

How to be **Cyber Safe + Savvy**

- Gain confidence using your computer and phone.
- Protect your online data.
- Guard against scams, identity theft, and fraud.
- And much more!



WELCOME



NATIONAL CRYPTOLOGIC FOUNDATION
CYBER CENTER FOR EDUCATION & INNOVATION

Dear Reader,

The incidence of cyber hacks to 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? Often the technology that is thrust into our lives is puzzling. You hear your families or other adults talk about cyber hacks 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) was incorporated in 1996 as the National Cryptologic Museum Foundation to support activities, displays, and artifact acquisitions for the National Cryptologic Museum. Over the years, our mission has broadened to include a robust Education Program and to deliver an innovative approach to solving cybersecurity challenges. The NCF strives to heighten public awareness of cryptologic and cyber professions while honoring the people — past, present, and future — whose contributions to our national security protect and make possible our way of life. Our partnership with the National Security Agency is a vital part of our mission and includes our support of the museum. Please visit our website to learn more about our foundation.

We encourage you to read this Data Care Booklet. This resource will help you gain confidence in using your

technical devices, protect your online data, guard against scams, and identity theft and fraud. The booklet is available free of charge on our website: cryptologicfoundation.org.

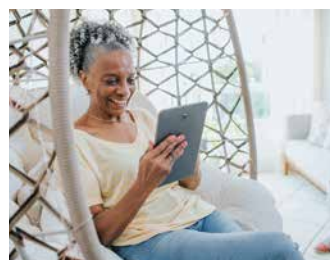
In the pages that follow you will learn the importance of taking care of your data, using devices with confidence, connecting devices with confidence, finding trust in online accounts, and protecting yourself from fraud and scams. Each chapter has summary takeaways and throughout are examples you may follow to help you be cyber safe and savvy!

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

Sincerely,

Laura C. Nelson
President & Chief Executive Officer

TABLE OF CONTENTS



Introduction 4

CHAPTER 1: Using Devices With Confidence 9

- Look how far we've come 10
- We love our devices — most of the time 13
- How to embrace the newness of technology 14
- Tips, tricks to figure out devices 15
- Make a video call on an Apple device 16
- Make a video call on an Android device 18

CHAPTER 2: Connecting Devices With Confidence 21

- Take control of your settings 22
- How to control access to your phone 25
- How to adjust settings on Apple devices 26
- How to adjust settings on Android devices 28
- Why it matters how you connect 30
- The can of worms that is public Wi-Fi 33

CHAPTER 3: Finding Trust in Online Accounts 35

- An internet rife with risk 36
- Look for the "S" 39
- How to build better passwords 40
- Smart password management 42
- The one secret to staying safe online 44

CHAPTER 4: Protecting Yourself From Fraud 47

- Required: A healthy dose of skepticism 48
- Phishing: Don't take the bait 50
- Test your phishing-detection skills 52
- Scams: This time, it's personal 54
- Common scams and how they work 55

Test what you've learned 61

Glossary 63

AN INTRODUCTION TO DATA CARE

Hello and welcome!

Congratulations on taking an important step towards embracing — and enjoying — new technologies and keeping yourself and your data safer as you use the internet.

Every time we share our email address, open an account to buy something online, or post news of a vacation on Facebook, we share revealing data about ourselves and our lives — more data than we ever realize. This data travels farther and wider on the internet than anyone could ever keep track of, so we have to learn how best to take care of this personal data. We have to learn about **data care**.





That's what this book is meant to do: teach you how to understand and manage the ways you share personal data online as you use the internet to shop, communicate with family and friends, manage your household, and keep up with news and events. In short, this book will teach you how to keep yourself and your data safer online. That matters because all the data about individuals circulating online is more than sufficient to build a detailed profile of anyone's identity. That means there's enough information for someone to step into that identity and do bad things to that person or in that person's name. From outright theft of money and goods to identity

fraud, crimes that originate online can leave painful marks in the real world.

