

YOUR PHONE COULD EXPOSE YOU TO ALL KINDS OF TROUBLE.



OUTSMART CYBERTHREATS

Learn how to take good care of your data.
BONUS: Discover a cool new career in cybersecurity!



Summer 2023

The number of cyber incidents affecting U.S. businesses and individuals is growing daily.

Every time you use your smartphone, tablet, or computer, you share your personal data. Do you know how to keep your data safe? Maybe you have heard your parents, grandparents, or other adults talk about cyber attacks in the news. What does that mean? How might it affect your family? How might it affect you?

In an increasingly digital world, you must learn about cybersecurity and practice data care to protect yourself, your devices, and online accounts by creating strong passwords and not opening messages from unknown senders.

The National Cryptologic Foundation (NCF) is a leading expert in K-12 cyber education and encourages you to read this Cybersecurity Booklet with your teachers, and parents. This resource will help teach you how to stay safe from cyber threats while encouraging you to learn about cyber and STEM (science, technology, engineering, math) subjects.

In the pages that follow, you will learn the importance of taking care of your data. School districts, hospitals, healthcare organizations, and public companies, among others, don't have the talent and skills to defend themselves and the need for cybersecurity professionals grows daily. We want this booklet to spark YOUR interest in cybersecurity to develop skills in middle and high school that can lead you to choose cybersecurity as your profession. It's a growing industry! Go to cyberseek.org to see the current cyber positions available today and those expected in the future, in your state.

The NCF is among a group of organizations who are collaboratively developing resources for K-12 students and educators that are available to download at no charge. Please visit our website cryptologicfoundation.org to access these resources.

We extend our gratitude to our development partner Start Engineering, and Gula Tech Adventures, for funding this critical Data Care project.

Sincerely,

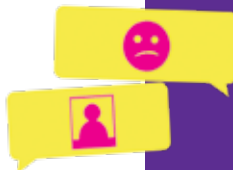
A handwritten signature in cursive script that reads "Laura C. Nelson".

Laura C. Nelson
National Cryptologic Foundation
President & Chief Executive Officer

National Cryptologic Foundation, 808 Landmark Drive, Suite 223, Glen Burnie, MD 21061
443-795-4498 ♦ booklet@cryptologicfoundation.org ♦ www.cryptologicfoundation.org



PART 1: A DAY IN THE LIFE OF YOUR PHONE	4
Your phone has a busy day	4
Apps that track you the most	5
Big Idea 1: Data security	6
Your business is big business	7
Which leads us to cyber crime	8
Cyber criminals love your data. Here's why.	8
How schools get hacked	9
Another way to think about cybersecurity	10
What makes for success in cyber careers?	10
Something for everyone	13
PART 2: HOW THINGS GO WRONG ONLINE...	14
The next, no-good, very awful day	14
Key cyber safety terms	15
The trouble with trust	16
How to spot a phishing attempt	17
Big Idea 2: Establishing trust	18
How to know a website is safe	19
How strong are your passwords?	20
The trust pact	20
The security mindset	22
Watch what you say or send or snap	22
PART 3: CONTROL YOUR RISK ONLINE	24
The day gets better ... eventually	24
People do dumb things	25
Living with online risk	26
Pop quiz	26
Big Idea 3: Risk	28
How the scam worked	29
The world wants you	31
PART 4: EXPLORE A FUTURE IN CYBERSECURITY	32
How they do what they do	32
It's all in how you look at things	33
Is a spot in cyber right for you?	34
Types of cyber jobs	35
Meet some folks in cyber	36
Teach Cyber information	38
National Cryptologic Foundation offerings	39



➔ PART 1: A DAY IN THE LIFE OF YOUR PHONE



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 Words with Friends online with who knows who and asking everyone around the table for help. *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



PHOTOS BY ISTOCKPHOTO.COM UNLESS OTHERWISE INDICATED



APPS THAT TRACK YOU THE MOST



principal about school pictures being taken the next day. Not awesome. Now your mom is really going to care about what clothes you wear.

