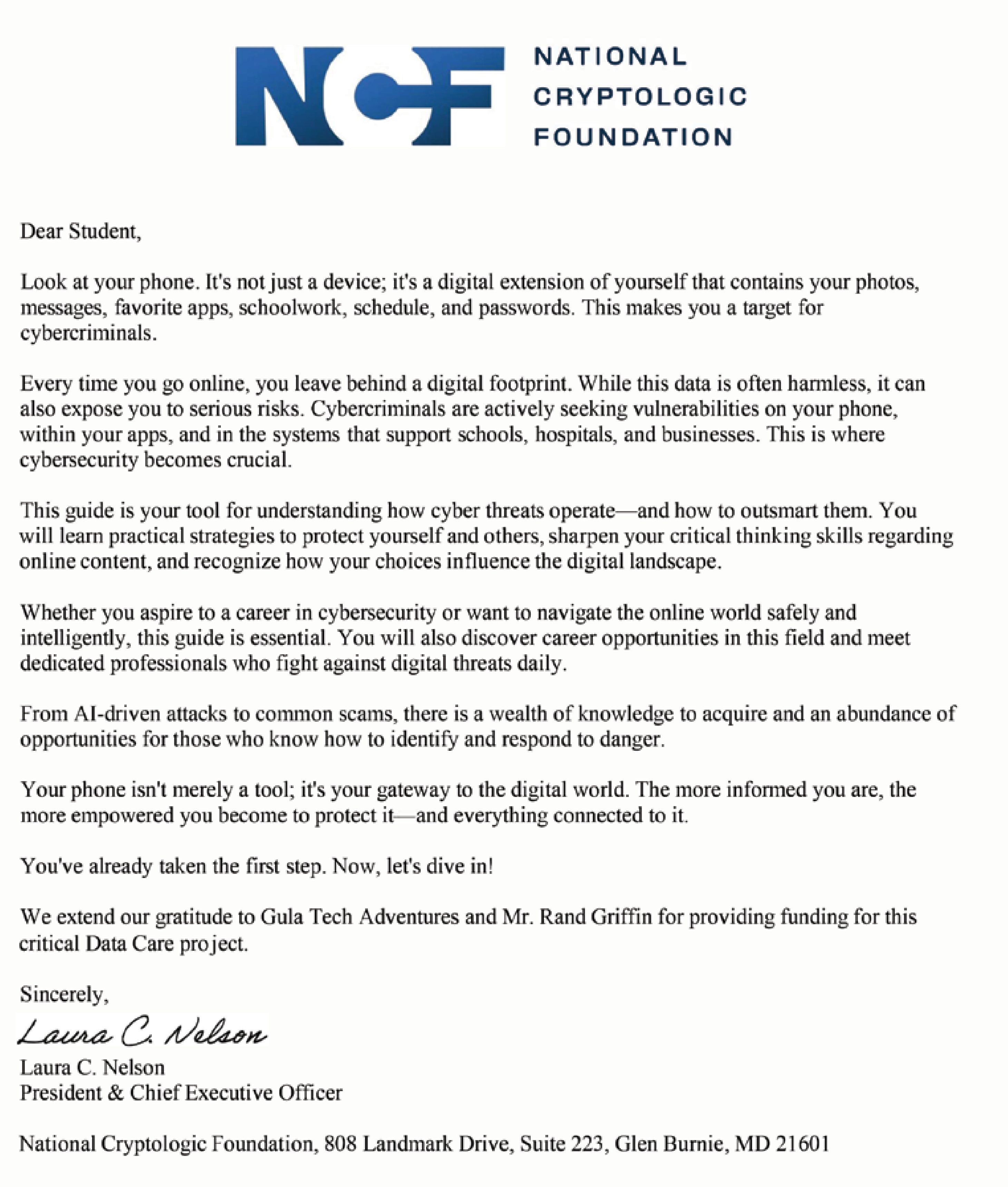
YOUR PHONE COULD EXPOSE YOU TO ALL KINDS OF TROUBLE.

# OUTSMART CYBERTHREATS

Learn how to protect your data and yourself online.

BONUS: Discover a cool new career in cybersecurity!



NATIONAL CRYPTOLOGIC FOUNDATION

Dear Student,

Look at your phone. It's not just a device; it's a digital extension of yourself that contains your photos, messages, favorite apps, schoolwork, schedule, and passwords. This makes you a target for cybercriminals.

Every time you go online, you leave behind a digital footprint. While this data is often harmless, it can also expose you to serious risks. Cybercriminals are actively seeking vulnerabilities on your phone, within your apps, and in the systems that support schools, hospitals, and businesses. This is where cybersecurity becomes crucial.

This guide is your tool for understanding how cyber threats operate—and how to outsmart them. You will learn practical strategies to protect yourself and others, sharpen your critical thinking skills regarding online content, and recognize how your choices influence the digital landscape.

Whether you aspire to a career in cybersecurity or want to navigate the online world safely and intelligently, this guide is essential. You will also discover career opportunities in this field and meet dedicated professionals who fight against digital threats daily.

From AI-driven attacks to common scams, there is a wealth of knowledge to acquire and an abundance of opportunities for those who know how to identify and respond to danger.

Your phone isn't merely a tool; it's your gateway to the digital world. The more informed you are, the more empowered you become to protect it—and everything connected to it.

You've already taken the first step. Now, let's dive in!

We extend our gratitude to Gula Tech Adventures and Mr. Rand Griffin for providing funding for this critical Data Care project.

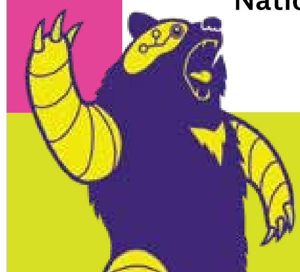
Sincerely,

Laura C. Nelson

Laura C. Nelson
President & Chief Executive Officer

National Cryptologic Foundation, 808 Landmark Drive, Suite 223, Glen Burnie, MD 21601

# WHAT'S INSIDE



ILLUSTRATIONS BY HUAN TRAN

# Your phone has a busy day

**6:45 AM:** Right next to your ear, something clicks and beeps as the alarm on your phone goes off. Your Sleep Cycle app claims to know just when to wake you up, but it's always too early.

**7:20 AM:** Over breakfast, you check out new Instagram Stories from Nike and some friends — you heart a couple, comment on a few, share some more.

**12:45 PM:** At lunch, that guy Greg is playing Zynga Poker online with who knows who and bragging about how much he's won. ***Guh.*** Your phone buzzes with a text from a friend from camp last summer about a fun new game called Space Noodle with a link to download. Quickly, you click and get the game yourself.

**3:15 PM:** Here comes a text from the principal about school pictures being taken the next day. Not awesome. Now your mom is *really* going to care about what clothes you wear.