Data care is a way forward

Understanding how easily our personal data leaks out of our control while using the internet should make all of us wary about what we do and where we go online. But that knowledge shouldn't keep us from ever venturing online. Instead, it should focus our attention on data care.

After reading this book, you will understand and be able to practice good data care. Just as we should all be active, informed participants in our own health care, we should be continuously

AN INTRODUCTION TO DATA CARE

learning and doing what is possible to take care of our online data. That means understanding how to set up and operate devices; connecting safely to the internet; building and managing strong passwords; and recognizing and avoiding risks that cross our screens. In our online lives, these data care basics will help to protect us from scams, hoaxes, identity theft, fraud, and direct attacks on our digital selves. That's what good data care is all about.

Confidence and trust

To learn and practice good data care habits, you should understand and feel confident about operating personal technology

devices that connect us to the internet. That means everything from phones to computers to smart speakers to digital watches. If you already know about on-device settings and passwords, as well as Wi-Fi and cellular data networks, feel free to skip right to Chapter 3. If not, the first part of this book will help you build confidence in your ability to make your devices do what you want them to do.

Chapter 1, Using Devices With Confidence, explores the numerous types of personal technology devices you can use to go online and provides guidance on how to make them work the way you want them to.





Chapter 2, Connecting Devices With Confidence, addresses how to set up personal technology devices and manage connections to the internet in ways that keep your data as safe as possible.

The second part of this book will help you learn what to trust or NOT trust online. We use the internet to pay bills, go shopping, communicate with friends and family, and consume news and entertainment. At each turn, we must assess the trustworthiness of what appears on the screen in front of us. Unfortunately, these online experiences do not come with Good Housekeeping seals of approval. We ourselves must learn how to tell the differences

AN INTRODUCTION TO DATA CARE

between what we can trust online and what we cannot.

Chapter 3, Finding Trust in Online Accounts, examines how to take care of the data we necessarily share through online accounts, focusing on building and maintaining strong passwords, conducting secure online exchanges, and making clear-eyed assessments of risk.

Chapter 4, Protecting Yourself From Fraud, considers how to find trust in the online tools we use to communicate with friends and family as well as to find news, entertainment, and information about the world. Convenient and engaging, these tools

can also be used to mislead and deceive. Proper data care habits should include vigilant monitoring not only of the information that we transmit but also of the information we receive and consume.

A few advanced sections

At spots in the book, we will dig deeper into the “nitty-gritty” of data care, providing more detailed, technical information about some of the topics under discussion. Look for the little shovel icons that show up in the margins to identify this kind of material. This information goes beyond the fundamental lessons of data care, and you can skip it with no con-



cerns over missing anything. And if you ever want to return to the book to learn more, the information will be there waiting for you.

A simple, regular habit

Good data care can become a simple, regular habit, as normal and natural as looking both ways to cross the street, locking the front door, and taking other routine measures to stay safe in a sometimes risky world. With guidance and practice, starting with this book and continuing into your everyday life, you can learn and apply all the best data care practices you need to stay safer in both your online and real-world lives.

CHAPTER 1

Using Devices With Confidence

- Overcome frustrations with your devices.
- See why data care matters so much.
- Learn how to make a video call.



"About this 'smart phone' I wished for. My second wish is that you show me how to use it."