6:45 PM: After dinner, you put in your ear buds, tee up a new Spotify playlist your sister shared, and search Amazon for new shoelaces to go with the sneakers you bought there last week.

7:50 PM: You sneak in some Netflix before 8 o'clock 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, clothes interests, sense of humor, musical tastes, 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 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.

BIG IDEA 1: Data Security



Data is everywhere. It's all around us, all the time. Keeping it secure, private, and reliably accurate is a crucial challenge for individuals and organizations alike. One aspect of data security is maintaining control over physical access to devices that store data. Another involves virtual access and all the things we need to do to keep digital data safe from bad guys.

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?

To get access to your data stored in computer systems, you typically have to 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.

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. In 2018, companies spent almost \$20 billion on data gathered from our online activities. With data in hand, they find it no trick at all to connect all the dots and get to know us inside and out.

Companies model our behaviors and preferences to **understand** and **predict** what we buy, care about, feel, and do in the real world. Facebook, for example, revealed in 2017 that it could figure out when teens in Australia and New Zealand were feeling “insecure” or “worthless”—findings that the company

then actually shared with advertisers.

Most of the time, companies use online data for understandable business purposes—to improve their services and products, learn more about what we all 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 options for lacing up the sneakers you just bought. We might feel a little creeped out by how well our personal technologies seem to know us, but the effects can sometimes actually be useful.



Which leads us to cyber crime



But. All of those bits and pieces of our digital selves sloshing around online also present **risk**. People with bad intentions are able to misuse our online data and have made **cyber crime big**

business as well. Damages attributed to cyber crime cost billions of dollars every year. Data breaches expose hundreds of millions of online accounts to potentially criminal exploitation. Every



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 fraudu-



HOW SCHOOLS GET HACKED

One of the worst data breaches of any kind struck over 13,000 K-12 schools in 2019. The FBI discovered that hackers had gained access to the personal information of many tens of millions of students through the records of Pearson, a nationwide testing services company. The data included students' names, emails, and dates of birth. Most known breaches of K-12 data happen because of 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. All of the recent increases in online and distance learning—from COVID and other factors—only amplify schools' reliance on these outside companies for materials and technology and learning services. These growing exchanges will expand the "attack surfaces," or vulnerabilities to cyber threats, that K-12 schools are going to have to learn better how to protect.

individual or organization online can be affected. More than 1,000 schools have suffered cyber attacks in recent years, with damage ranging from lost money to leaked data to disrupted operations.

Keeping online data safe from bad actors 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.

Cybersecurity is a **fast-growing 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.

lent 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.

Another way to think about cybersecurity



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.

The bigger job, though, is one that we all have a part in: taking better care of our data to start with. That means understanding what we share about ourselves with companies online and thinking hard about what makes us comfortable.

It means both **demanding that companies take care of our data** in ways that we wish 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 that come our way, and sharing our personal information only with trusted, known entities.

Cybersecurity plus this broader sense of individual responsibility for data add up to a larger idea we're calling "**data care.**" This term describes a sweeping enterprise with many different parts and pieces, all directed towards making sure that online data gets used in appropriate, secure ways. Data care encompasses activities ranging from our **individual online behaviors** to technical cybersecurity measures to the larger sphere of **rules, behaviors, norms, and procedures** that determine how we as a society manage digital data and

HELP WANTED

**Cyber jobs
to fill in 2021:**

3.5 million!


the online experiences associated with it.

You probably understand that health care involves a lot more than just doctors prescribing medicine and fixing broken bones. In fact, your health care starts with you—the food you eat, the sleep you get, the care you take of your body. And that doctor’s office works because of the nurses, assistants, and office workers

who are so good at their jobs. Beyond the doctor’s office, insurance companies manage payments for health care providers; all kinds of companies develop drugs, manufacture medical equipment, and provide medical services; researchers investigate the causes and cures of disease; governments make rules about what all these people should and should not be doing; and much more.