PHOTOS BY ISTOCKPHOTO.COM UNLESS OTHERWISE INDICATED

**6:45 PM:** After dinner delivered by DoorDash, you put in your ear buds and sink into scrolling for funny TikToks. After a while, you remember you wanted new shoelaces to go with the sneakers you bought on Amazon last week. A quick chat with Siri shows you dozens of options, and you quickly find just the right color for free delivery.

**8:35 PM:** You sneak in some YouTube before 9 PM phones-off, just as a text comes in with an update to the game you got at lunch. Weird, but convenient, so you click the link and watch the file download before shutting down for the night.

After a day like this, your phone has learned about your **sleep habits**, **sense of humor**, **clothes interests**, **food preferences**, **game-playing habits**, and **footwear fashion sense**. And that's just for starters. Every time you interact with a company or an app online, you deliver even more information.

Companies have a voracious appetite for information. In a study to determine which apps gather the most data, every company named above was in the top 25. Besides obvious items like your **email**, **name**, and **phone number**, these apps also collect things like **age**, **gender**, **geographical location**, and **home address**. They can even learn about your hobbies, bank account, and any pets you own. Oh, and often companies gather much of the same information about **everyone you connect with** through an app — your family, friends, online contacts, and so on.

## APPS THAT TRACK YOUR EVERY MOVE

# BIG IDEA 1: Data Security

Data lives in many places and in many forms. Keeping it secure and private is crucial. One part of data security involves control over **physical access** to devices that store data. Another involves **virtual access** and all the technical measures that keep digital data safe from bad guys.

**PHYSICAL ACCESS:** Think about all of the machines that gather and store data.

- ➜ How many can you name?
- ➜ Where do people store data in your school?
- ➜ What kinds of restrictions are in place at your school to keep people out of spaces where data is stored?

**VIRTUAL ACCESS:** To get access to your data stored in computer systems, you typically must get through two "gates": **authentication** and **authorization**.

**Authentication** is you proving that you are you. It usually involves something that

- ➜ only you know, such as **a password**,
- ➜ only you have, such as **a key**, or
- ➜ only you are—your **fingerprint**, for example, or your **retina**.

**Authorization** is what you are allowed to see or do with data once you have proved that you are you.

AI can make both of these gates smarter and stronger, adding sophisticated security measures to do with unique behaviors and traits of users — things like how they type and use a mouse to when and where they usually login to the kinds of things they do with their data once they're inside a system.

The best data security systems combine both **physical** and **virtual** controls in multiple layers or sequences of security measures. If one layer were to fail in a cyber attack, then the next layers would be in place to prevent further access to the stored data.

Think about where you put your phone overnight, when it is out of your physical keeping. What kinds of physical and virtual security layers are in place to protect it? Can you imagine how each of these layers might fail? **What could you do to improve the overall security profile of your phone?**

# Your business is big business

It has become big business — no, huge business — to gather, analyze, and then sell information. The global market for buying and selling data ran to more than $250 billion in 2022. Big data lets companies connect all the dots and get to know us inside and out — **what we buy, care about, feel, and do in the real world.**

The explosion of **artificial intelligence** tools in recent years has only super-charged these data-gathering and analyzing activities. Companies use AI tools to harvest even more personal data, find and monitor social media accounts more fully, and track where we go online with greater precision and detail. And all our ChatGPT queries and Alexa commands conveniently serve up valuable data about our interests and needs to the companies offering these tools.

Companies do mostly use online data for understandable business purposes — to improve services and products, learn more about what we want from them, and devise new approaches to marketing and advertising. Those shoelace ads that pop up in your Google searches, for example, result from the tracks you leave online looking for new laces for the sneakers you just bought. And AI tools like chatbots and virtual assistants are built atop all this online data, often saving users and companies alike time and money. "Talking" with personal technologies that seem to know who we are and what we want might be a little creepy, but the results can be useful.

# Which leads us to cyber crime

*But.* All those bits and pieces of our digital selves sloshing around online also present **risk**. People with bad intentions acquire and misuse our online data, making **cybercrime** big business as well. Damages attributed to cybercrime cost billions of dollars every year. Data breaches expose hundreds of millions of online accounts to potentially criminal exploitation.

In addition, people can use **AI tools** to amplify the dangers of cybercrime and make attacks bigger, more frequent and effective, and harder to detect and defeat.

Keeping online data safe from bad actors and their AI weapons is the main concern of people who work in **cybersecurity**. They try to build safer networks, more secure phones and computers, stronger security programs, and systems for managing data that resist intrusion or attack. **And they get to use AI tools, too.** All the ways AI can make cyberattacks more effective also contribute to making AI-powered cyber defenses stronger, smarter, and more nimble.

Cybersecurity is a fast-growing, fast-changing industry, with exciting opportunities and ample rewards for people with the skills, interests, and drive needed to succeed. In this book, you will identify skills and interests of your own that might make you a good candidate for work in this field.

## HOW SCHOOLS GET HACKED

**PowerSchool, a leading educational technology company, provides software that helps almost 15,000 U.S. schools manage students' personal data and test scores, as well as information about teachers' compensation and benefits. The company is a longtime supporter of high standards for student data privacy practices. And yet, just after Christmas in 2024, a hacker in Ukraine used pirated login credentials to break into the company's systems and steal enormous volumes of students' and teachers' personal data, ranging from grades and addresses to — in some cases — Social Security Numbers. As usual in K-12, the breach resulted from lax safety practices by companies or organizations working with schools, not the schools themselves. But the risks to students' data remain, and the problem is only getting worse. More online and distance learning, ever-growing volumes of data, and new forms of learning technologies are filling schools with more and more online computer systems. This growth in digital data will only increase the number of "attack surfaces," or vulnerabilities to cyber threats, that K–12 schools are going to have to learn better how to protect.**

## CYBER CRIMINALS LOVE YOUR DATA. HERE'S WHY.

**Bad guys online don't care so much about kids themselves IRL — but they do love kids' data. That's because kids usually have no financial history attached to their data. With a full set of real-person data and no financial history attached, criminals can do all sorts of fraudulent things to borrow and spend money, all in real kids' names. The bad part is that when these kids grow up and apply for credit cards, student loans, or other forms of credit and debt, they will find their identities have already been tied to irresponsible or even illegal money behaviors — even if they had nothing to do with them in the first place.**

# Everyone has a responsibility

Even if you don't make cybersecurity a career, you still have a job that every internet user shares: **take better care of personal data to start with**. It's a lot like taking care of your health. In fact, you can think of health care and "data care" in some of the same ways. They both require continuous learning and attention, and the consequences of letting your guard down can be dire. Prevention and vigilance, on the other hand, are key. Good "data care" means understanding what we offer up online about ourselves and thinking hard about what makes us comfortable. It means both demanding that companies take care of our data and being able to take back the data we have shared if they prove untrustworthy. We also need to practice appropriate online safety — **building and maintaining strong passwords, staying alert to scams and sharing our personal information only with trusted, known entities.**

So when we talk about cybersecurity, or "data care," we are really talking about a job that nearly everyone must do. From ordinary, daily internet users to individuals and companies whose business involves digitized data to governments that make rules and enforce laws about online security — all these groups need to do their part for the internet to be as safe as it can be for everyone who uses it.