Look How Far We've Come

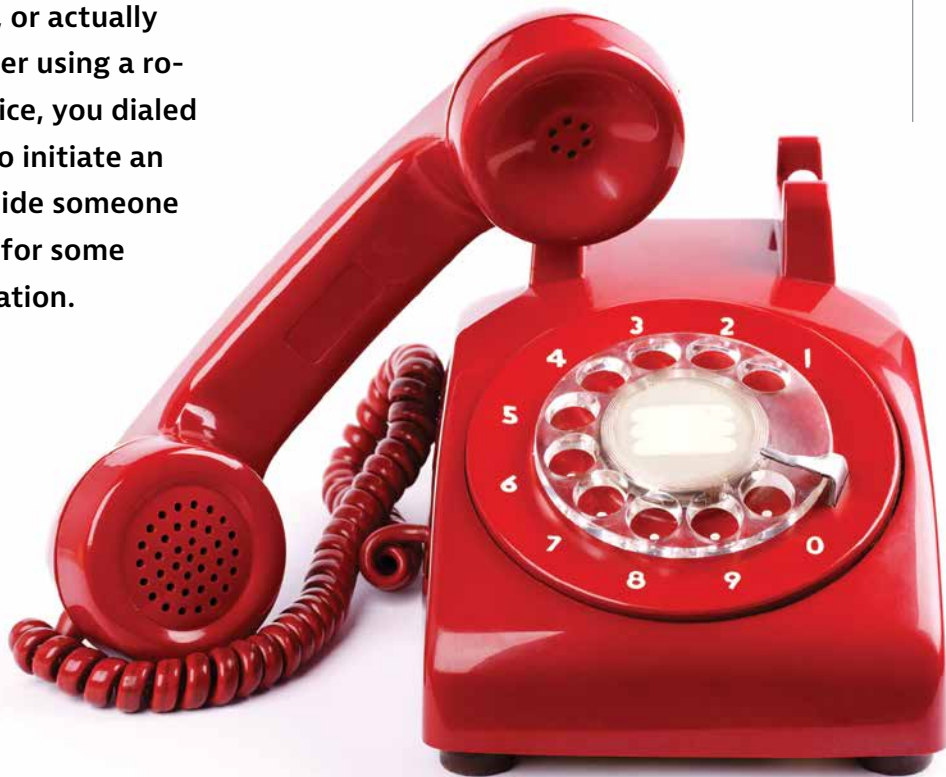
Remember the dial tone? It was great. You picked up the phone, heard a quick click, then a steady hum, and you had one thing to do — dial a number, or actually seven numbers. Whether using a rotary or touch-tone device, you dialed those seven numbers to initiate an insistent ring-a-ling inside someone else's house, a request for some time to have a conversation.

Then at the end of the conversation, you just put the hand-set back in the cradle, automatically terminating the connection, and went on with your day. The phone,

as well as the line into your house that connected it to the network, served just one purpose: to enable you to make a phone call to someone

else who also had a phone in their house. One device, one purpose, with a dedicated channel for making it all work. This is how most of our home technology devices worked in pre-internet days. Televisions brought sitcoms, sports, and movies into our houses with antennas that captured Very High Frequency and Ultra High Frequency radio waves. Radios delivered sound by capturing waves from a different part of the electromagnetic spectrum.

These communications technologies were "dumb," with data traveling just one way: inbound. Other home technologies were even "dumber," not taking in data at all, just power. Think stereo



equipment, refrigerators, doorbells, and so on. The rule of one function per single, one-way device kept things simple and largely contained within our homes. We watched TV, vacuumed the carpet, and set an indoor temperature using devices dedicated uniquely to these functions. Nobody else knew when and how we did these things unless we wanted them to know.

Times change ... constantly

Of course, things have changed. Take phones, for example. We still use them to make phone calls. But we also use them for written communications, such as emails or text messages. We use them to listen to music, watch movies, sports, and TV shows, monitor our health, manage our finances, play games, and buy things in stores. We can also do a lot of these things on home computers, tablets, even our watches. To be sure, we did all of the same things before the internet and



multiple computing devices pervaded our homes; we just did them all individually. And now we also do things we never even imagined doing before the internet: use social media, record and share images and videos from almost anywhere we go, and constantly transmit our geographical location to

the ever-watchful cell towers sited within a few miles of almost every street corner in the country.

Creating data 24/7

Wait, what? The internet knows where we are when we use our phones? And other connected devices? Yes it does,

CHAPTER 1: Using Devices With Confidence

to within about 15 feet of our precise location under an open sky. And it knows much, much more. Depending on what you are doing on your phone or with any other connected device, you are sharing information about your identity, age, household, clothing or entertainment preferences, finances, housekeeping habits, and any number of other behaviors or traits you might have assumed were private.

