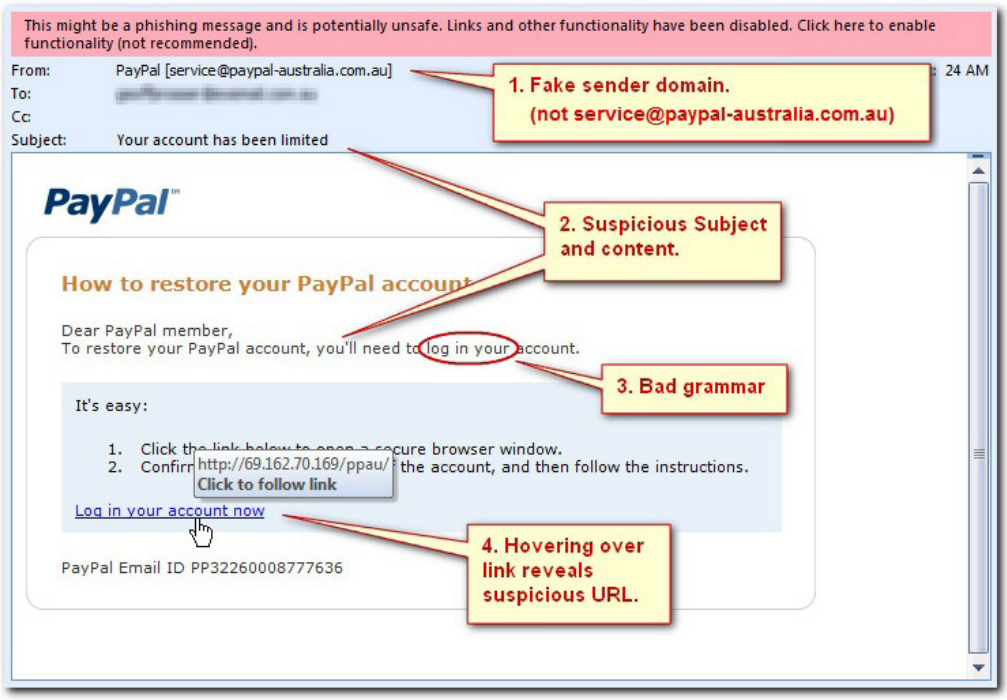


Cybercriminals are constantly working up ways to break into online networks and separate Internet users from their PII. Some of the most common, most effective ways involve deceptive emails and other communications channels deployed to acquire people's user ids, passwords, and/or other account information, especially as associated with financial institutions or other storehouses of valuable digital assets. "Phishing," and its many variants, 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 phishing scams seek to present their communications as coming from 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://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

http://smartermsp.com/quiz-can-outsmart-phishing-scam/

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?

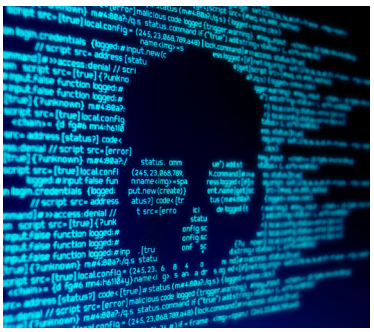
4. What was the hardest part about the quizzes? What was the easiest? What was surprising or different from what you'd expected?

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

MALWARE AND TYPES OF ATTACKS

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.

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 evermore devious, damaging forms.



Malware that circulates through a device/network:

► **Viruses:** Malicious code that reproduces itself on the same device; usually done through infecting a computer program. **Tips:** Be aware of attachments in emails; run antivirus software; install patches and updates; do not use unrecognized USB drives; don't click on links in social media; use a personal firewall.

► **Trojan horses:** A seemingly legit 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. **Tips:** Read reviews prior to downloading random programs/apps; monitor accounts for activity.

► **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. **Tips:** User education; system monitoring; use a personal firewall.

Malware that hides itself in a device/network:

► **Rootkit:** Software that is used to hide the presence of other types of software (usually malicious). Usually used to install botware, spyware, spamware, and keystroke loggers. **Tips:** Still hard to detect and prevent; update browser patches; layer your security; follow tips above.

Malware that collects data:

► **Adware:** Annoying or offensive ad pop-ups, banners, or graphics; this malware can also track online activities. **Tips:** Run an ad-blocker extension; browse in private setting; avoid clicking on unknown emails; don't click pop ups; don't install toolbars; run antivirus software

► **Spyware:** Tracking software used without the consent of the user, e.g., keylogger, programs installed on phones. **Tips:** Avoid unknown USB drives; use a good antivirus program; consider a keyscrambler; cover your webcam; avoid public wifi.

► **Ransomware:** Encrypts data on a device until the user agrees to pay a fee to unlock. **Tips:** Back up data often; don't click on attachments/links; use a previewer or attachment scanner; patch; education.

Malware that modifies or deletes data:

► **Backdoor:** Once installed, it allows the malicious user to avoid system security settings. **Tips**: Use firewalls; monitor your network activity.

► **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. **Tips:** Don't click on links or attachments that you don't trust; avoid pirated software; patch; run antivirus software.

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, or to launch attacks. **Tips:** Don't click links or download any attachments; run antivirus and antispyware software; firewall; keep all your software up to date.

ACTIVITY 3: 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.

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 the news continually reminds us, 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.