PHOTO BY JOPWELL FROM PEXELS

**HELP WANTED**

**Cyber jobs to fill in 2025: 750,000***

## WHAT MAKES FOR SUCCESS IN CYBER CAREERS?

You might think knowing all about computers and software and networks is what it takes to succeed in cybersecurity. For some jobs, that's definitely the case. But for far more jobs, it takes other kinds of skills and interests. High-level cybersecurity leaders agree that imagination, problem-solving, teamwork, a commitment to keeping people safe online, and a desire to learn matter more than technical skills. People with these kinds of abilities can make huge contributions to keeping online bad guys at bay and making the internet safer for all of us.

*SOURCE: 2023 OFFICIAL CYBERSECURITY JOBS REPORT BY CYBERSECURITY VENTURES

## HOW STRONG ARE YOUR PASSWORDS?

**Think you know how to build a strong password? Most people don't.**

**Cracking simple passwords is child's play even for novice hackers. A password of eight letters can be cracked in about five seconds. Add a few numbers and it takes about a minute. AI tools can crack passwords even more quickly, and such tools are widely available in online criminal marketplaces.**

**The most common passwords are things like 123456, password, letmein, abc123, and so on. If any of your passwords look like these, put this book down and go change them. NOW.**

**A strong password is unique—a one-of-a-kind code you use only once. It should be longer rather than shorter (12 or more characters). Use numbers, upper- and lowercase letters, and symbols. Avoid personal information. Best of all is to figure out a system to generate and remember passwords.**

**You can even use full sentences or phrases, like "rain, rain, go away" or "my avatar has blue hair." Do things like substitute 3's for E's and 1's for L's to make them harder to crack. The good news is that even AI can't crack complex passwords. A complex, 16-character password would take more time to crack than the Earth has existed.**

**Password managers can also work, as long as you don't forget the main, master password. Get more advice on passwords—and other online safety practices— at StaySafeOnline.org.**

***Your data will get to places online you'd never imagine.***

*Taking care of your data starts with YOU and what you decide to share online about who you are, where you go, and what you do.*

## Something for everyone

As you can tell from this view of cybersecurity, the field is staggeringly complex and wide-reaching. It involves people with a **huge range of skills**, **interests,** and **abilities** performing many kinds of jobs related to generating, gathering, analyzing, using, and protecting the nearly unimaginable volumes of data flowing through digital devices and networks. And really, it all starts with you. **Your behaviors and choices now can help keep your data safer online.** In this book, you will learn how what you choose to do now can help launch you on a path to a career in this world.

Cybersecurity can be technical and computer-focused, and skills in these areas are vital to online digital protections. But to build and maintain a safe environment for online data, we also need people who can do things besides write code, build networks, and develop security systems. We need **imaginative problem-solvers, creative communicators**, **insightful policy-makers, knowledgeable teachers, thoughtful business leaders, and, perhaps most important, informed citizens**.

In Part 2 of this book, you will learn some things you can do now to protect yourself and your data online. And you'll also learn some things about yourself and your interests that might make you a good candidate for work in a data-related field. **If you don't think a career like this is for you, you might be surprised. Read on to find out!**

### PART 1 TAKEAWAYS

**➔ Every time you interact with a company or an app online, you generate data.**

**➔ AI amplifies the ability of companies to collect and learn from our personal data.**

**➔ Companies create models of our behaviors and preferences to understand and predict what we buy, care about, feel, and do in the real world.**

**➔ Cyber criminals steal data in order to sell or ransom it for big bucks.**

**➔ AI makes cybercrime more dangerous AND cybersecurity more effective.**

**➔ Damages attributed to cyber crime run to the billions of dollars every year.**

**➔ Keeping online data safe from bad actors is the main concern of people who work in cybersecurity.**

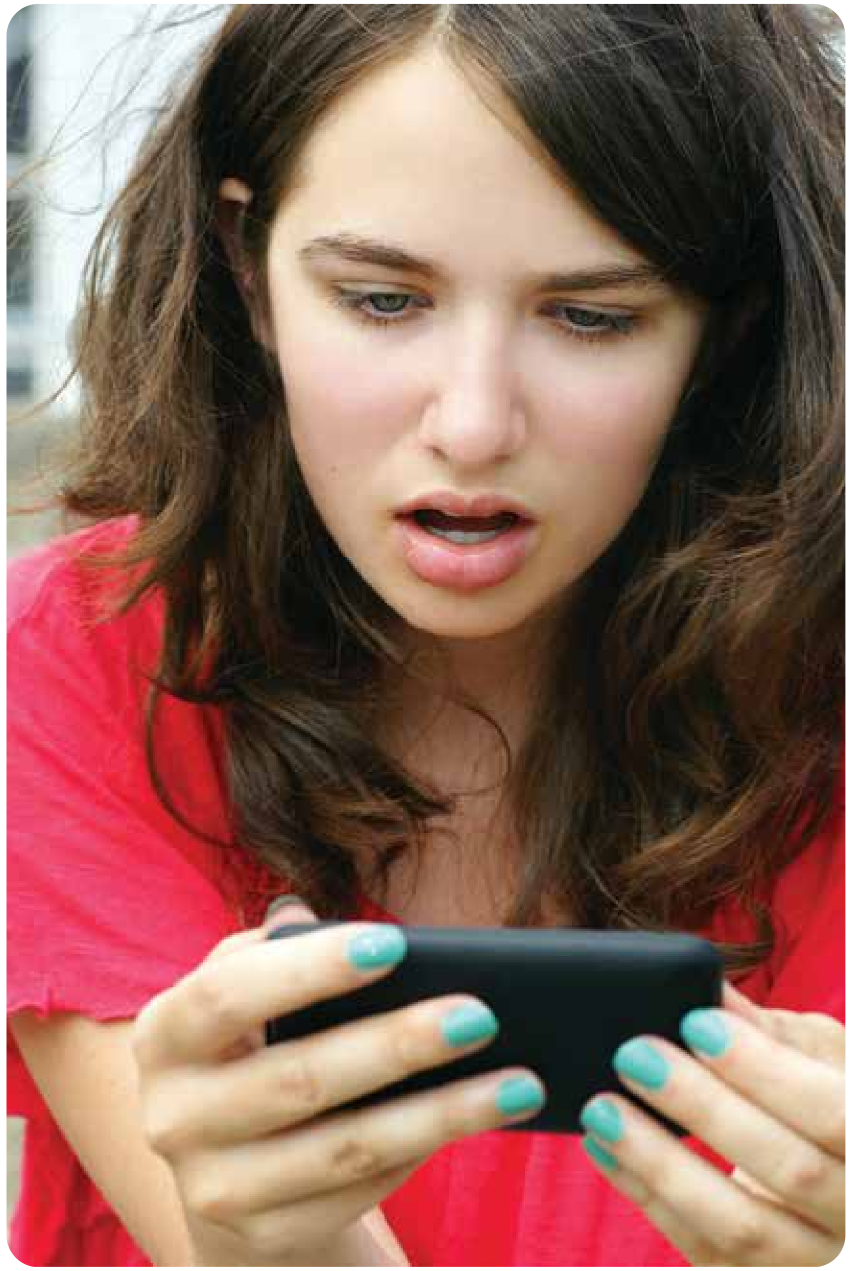
**➔ The cyber field is rich in jobs and needs imaginative problem-solvers.**