Welcome to "data care"

The personal data we generate and share just by using the internet can tell the world vastly more about who we are, what we do, and how we do it than almost anyone realizes. That is why good data care is so important, starting with learning how the flow of online data works and what it tells the world about us. These technologies can do wonderful things to make our lives easier, safer, more fun and interesting, and just plain better. But at



the same time, they open us up to uncertainties and risks that we might never imagine in both our online and real-world lives. Learning about and practicing proper data care has become a basic requirement of modern life, as important as locking our front doors, driving safely, and taking care of our health.

Control what you can

Data care involves learning about and managing all the points of control you have over your personal data. That means understanding how data originates with your personal technology

devices, runs through all of your on-line accounts and activities, and ends up filed in databases that companies and governments use to store information and behaviors associated with the way we use the internet. In this book, you will learn the basic lessons of data care that you need to keep yourself and your data as safe as you can — out of the hands of criminals, away from prying eyes, and accessible only to you and the people you want to see it.

Building confidence

The first step in good data care is gaining confidence in operating the many devices we use to go online. Managing electronic devices can be challenging for all kinds of reasons, even to the point of making us want to shy away from using them (see the next page). Some time, effort, and the right kind of support can help you break through these challenges.

WE LOVE OUR DEVICES — MOST OF THE TIME

1. NEW FEATURES ARE GREAT, ONCE YOU LEARN THEM.

Phones, tablets, and computers can do more and more things all the time. Keeping up with all these changes is a constant learning process, but the payoffs can really make life easier!

2. KEEP TRYING, YOU'LL GET IT.

Sometimes even seeing and using the buttons and controls on a device is challenging. But you can change the device settings to make things easier — see page 26 for more.

3. CONNECTIONS CAN BE ANNOYING, BUT THEY WORK MOST OF THE TIME.

“Can you hear me now?” It’s no accident that Verizon, AT&T, and T-Mobile still make network reliability a central plank of their advertising. Because not one of them is completely reliable. And wired internet

connections work best and most affordably in population centers, which is unfortunate for much of rural America. If you’re having trouble connecting, try turning off your device and then restarting it. Sometimes this simple act is the most effective!

4. GET HELP IF YOU NEED IT.

Using a smartphone is different from using a laptop or an Alexa—let alone making a home Wi-Fi network run properly, which can stump even the electrical engineers among us. But you can get

professional tech support even at home — just search Google for “home tech support near me” to find a service in your area.



CHAPTER 1: Using Devices With Confidence

HOW TO EMBRACE THE NEWNESS OF TECHNOLOGY

Keeping up with these technological changes will take more of the learning and adjusting and coping that we have all had to manage in these recent

years. But proper data care requires us to keep up with the new technologies that connect our online and offline lives. It's easy — but not necessary! — to feel

overwhelmed. The first step towards gaining confidence with personal technology is to change the story we tell ourselves about it.

"I'll never learn how to use this phone because I'm bad at technology and it's all just beyond me."

STOP!
Blame the technology, not yourself.

Change comes fast to technology, and keeping up with how to use it is hard — for almost everyone. The "I'm bad at technology" story we tell ourselves comes, in part, from a widely advertised image of technology as wonderful, liberating, exciting, and life-altering. So those of us who don't "get" technology in this way must be to blame, not the devices themselves.

But designing devices that are bigger and faster does not equate to making them easy to use. Instructions can be confusing, controls hard to operate, and terminology mystifying. Recognizing these facts can point us towards a different story about technology and how we use it.

"I just don't understand how to use this thing."

STOP!
Add the word "yet" to your thinking.

"Yet" is a word with superpowers. Adding "yet" to a thought like this points us towards change and growth, a future different from the present and defined by our choices and efforts. What once seemed like a dead end becomes just a bump in the road.

**“Kids these days
get this stuff
much better than
I ever will.”**

STOP!

Instead, say to yourself, “I’m going to ask my niece about this phone; she has the same kind.” Actions build confidence. Finishing up with a possible solution empowers us to act. Aligning technology choices with those of our family and friends means we have built-in support for those halting first steps we take with every new piece of home computing equipment. Instructions and online support help, too, of course, but there’s often no substitute for solving a problem side-by-side with someone we know and trust.