PHOTO BY JOPWELL FROM PEXELS



***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

Just like health care, data care is staggeringly complex and wide-reaching. It involves people with a **huge range of skills, interests, and abilities** performing many different kinds of jobs related to generating, gathering, analyzing, using, and protecting the nearly unimaginable volumes of data that zoom and flash through digital devices and networks. And just like health care, data care 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!**

→ Every time you interact with a company or an app online, you generate 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.

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

→ To be safe online, you need to build strong passwords and stay alert to scams.

→ 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.

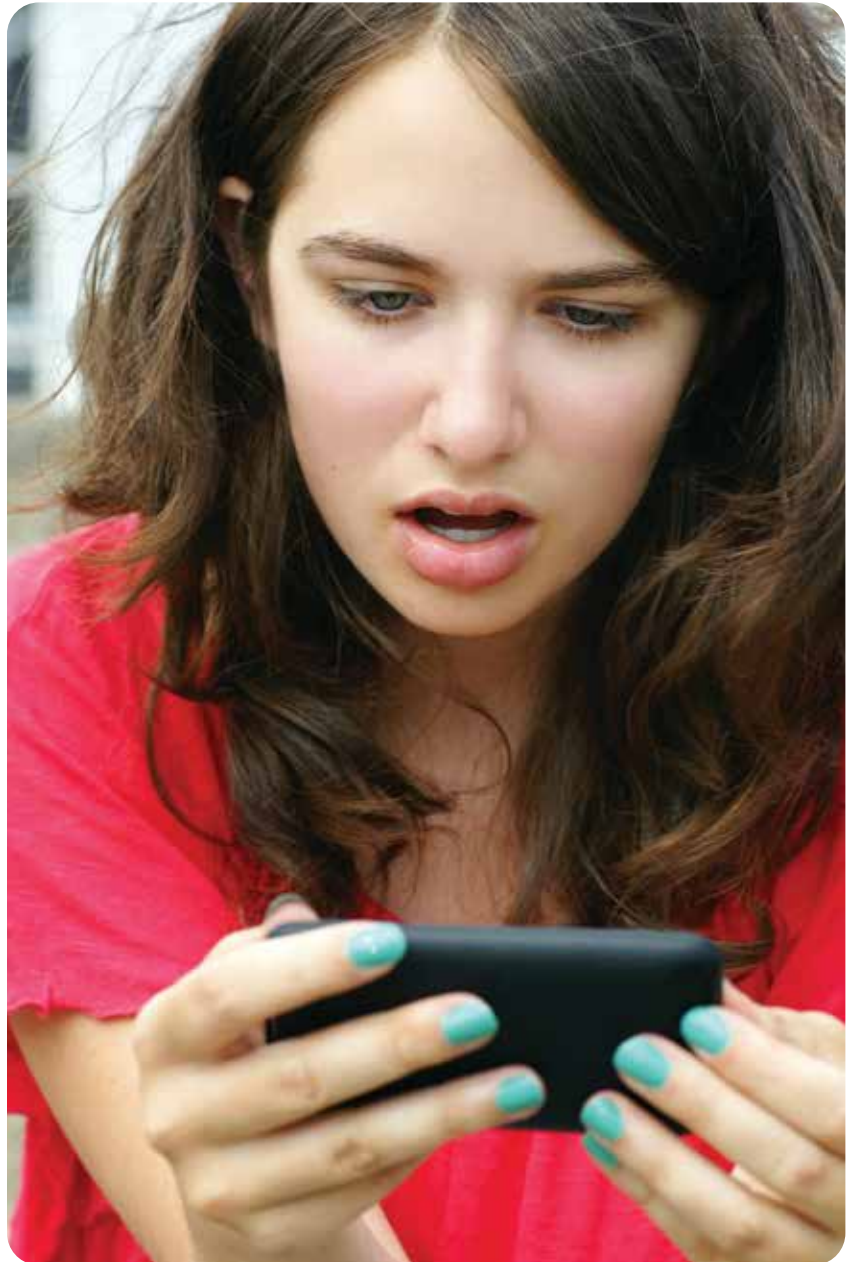


The next, no-good, very awful day

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 have encrypt yours phone and all files are lock down. Loser. Send \$18**



with credit card on this link or you never get to open any phone apps again: <http://tiny.url.com/41s00pNe33>"

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!!