# The next, no-good, very awful day

**6:45 AM:** The same clicking and beeping sound wakes you up as the alarm on your phone breaks through the deep sleep you were enjoying. Some days start off worse than others. Well … just you wait.

**7:07 AM:** After brushing your teeth, you pick up your phone and notice that your lock screen has more notifications than usual. Way more. It's jam-packed with text message notifications, from top to bottom.

**7:09 AM:** You've read the first 14 messages. They all say the same thing: **"We are Space Noodle Assault Team 1! We encrypt your phone and lock all files down. You lose. Send $18 with credit card on this link or you never get to open any phone apps again: http://tiny.url.com/41s00pNe33"**



MIRAGE3/123RF

**7:14 AM:** In the next batch of messages, a bunch of your friends are complaining about getting a text from you recommending a game called Space Noodle. And then getting a weird message about their phones being locked down for ransom. What the … !?!

**7:17 AM:** Daaaad!! Moooom!!

**7:21 AM:** With the help of your parents, you swipe left to delete all the text messages without opening them, do a hard reboot of your phone, and test it out to see what's what. *Phew!* Everything works. Just a hoax? Or maybe a misfire? Whatever. You quickly delete the Space Noodle app and start texting back to your friends, saying sorry, sorry, sorry, and here's how you can check to see if your phone's all right.

How did all this happen? Turn the page to find out.

## KEY CYBER SAFETY TERMS

**Deepfake:** A video, picture, or sound that has been changed using AI to make it look or sound real when it's not. For example, someone might use a deepfake to make it seem like someone is saying or doing something they never actually did.

**Malware:** Short for "malicious software," malware is software designed by cyber criminals to gain access to and damage other people's computers or computer networks. It's usually spread by emails or texts that encourage people to click on links or open attachments that can then serve to infect people's devices.

**Phishing:** Seemingly legitimate or innocent emails asking you to respond with personal data or a click on a link; once you take the bait, though, the hacker gains access to your online identity or even your device and does bad things. See page 17 for more on phishing.

**Ransomware:** Software that encrypts data on someone's device until the person agrees to pay money to regain access to files.

**Spyware:** Tracking software that collects data by capturing keystrokes, browsing habits, or other user data and behaviors. All this information is visible to the hacker who has installed the spyware on someone else's computer.

**Virus:** Software written to damage a computer's performance, steal or alter stored data, or interfere in other ways with the normal functions of a machine or network.

**Worm:** Damaging software that replicates and spreads on its own among computers linked through a network. The further they spread in a network, the faster they can replicate and cause problems, from slowing down networks to damaging files and operating systems.

# The trouble with trust

What went wrong with your phone to make for such a crummy start to the day? Well, first, nothing went wrong with your phone. **Something went wrong with how you used your phone** — specifically, how you trusted what was happening with your phone.

That text message with a link to download Space Noodle didn't actually come from your friend from summer camp. It came from the hackers — perhaps Russians, perhaps the Chinese, or maybe someone pretending to be Russian or Chinese — who infected your friend's phone with malware.

The malware then got access to all your friend's contacts and generated the extortionate text. When you clicked on the Space Noodle link inside the text, you downloaded that same malware onto your phone, and voila! Threatening text messages were sent to any of your friends who also clicked and downloaded the app.

You trusted the text because it seemed to be from someone you already knew and trusted in real life. But getting a tip on a fun, new game from your friend in person is different from getting a tip via text. And AI can make it even harder to know if you should trust what shows up on your screen. Because of all the personal data AI tools can uncover about us from scraping the web, details and facts about our lives can show up in misleading ways. **Scams powered by AI can customize individual messages like this one with information we'd expect only real friends to know.** And once downloaded, AI-powered malware can learn and adapt to our device's unique software environment and work in devious, changeable ways, like scouring our contacts and sending out personalized but fake messages.

**So how do we know who and what to trust online?** We all bring a lot of trust to the things we do online. We buy sneakers and books and stocks and bonds, we pay bills, we post pictures and stories of our real-world lives — all with trust that these exchanges are safe. And yet, at the same time, we need to practice unblinking caution at all times for fear of answering a fraudulent request for data that we shouldn't trust. Building and maintaining trust between people, face to face, is hard enough. And as a species, we've been at it for tens of thousands of years. Trust between a person and a machine — over the internet and with AI in the mix — is even more elusive and challenging. And we've only just started to figure it out. Turn the page to learn more.

## HOW TO SPOT A PHISHING ATTEMPT

**Knowing a bogus email when you see one has always been tricky. But bad grammar, wonky formatting, and low-quality images used to be reliable indicators. Now, though, new AI tools have made phishing emails much harder to identify, with more individualized content, smoother writing, and graphics that look exactly like what a real company would use. Worse, AI has made it easier to launch phishing campaigns, so the volume of bogus emails has exploded since 2022. Even so, there are always some give-away traits:**

***They're too good to be true!*** **Money for nothing just doesn't happen, in email or real life.**

***Act now!*** **If you're being rushed to do something, you're probably being tricked.**

***Funky hyperlinks.*** **Hover your cursor over a link and look at the URL at the bottom of the page. If it's weird, steer clear. Even an AI-made phishing email must lead to a fake URL.**

***Unexpected attachments.*** **If you're not expecting an attachment, don't open an attachment. Simple rule. You can always write back to confirm something with the sender.**

***Unknown sender.*** **If you don't know the person sending you something, don't open it. Another simple rule.**

**To practice identifying phishing emails, do an internet search for "phishing quiz" and pick out three or four of the quick and usually fun quiz options that come up.**

# BIG IDEA 2: Establishing Trust

To trust an online data system, we need to have faith in three things: the confidentiality, integrity, and availability of our data. This is the "CIA triad," and all trustworthy online systems should be designed so that:

1. **Data is confidential, accessible only to ourselves and appropriately authorized people in the organization holding our data.**
2. **Data has integrity; it is correct, authentic, and reliable, corresponding to off-line reality as we know and expect it to be.**
3. **Data is available, and we can get to it and put it to use when and where we need to.**

Designing a system that meets these three goals AND is easy to use is tricky. You wouldn't trust a bank if you could log into your account with just your name. On the other hand, if you had to enter a username, change your password every week, do a retina scan, and answer three security questions just to check your balance, what an incredible pain!