TIPS, TRICKS TO FIGURE OUT DEVICES

- 1** Online support is almost always available and more detailed than the instructions that come in the box.
- 2** Check out YouTube for videos showing how to operate a new device. There’s a reason the site is ranked #2 in the most-used search engines.
- 3** Give up the fear of breaking something. It’s almost impossible to damage a device by pressing buttons and just trying things out. Simply exploring a device can help you understand how it works.



CHAPTER 1: Using Devices With Confidence

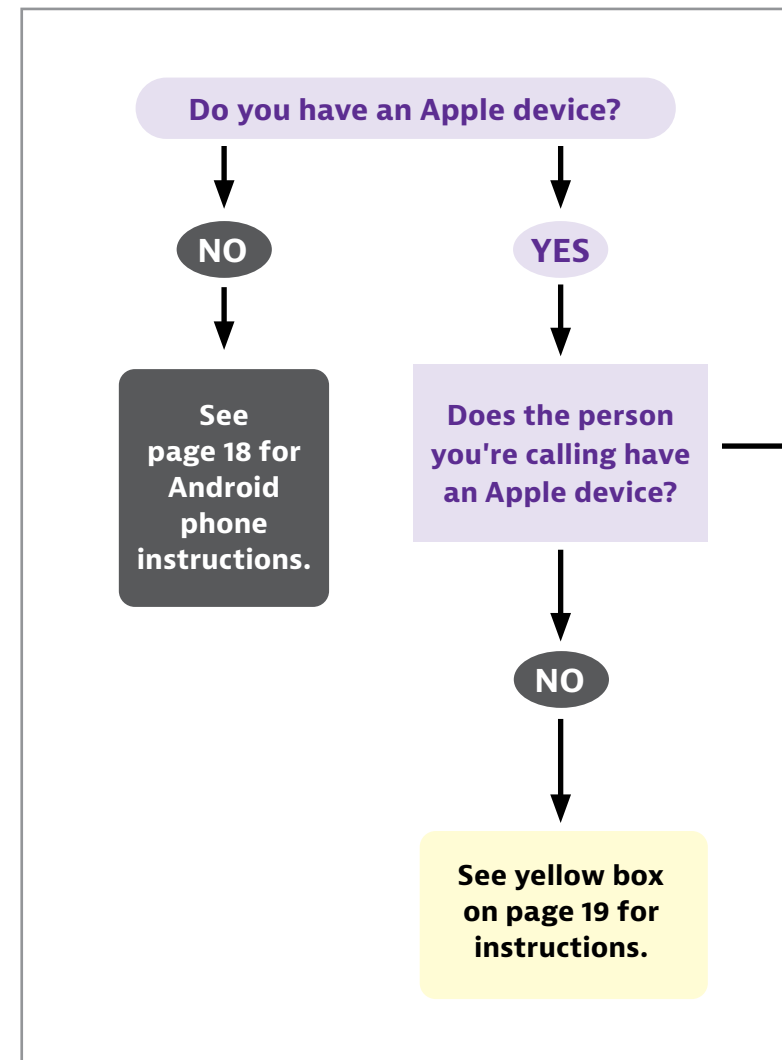
TRY IT YOURSELF: MAKE A VIDEO CALL ON AN APPLE DEVICE

The beauty of today's phones is the ability to see who you are talking to! Not only that, you can see what they are seeing. You can watch your granddaughter take her first steps or play in her first basketball game. From your home, you can go shopping for a couch with your son in the store, using the camera on his phone. There are many different ways to make a video call, and you're sure to find one that works for you. As with most things, the more you try it, the easier it will get. With video calls, it's best to plan the call with the recipient ahead of time so as not to catch folks unaware.