7:18 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



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.



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.



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



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



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.

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 of your friend's contacts and generated the extortionate text. When you clicked on the Space Noodle link inside the text, you downloaded that





HOW TO SPOT A PHISHING ATTEMPT

same malware onto your phone, and **voilà!** 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. As they say, on the internet, nobody knows you're actually a dog. With just a little bit of online "cover," **people can appear as almost anyone they want to be.**



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 from someone 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, is even more elusive and challenging. And we've only just started figuring out how to do it.

Knowing a bogus email when you see one is tricky. The best ones look really convincing, just like lots of other emails in your inbox. 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. But 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.

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



Trust lies at the heart of a robust, reliable system of data care. 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 data care system that meets these three goals AND is easy to use is tricky. Security and usability are always in tension. If you could just put your name into a bank’s website, check your account, and make a withdrawal, anyone who knew your name and where you banked could easily steal all your money.

On the other hand, if checking your balance meant you had to enter a username and strong password, do a retina scan, and answer three security questions, you would probably feel your money was well protected. But what an incredible pain!

Cybersecurity always means making trade-offs between **usability** and **security**. As a user, you should be gauging how well websites protect data you submit: Do passwords have length and character requirements? Does logging in require a one-time code delivered by text to a separate device every time, or “two-factor authentication”? Does the URL start with “https” or just “http”?

Designers of data care 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 that seems squirrely. Remember, the only safe, reliable assumption about online data is that **nothing is ever completely safe**.

How to know a website is safe

Both sides of the person-machine trust pact must do their part. As users of online systems, we all become quickly acquainted with the basic tools used to join 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 people do manage to mess it up all the time. More on that later.

On the machine side, things are much more complicated. Sensitive information should always be encrypted. Have you ever noticed that web addresses begin with either "http" or "https"?

The "s" stands for "secure," meaning your data is encrypted into meaningless gibberish as it moves from you to the machine and back again. And only the machine has the key to translate, or decrypt, the gibberish back into your personal data.





HOW STRONG ARE YOUR PASSWORDS?

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

A password of eight letters can be cracked in about five seconds. Add a few numbers and it takes about a minute.

Cracking simple passwords is child's play even for novice hackers. 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 (more than eight characters). Use numbers, upper- and lower-case letters, and symbols. Avoid personal information. Best of all is to figure out a system you can use to generate, remember, and use passwords. You can even use full sentences or phrases, like "rain, rain, go away" or "my avatar has blue hair." Password managers can also work, as long as you don't forget the main, master password.

Get lots more advice on passwords—and other online safety practices—at StaySafeOnline.org.

The trust pact

Organizations should have 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 all the time!). Machines storing your information should be on, accessible, and physically protected at all times, with backup systems in place for the inevitable hiccups.

Many things can go wrong on both sides of this trust pact, and when they do, 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.** In fact, these exchanges are only “engineered” to seem trustworthy, tricks meant to deceive. Many bad things happen online because

people trust things that are not what they seem. And this trust leads them to do things they should not do.

One of the most common forms of social engineering online is “**phishing,**” which resembles the Space Noodle text. A message arrives pretending to be from someone already familiar to the recipient. It asks for information that



WATCH WHAT YOU SAY OR SEND OR SNAP

Kids love their messaging apps. It's so easy to dash off a what's-up 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 disap-

pear. And it's something private, like a picture that the whole world should definitely NOT be seeing. Teenagers' worst selfie



PART 2 TAKEAWAYS

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. One study found 30 percent of people open phishing emails and 12 percent click on links in them.