AI tools raise unique data challenges, for both system designers and users. The value of the tools' outputs depends on the quality of the data used to train them. If the training data is garbage going in, the responses will be garbage coming out. Designers of AI systems don't always use the right kind of training data, and users of AI tools will mostly have no idea one way or the other. So "data integrity" is hugely important but very difficult to assess, which complicates the question of how much to trust AI systems.

Using any online data system — from Instagram to Amazon to ChatGPT — requires ongoing consideration of how much trust it deserves. **Usability and security are always in tension.**

Designers of data systems must balance security requirements with user convenience, but the balance might not always be right for you. You can always just walk away from any website or system that seems squirrelly. Remember, the only safe, reliable assumption about online data is that **nothing is ever completely safe.**

# How to know a website is safe

Establishing trust between person and machine is probably easier than maintaining it. As human users, we all become quickly acquainted with the basic tools for joining an online network: the username and password. You introduce yourself to a machine with a username, as in: "Hi, I'm FreeToBe@youandme.com. Can I come in?" The machine says, "Hmm. I'm not sure I believe you are who you say you are. I'm going to ask you something that you and only you should know."

Then you enter a password to prove that you are you **(remember authentication?)**, and you get access to the data in that system that you are allowed to see **(authorization)**. Pretty simple, in theory, even though the password part can trip people up. More on that later.

On the machine side, things are more technical. Sensitive information should always be encrypted, and by far most websites now use powerful encryption tools to make all traffic—sensitive or otherwise—impossible to hack while in digital transit. **You can tell a website is safe if the address begins with "https," with the "s" standing for "secure."** Even AI can't crack this kind of code, at least not yet. So you know the technical side of things is safe if "https" is in force. But there's more — turn the page.

## The next steps get tricky

To keep trust alive in the person-machine exchange, though, both people and machines must keep doing the right things. Individuals should be effectively managing and protecting login credentials. Organizations should be enforcing strict rules about who gets to see the information you provide, let alone who gets to do anything like change it or move it or sell it (which happens too often!). Machines storing your information should be on, accessible, and physically protected at all times, with backup systems in place for the inevitable hiccups.

When things go wrong, the level of trust suffers. If you enter your password incorrectly too many times, the machine might say, "Sorry, come back later and try again." When you learn that a machine has messed up handling your data, you should think twice about sharing any more of it.

But even when things go right between you and the machine, things can go wrong online. **Your phone got infected with malware because hackers exploited a friendship of yours to finagle transmission of an apparently harmless text message. You read the text, clicked a link, and bad things happened as a result.**

*To take better care of your data, imagine how things can go* ***wrong*** *to improve chances for things to go* ***right****. Develop a*

**security mindset.**

***You should bring it with you everywhere you go online.***

# The security mindset

But none of this happened because of a failure in machine security. It was all human error, induced by so-called social engineering. **Social engineering involves tricking people into believing they are involved in trustworthy exchanges and making mistakes.** Indeed, over 90 percent of data breaches arise from careless human behaviors, like clicking on links to malware, giving up login credentials, or other, generally sloppy ways of handling access to networks.

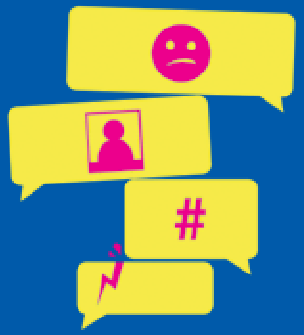
And AI just makes it all worse—enabling more personal data harvesting, refining code to make malware more elusive, automating attacks to make them faster and more numerous. All these "advances" make it more likely that people will trust things that are not what they seem and do things they should not do.

The Space Noodle scam is a form of **"phishing,"** which can come at you by text or email. A message arrives pretending to be from someone you already know. It asks for information that allows the sender to gain improper access to the recipient's machine or online account or other digital asset. No matter how well we guard against these tricks, they still work. (See page 17.)

Phishing is just one weapon in cyber criminals' arsenal of deceit and trickery. A witches' brew of **viruses, scams, disruptive schemes, and direct attacks** lurks in the dark corners of the internet. And AI makes it easier for criminals even without technical expertise because attack-ready AI systems are widely available for sale on black internet markets.

With threats always lurking and getting more deceptive all the time, what do we do? As a broad principle, assume that all the networks that store and transmit data are unsafe. If you expect all data systems to have flaws, you will approach any digital request for a click or personal information with heightened caution. You will develop the habit of looking for ways that things can go wrong in online security systems. In other words, you will start to develop a **"security mindset,"** an ability to think like an attacker — not just a user — of online networks.

The best cybersecurity professionals, no matter their role in protecting the internet, approach their tasks with a security mindset. In Part 3, you'll learn more about what a security mindset can look like and how to start developing your own personal version of it. It just might be the best online safety tool you ever learn to use.



## WATCH WHAT YOU SAY OR SEND OR SNAP

**Kids love their messaging apps. It's so easy to dash off a "hey" or a joke, a funny selfie, a video, whatever. And then the message disappears, drowned in a quickly rising thread, as the moment passes. Except when the message doesn't disappear. And it's something private, like a picture that the whole world should definitely NOT be seeing. Teenagers' worst selfie nightmares came true in 2014 when over 100,000 revealing Snapchat messages got hacked, and in short order, thousands of extremely inappropriate photos and videos of kids, some as young as 13 years old, got posted online for all the world to see. The lesson? Expect anything you post or share online to become public. Once you hit send, you lose control, and the message is loose in the world.**

## PART 2 TAKEAWAYS

- **Expect anything you post or share online to become public.**
- **Phishing hackers are counting on people not paying close attention to emails and just clicking or answering without looking very hard at what they're doing.**
- **To trust an online data system, we need to have faith in three things: the confidentiality, integrity, and availability of our data.**
- **AI makes online trust even harder to find—scams, deepfakes, even responses to simple ChatGPT queries can seem totally real but be completely false.**
- **A strong password contains at least eight characters, including numbers, upper- and lower-case letters, and symbols.**
- **Social engineering involves tricking people into believing they are involved in trustworthy exchanges or activities.**
- **Developing a "security mindset" will keep you safer online and could lead to an exciting cyber career.**

# The day gets better ... eventually

**7:45 AM:** All dressed up for pictures, you enter the school, wondering what kind of response you'll get from friends with malware-infected phones.

**7:48 AM:** After having three phones full of ransom demands thrust under your nose, accompanied by variations of "bruh, this?!", you get your answer. People are annoyed.

**8:25 AM**: Adele, that sometimes mean girl with a locker near yours, looks you up and down as you're stowing your backpack. "Hah!" she says. "Don't you look sweet! Didn't you know? The school picture text was a hoax. Read the school calendar much?"

**9:40 AM:** By the time you get to morning break, you realize you are one of the few people who fell for the school picture hoax. Walking around all day in dressy clothes feels a great big fail.

GETTY IMAGES/ JON FEINGERSH PHOTOGRAPHY INC

**11:30 AM:** At lunch, you learn that they caught the kids who sent the hoax text. Turns out they snuck into the principal's office, found the username and password for the school's text message account on a Post-it note, and sent the text out as a joke. No real harm, but it's still a big problem for those kids — and a lesson for the principal to take better care of his login credentials.

**2:45 PM:** Your dad is excited about something when you get home. "Hey, look, we can get Ray-Ban sunglasses for $20 a pair on super sale, today only. I saw a tweet about it." Your newly sensitized cybersecurity antennae tune in right away. "What?! Dad, that sounds totally sketch. They never go on sale. Some random tweet? C'mon!"

**2:55 PM:** Sure enough, a quick search for "Ray-Ban sale scam" serves up multiple debunkings. Your dad gives you a sheepish look. "Um, thanks. I should have known better after our morning today." You answer, "I know, right, I am ready to turn off my phone forever."

**4:15 PM:** ***Buzz***. Your phone perks up with a text from your friend Rafael. "Wanna play some Murder Mystery 2 in my private server?" And off you go to Roblox land. Maybe phones aren't so bad after all.

## TIPS TO STAY SAFE IN THE AI ERA

AI makes online safety more complicated. It sucks up more personal data from more sources, analyzes it more fully, produces totally realistic digital content, and is constantly evolving. But AI also powers new tools and systems to keep us and our devices safer. As always, combine your human intelligence with AI tools to stay safe, starting with these tips:

### SETTINGS

- Look for ways to set up devices, browsers, and online accounts to limit or prevent sharing personal data.
- Opt out wherever you can of data collection or personalization operations.

### BEHAVIORS

- Avoid sharing personal information with AI chatbots or assistants—they gather data and link it to users' individual profiles.
- Learn to spot AI-generated images, videos, and text.
- Fact-check and verify things you learn online from multiple sources, especially the more surprising or dramatic these things are.

### TOOLS

- Take advantage of AI-powered antivirus and spam detection tools, often available as apps, built into devices, or as part of software packages.
- Use multi-factor authentication, especially with sensitive data — AI makes password cracking easier for bad guys.

## HOW DOES AI ACTUALLY WORK?

**AI systems combine two things to do the incredible work they do: enormous amounts of data and amazingly powerful computers. First, computer experts create complicated models of the world out of huge sets of data. Then, they feed this data into sophisticated computer programs that identify patterns in data as corresponding to objects in the world, essentially creating a map of reality inside an AI system. The AI system "learns" about the world this way in a process called "machine learning." It then uses this learning to answer questions about the virtual map of the world that help people then learn things about the real world.**

**Machines, in fact, learn in ways similar to how our brains learn. Our brains are made up of distinct, interconnected parts that process information from the world in different ways, depending on the kinds of brain cells, or "neurons," that make up these parts. Working together, these interconnected parts form "neural networks" that perform reasoning operations to help us learn about the world. AI systems are built this way, too, using digital "neural networks" to identify and match patterns in data to learn about objects in the world. So "machine learning" combines with "neural networks" to make AI systems faster, more powerful, and more complicated than computers ever used to be.**

# Living with online risk

Sometimes the hard way is how you learn a lesson. At the end of a no-good, very awful day with your phone, you applied new understanding of how things can go wrong online to save your dad from giving up his credit card info to the sunglasses scammers. Your security mindset in action helped you recognize a clear and present risk, and you acted to keep your family safe from internet trouble.

As you know by now, every online data exchange involves risk. But that doesn't keep us from going online. Every time we share or collect data, we must assess risk and then decide whether or not to do what we have set out to do. AI complicates this assessment of risk because it creates digital "realities" that might not in fact be "real." Deepfakes, highly polished phishing messages, and hallucinatory answers from AI chatbots can all seem believable and trustworthy even when they are totally not so. For your personal online safety and career options, though, getting a handle on risk is fundamental. So let's talk about risk.

**Risk can be understood as a combination of two factors: the chance of a bad thing happening and how bad the thing would be if it actually happened.** In other words, likelihood of damage and severity of damage. Analyzing both variables is necessary for assessing the risk of any online data exchange. Sometimes the likelihood might be high but the severity not so bad, so you complete the exchange. Putting up a silly Story on Instagram might be embarrassing but probably not harmful, so you do it anyway.

Other times, the chance of damage is low but the potential severity is great. Paying someone by PayPal connects your bank account or credit card to another person's financial institution, but the encryption and overall security of the transaction are so strong that you do it for the convenience. And then there are times when both the likelihood and severity of damage are too great to complete the transaction, such as with the sunglasses scam. With AI working in the background on so much of what we do and see online, it can be hard to make an informed assessment of risk factors. The tips on the page 25 can help, along with your own careful attention to information you share.

In all cases, though, **you assess the risk factors in play and then decide what action to take.** Exactly this calculation lies at the heart of nearly every job you can imagine in the professional world of cybersecurity.

**How cybersecurity professionals assess risk depends on the kind of responsibility their jobs give them for taking care of data**. You can think of cybersecurity jobs as falling into any of three broad "fields" within the career landscape. Looking back at the kinds of trouble you had with your phone can illustrate what these fields are all about.

## BIG IDEA 3: Risk

Risk is a part of our lives every day. We are always judging how bad something might be against the chance of it actually happening as we make decisions about what to do or what NOT to do. Assessing risk to online data and systems occupies the attention of all cybersecurity professionals. It's almost a formula: **the possibility of damage to a network or system times the likelihood of such damage actually occurring.**

Three basic factors drive cybersecurity professionals' assessment of risk, and each of these factors draws on different kinds of skills and interests. Read on to see where you might fit in the business of assessing risk:

**VULNERABILITY:** a weakness in the security of a system, like a broken lock on your front door. Finding vulnerabilities can take technical knowledge of programs, computers, and networks. The work can be like navigating a maze or solving a Rubik's Cube. If you like these kinds of activities, this area of cybersecurity might be fun for you.