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.** The problem is you never know where the next strike will come from. So what do we do?

As a broad principle, assume that all of the networks that store and transmit data are unsafe. If you expect all data

care 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 what role they play 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.

→ 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.

→ 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.



nightmares came true in 2014 when over 100,000 revealing Snapchat messages got hacked, and in short order, thousands of ex-

tremely 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.



The day gets better ... eventually

8:15 AM: All dressed up for pictures, you enter the school, wondering what kind of response you'll get from friends with malware-infected phones.

8:22 AM: After having three phones full of ransom demands in broken English thrust under your nose, accompanied by variations of "yo, 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?"

10:15 AM: By the time you get to morning break, you realize you are one



GETTY IMAGES/ JON FENGERSH PHOTOGRAPHY/INC

of the few people who fell for the school picture hoax. Walking around all day in dressy clothes feels like having a “loser” label stuck to your back.

12:30 PM: 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.

3:45 PM: Your dad is excited about something when you get home. “Hey, look, we can get RayBan sunglasses for \$20 a pair on super sale, today only. I saw a tweet about it.” Your newly sensitized data care antennae tune in right away. “What?! Dad, that sounds totally sketch. They never go on sale. Some random tweet? C’mon!”

3:55 PM: Sure enough, a quick search for “RayBan 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, “Sure thing. 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.



PEOPLE DO DUMB THINGS

In a 2018 visit to the Oval Office, Kanye West took out his phone and entered his passcode to unlock it—in front of a bank of TV cameras broadcasting the event live. Millions of people instantly learned that Kanye’s passcode was “000000,” something so easily guessed and carelessly revealed that you could almost hear the immediate smacking of palms on online security experts’ foreheads all across the country.

In fact, Kanye is far from alone in making bad decisions about online security. An IBM study found that almost all online security breaches—fully 95 percent—resulted from people making mistakes or doing dumb things with access to online data. When the most common password used online is “123456” and the second-most common is “123456789,” it’s easy to imagine how little thought people are putting into taking care of data. Which just goes to show how much safer the internet would be if not for the people who use it!



POP QUIZ!

Time to show what you know! Take this quiz to see how well you can assess risk in real-life scenarios involving personal data.

1. Everybody you know wants a WhatZaDoodle. You find one at <http://www.WtZaDoo4U.com>—and for half of what it costs on Amazon! You rush to put in your parents' credit card info and click the "buy" button. Safe or not? And why?

ANSWER: Not safe! The website address says "http," not "https"; you should assume sensitive information will be exposed because the website does not automatically encrypt online transaction data.

2. You can get a virus on your phone or computer from opening an email. True or False?

ANSWER: False. You must click a link or download an attachment for a virus to infect your device. Even so, if a suspicious email shows up in your inbox, it's best to delete it unopened.

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 have to assess risk and then decide whether or not to do what we have set out to do. For your personal online safety and your career options, 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 degree of damage. Analyzing both of these variables is necessary for assessing the risk of any online data exchange. Sometimes the likelihood might be high but the potential damage not so bad, so you complete the exchange. Putting up a silly picture of yourself 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 damage is serious. 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 chance of damage and the damage itself are too great to complete the transaction, such as with the sunglasses scam.

In all of these instances, **you assess the risk factors in play and then**

make a decision about what action to take. It is exactly this calculation that lies at the heart of nearly every job you can imagine in the professional world of data care.

How data care professionals assess risk depends on the kind of responsibility their jobs give them for taking care of data. You can think of data care jobs as falling in 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 data care 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 data care 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 data care 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 data care careers. People in the logical field study the ways that bad guys use software 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 any and all kinds of cyber attacks.

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. People in this field study and/or try to shape the thought processes, actions, and values we bring to online activities. 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 data care
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, data care 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.



→ 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.