**THREAT:** the bad guys, the burglars prowling around at night looking for houses to break into. Identifying and tracking down threats means figuring out who might want to get their hands on data in a system you are protecting. It could be anyone from run-of-the-mill bad guys to organized criminals to other countries' military or intelligence forces. If you like thinking about what makes other people tick, analyzing threats might be a good job for you.

**ATTACK:** the event itself, a burglar breaking in and looking for something to steal. Attacks can come from any direction at any time. You have to be alert and prepared, ready to defend your networks against an attack and then fight back. If bad guys make your blood boil and you like the intensity of competition, you might find work in this area satisfying.

# How the scam worked

The Space Noodle scam had two parts: (1) malware written by someone with bad intentions and (2) a strategy to trick you into trusting a fraudulent text message.

The development and delivery of the malware highlight the **"logical field"** of cybersecurity careers. People in the logical field study the ways that bad guys use software, AI tools, and online devices to attack networks and network data. They also develop programs and machinery, all based on the "logic" of circuits and electronics, to protect against cyberattacks. Luckily, they also get to use AI tools in the cause of online safety. The computing power, learning potential, and extensive, real-time monitoring capabilities of AI cybersecurity measures make for strong defenses against cybercrime.

The strategy to trick you is based on your trust for a friend, and it shows the importance of understanding human psychology and behavior. This **"social field"** addresses the interpersonal, or social, elements of online exchanges, whether they start in real life and move online or take all-digital form. Here, too, AI complicates things because it can interact with us online in ways that can seem human, meaning "social" considerations must extend to both human and virtual actors. People in this field study and/or try to shape the thought processes, actions, and values we bring to online activities, as well as new issues to do with how AI works. Teachers, researchers, government officials, businesspeople, and law enforcement are among those concerned with how our social, real-world selves can expose us to online risk.

The school picture hoax happened because kids got physical access to data in a place meant to be off-limits. So, in this **"physical field,"** people work on security controls, creating and guarding spaces where data and equipment are stored. That means everyone from architects and engineers involved in design, to builders and security personnel, to makers and sellers of technologies used to monitor and protect physical locations.

*Effective, reliable cybersecurity work takes many people doing many kinds of jobs.*

*Whatever you're good at or like to do,*

***there's a place for you.***

# The world wants you

Whatever they do in these fields, cybersecurity professionals rely on the same core capacities: **assessing risk, knowing their subject areas, and solving problems with imagination.** And driving them all is a commitment to making the internet a safer place for everyone.

The more you can learn about the actual jobs these people do, the better you can decide if a career in one of these fields might work for you. By now, you know well that the professionals in these fields focus on keeping our data safe in all the ways it gets transmitted and stored online. In Part 4, you will start learning how to **connect your skills and interests to possible careers in these fields**. And you will find out more about what "keeping our data safe" means in jobs that people actually do.

## PART 3 TAKEAWAYS

- → **Almost all data breaches result from bad choices people make. We the people present the biggest risk to our own data.**
- → **To assess risk, you need to understand the chance of a bad thing happening and how bad the thing would be if it actually happened.**
- → **Risk is everywhere online. But we still use the internet all the time. We just have to be smart about it.**
- → **AI amplifies the risk of bad things happening online, but it also makes cybersecurity tools stronger, faster, and better.**
- → **Cybersecurity jobs involve an incredible variety of skills and interests. The jobs can be divided into three general areas: the logical field, the social field, and the physical field.**
- → **You're almost sure to find a place in the field that works for you, if you want to.**

# How they do what they do

People who work in cybersecurity do **a lot of different things in their jobs**. You might imagine they write code, work on computers, and study online network data and traffic. And that is often true. But just as often, they never write a line of code in their whole career.

Instead, they put other skills and abilities to work. People who are good at — and enjoy! — jobs in cybersecurity draw on **imagination and persistence** to solve problems. Tricky problems. They find patterns and connections where other people just see differences. They like figuring out puzzles in words, numbers, pictures, or pieces. Crosswords, Sudoku, Tangrams, those 3D puzzles you solve with interlocking wooden pieces.

Many of them like **solving tricky problems in teams** or, even better, in competition with other teams. Working together — under pressure, on the clock — brings out the best in them. They are good at listening to each other's ideas, connecting those ideas to what they themselves know, and putting it all together in a way none of them could do on their own.

PHOTO BY FAUXELS FROM PEXELS

**The jobs they do are important.** Cyberattacks can cost people, companies, and governments a lot of money. They can also do real damage. A 2021 attack came close to poisoning the water supplied to a Florida town of 15,000 residents, but alert plant operators stopped the hack and restored the system to safety. Still, the danger persists. Cyberattacks on water plants jumped by almost 70 percent from 2023 to 2024. Because so many of these plants use outdated software systems that are easy to break into, cybercriminals find them inviting targets.

In a cybersecurity job, you will always be working to **protect something valuable and important** to your organization, your community, maybe even your country. You will have to be imaginative, collaborative, and tenacious in fulfilling your mission. If you think that sounds like fun, you could be headed for success in the field.

## IT'S ALL IN HOW YOU LOOK AT THINGS

Do you like solving brain teasers and tricky puzzles? Can you see problems from a slightly different angle than other people? If so, you might be a good candidate for work in data care. Try solving these problems. Look for creative and different ways to "see" the questions. Remember, you can learn and get better at "imaginative problem-solving" once you get the hang of it.

**1. Find a word that completes the sequence below.**

Fun, boo, tree, gore, hive, mix, heaven, rate, sign, ____

Hint 1: Say the words out loud.
Hint 2: Say the words out loud, but drop the sound of the first letter.

**2. What number is missing below?**

46, 10, 28
17, 8, 44
39, 12, 57
96, __, 78

**3. A certain five-letter word becomes shorter when you add two letters to it. What is the word?**

***ANSWER #1:*** *The words rhyme with the numbers 1 through 9, so any word that rhymes with 10 would complete the sequence.*

***ANSWER #2:*** *15. The numbers in the middle equal the sums of the digits of the numbers on either side.*

***ANSWER #3:*** *Short. Adding two letters—"er"—to "short" makes it "shorter." Nyuk, yuk.*

# Is a spot in cyber right for you?

Learning about real-world examples of data breaches and cyberattacks can help you understand more deeply what "keeping our data safe" means. News stories about data security failures appear almost every week. You can find them on TV, in the newspaper, online—anywhere you go to find out what is happening in the world. And you can ask your parents or teachers to help you dig more deeply into these stories. Look for documentaries, magazine articles and books, and even people at your own school who work with the computers and networks used by students, teachers, and staff.

**More and more clubs and after-school programs focus on cybersecurity and online safety topics.** CyberPatriot, for example, teaches students how to protect actual online data networks. Participants then compete in teams to show off their skills at this vital dimension of real-life cybersecurity work. Check it out at uscyberpatriot.org.

ICONS BY KEVIN MYERS

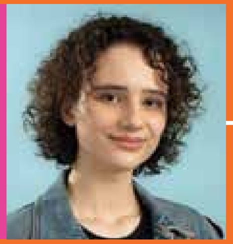
# TYPES OF CYBER JOBS

In the battle against online bad guys, people with more technical, security-focused jobs are on the front lines.

| | | |
|---|---|---|
| **INVESTIGATORS** | **Investigate and review cyber crimes.** | They often work with law enforcement and counterintelligence. |
| **ANALYSTS** | **Collect and analyze threat information from multiple sources.** | They also evaluate the capabilities and activities of cyber criminals. |
| **PROTECTORS** | **Search for weaknesses in software, hardware, and networks.** | Also known as "ethical hackers," they work in many different fields. |
| **PROGRAMMERS** | **Conceptualize, build, and test secure computer systems.** | They also create tools for virus, spyware, or malware detection. |
| **MANAGERS** | **Oversee the cybersecurity program.** | They also offer legal or policy advice and recommendations. |

# HOW CYBER STARS TOOK FLIGHT

See how leading lights in cybersecurity found their places in the field.

| | | | | |
|---|---|---|---|---|
| Yonesy Feliciano Nuñez | | Financial services intern → | Completed information systems certifications and graduate work → | Cybersecurity industry leader and innovator in making online finance safe and secure |
| Diva Hurtado | | Degree in international affairs → | Started on-campus hackathon and digital self-defense classes → | Creates digital security for learning apps, password manager services, and online tax filing systems |
| Alissah Abdullah | | Worked in cryptography and code-breaking → | Became White House information security officer → | Leading the charge for online credit card safety |
| Bianca Lewis (BiaSciLab) |  | Started hacking at age 10 → | Founded Girls Who Hack and started speaking worldwide about cybersecurity and girls' empowerment → | Is youngest member of Cult of the Dead Cow, the oldest hacker activist group |
| Dr. Calvin Nobles | | Specialized in cryptology and info warfare in U.S. Navy → | 25+ year cybersecurity career, focused on human factors engineering → | Serves as Dean of UMGC's School of Cybersecurity & IT, and Board Member at NCF |

SOURCE: LINKEDIN

And you can learn lots more about the field at the website of the National Cryptologic Foundation (www.cryptologic-foundation.org).

Many schools offer computer science classes as early as 6th grade. **See what catches your interest whenever you work on computers and look for chances to learn more**. While much of the content might be technical, remember that jobs in the field vary widely. Remember that "data care," just like healthcare, relies on a combination of expertise and practice across many interconnected areas of knowledge, with empowered and knowledgeable individuals at the heart of the effort.

In this book, we have tried to show you how to take better care of data in your personal life as well as how you can do it in a career. You get to decide if you want to work in cybersecurity or just apply these lessons to your own online life. Either way, you can be sure that people like you — our best and brightest students with a desire to make the world a better place — will lead the way to safer, better lives online for all of us.

PHOTOS COURTESY

## PART 4 TAKEAWAYS

→ **People with careers in cybersecurity do a lot of different things, but they all draw on imagination and persistence to solve problems.**

→ **Working together on tricky problems, cybersecurity professionals get things done that they couldn't do on their own.**

→ **Cyberattacks can do real damage. In a cybersecurity job, you will always be protecting something valuable and important to other people.**

→ **Learn more about the field by following news of cyberattacks and taking computer science classes.**

→ **Protecting the online world is a mission we all share. We need our best and brightest students to help make the internet safer for all of us. Could that include you?**

## The National Cryptologic Foundation (NCF) Education Offerings for Students, Teachers, Counselors, Administrators & Parents

→ The NCF and our strategic partner Teach Cyber developed the **High School Cybersecurity Curriculum Guidelines (CCG)**. The High School CCG encourages curriculum providers, teachers, and industry to create curriculum designed to inspire high school students to pursue a cybersecurity profession and develop thinkers with a cybersecurity mindset that will enhance any career they pursue. The Guidelines are available to state departments of education and school districts across the country through our partner Teach Cyber.

→ With our partner Teach Cyber, a year-long **High School introductory cybersecurity course** based on the CCG is now available. The goal of the course is to introduce students to the foundational concepts, principles, and tools of cybersecurity. All materials developed are under creative commons licensing and available to all 130,000 K-12 institutions at no charge through Teach Cyber.

→ The NCF hosts cybersecurity **professional development workshops for teachers** on the CCG and the cybersecurity course. The training prepares teachers to teach cybersecurity by building their cybersecurity knowledge meaningfully and how to teach it.

→ The NCF brings cybersecurity education into classrooms and homes through the **#CyberChats Podcast**. #CyberChats is a podcast for new and seasoned cyber fanatics, ages 11-18, that unlocks what hackers and hijackers don't want you to know. The podcast features cybersecurity professionals in industry, government, and academia, as well as a youth active in cybersecurity. Listeners learn from these experts how to secure their data and celebrate success stories in our community of cyber heads.

→ The NCF hosts mobile interactive education via its **Cybersecurity Escape Room** at any location proximate to Maryland, such as at a middle or high school, scouting event, or community center.

**Contact Alisha Jordan, Education Director, to schedule or discuss any of the NCF Education Program Offerings: ajordan@cryptologicfoundation.org.**

**Published by Start Engineering, LLC**

CEO: Bob Black
Creative Director: Stacie Harrison
VP, Learning and Communications: Eric Iversen

© Start Engineering, LLC

Illustrations by Huan Tran

For additional printed copies of this publication, please contact Bob Black at bblack@start-engineering.com, or 202-841-1524.

**Strengthening trust in the digital ecosystem.**

NCF NATIONAL CRYPTOLOGIC FOUNDATION

# OUR MISSION

Advance the nation's interest in cyber and cryptology as we:

★★★

Educate citizens to be cyber smart individuals and develop pathways for the future cyber and cryptologic workforce.

★★★

Engage and convene partners to address emerging cyber and cryptologic issues.

★★★

Commemorate our cryptologic history and those who served.

National Cryptologic Foundation
808 Landmark Drive, Suite 223, Glen Burnie, MD 21061
443-795-4498 | www.cryptologicfoundation.org
Dr. Alisha Jordan, NCF Education Director | ajordan@cryptologicfoundation.org

National Cryptologic Foundation @ncfcyber @NCFcyber National Cryptologic Foundation