→ Data care 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 data care 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 data care 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,



PHOTO BY FAUXELS FROM PEXELS

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.

The jobs they do are important.

Cyber attacks can cost people, companies, and governments a lot of money. They can also do real damage. In early 2021, hackers broke into the control system of a Florida water treatment plant and started to poison the water supply for a town of about 15,000 people. Alert plant operators stopped the attack and restored the system to safety. News of the attack sparked widespread reviews and improvements of computer systems used to manage water safety programs across the country.

In a data care 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 cyber attacks can help you understand what “keeping our data safe” actually 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. GenCyber, for example, is a summer camp program running on college campuses across the country. Sponsored by the federal government, it’s free to attend! Check out www.gen-cyber.com. And you can learn lots more about the field at the website of the National



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.

MEET SOME FOLKS IN CYBER



Rachel Tobac is a white-hat hacker and the CEO of SocialProof Security, a company that offers social engineering training and consulting for companies and individuals. SocialProof's clients include PayPal, Snapchat, Facebook, the U.S. Air Force, and Uber.



Yonesy Feliciano Nuñez is Chief Information Security Officer at Jack Henry & Associates, a company that handles payments for financial services clients. He has created new tools to keep money and information safe online.

Alissa Abdullah is Deputy Chief Security Officer at Mastercard, one of the largest financial services companies in the world. She worked on security issues in the White House for President Obama and has led numerous efforts to attract girls into the field of cybersecurity.



Diva Hurtado is a product manager at Dashlane and has a background in mobile gaming. She hosts digital self-defense classes for women and others who are disproportionately vulnerable to cyber attacks.

O'Shea Bowens is Founder and CEO of Null Hat Security, a minority-owned business focused on security solutions and outreach to diverse individual and corporate audiences. He started off as a hacker in his early 'teens and kept learning all the way to becoming an in-demand speaker and security consultant.



Chris Krebs was Director of the U.S. Cybersecurity Infrastructure and Security Agency until November 2020. He led the federal government's highly successful efforts to ensure a secure, fair election for president in 2020. He got into cybersecurity after studying environmental science in college and then getting a law degree.

PART 4 TAKEAWAYS

Cryptologic Foundation (www.cryptologicfoundation.org).

Your school will probably offer computer science classes once you get to 9th grade. Take a class or two to learn the basics. While much of the content might be technical, remember that jobs in the field vary widely. Everyone should understand something about computers and networks, but as many or more jobs await you in the “social” and “physical” fields as in the “logical” one.

Protecting the online world is a mission and a challenge that we all share. As more and more of our lives move to the internet, we need to take better care of our data as individuals and as a country. 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. What you need to decide is whether you want to do it. We need people like you, our best and brightest students with a desire to make the world a better place, to help us all lead safer, better lives online.



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

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

→ Cyber attacks can do real damage. In a data care job, you will always be protecting something valuable and important to other people.

→ Learn more about the field by following news of cyber attacks and taking some 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.

This publication is brought to you with grateful support from the Central Maryland Chapter of the AFCEA. Thank you!



AFCEA Central Maryland Chapter (AFCEA-CMD) is a non-profit membership association dedicated to supporting our future leaders in STEM (Science, Technology, Engineering and Mathematics) while building relationships across government, military, industry and academia. We strive to make an impact through our KickStarters (K-12) program, awarding over \$5 million in college scholarships, providing grants to schools, supporting the local intelligence community, and more.

Published by Start Engineering, LLC

CEO: Bob Black

Creative Director: Stacie Harrison

VP, Learning and Communications: Eric Iversen

Illustrations by Huan Tran

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



Advancing the nation's interest in cyber and cryptology through leadership, education, and partnerships.



OUR MISSION

The NCF strengthens trust in the digital ecosystem to ensure democracy and freedom.

We **educate** and engage our citizens to be cyber smart individuals and develop pathways for our future cyber and cryptologic workforce.



We **engage** and convene partners to address emerging cyber and cryptologic issues.



We **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