BEFORE YOU GET STARTED

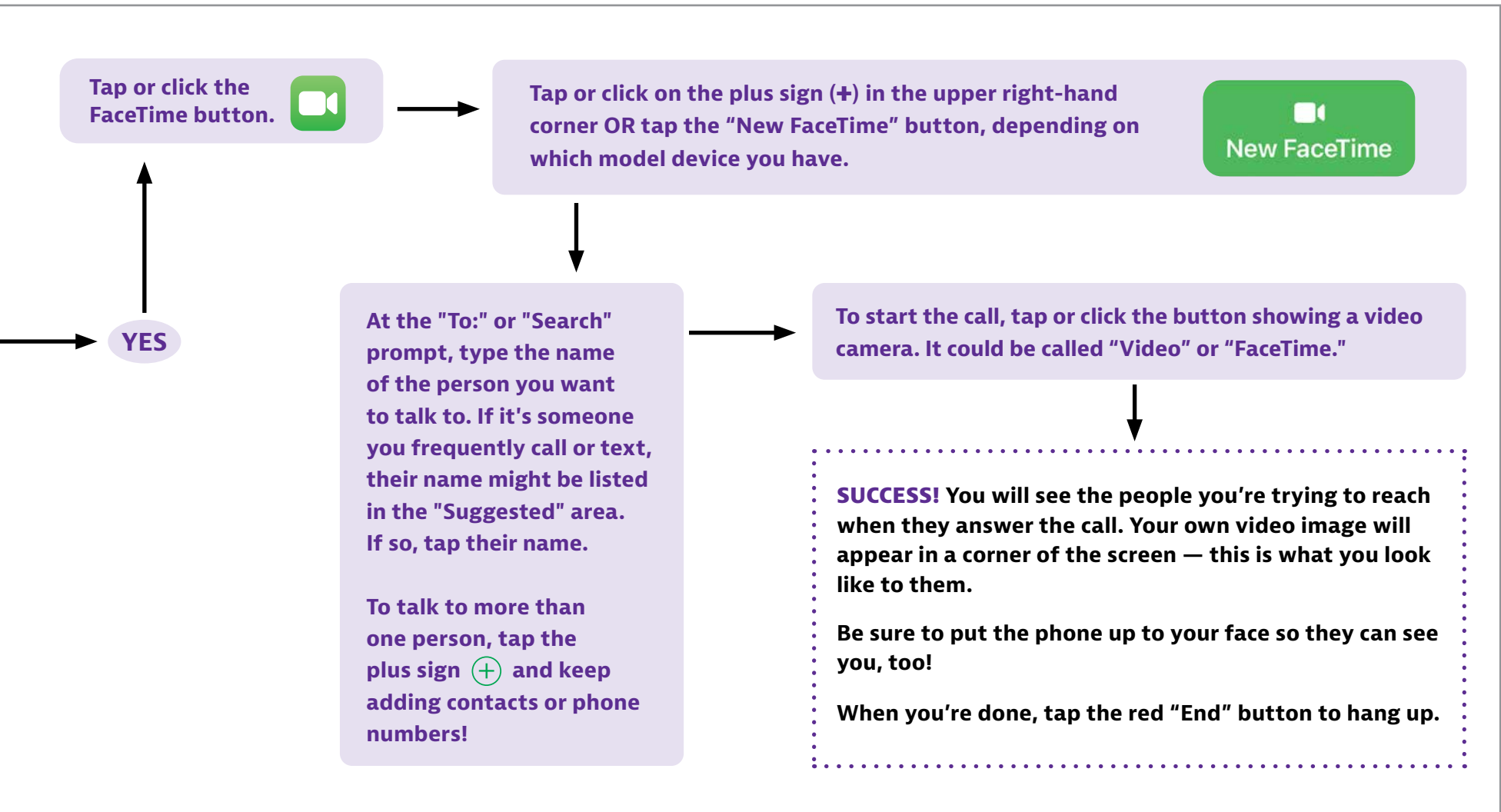
Most Apple computers and phones produced in the last 10 years or so can make FaceTime video calls. To make a call, you must:

- Be connected to the internet.
- Be signed in to FaceTime with your Apple ID. If you don't have an Apple ID, go to <https://appleid.apple.com/> to sign up for one for free.
- Have a built-in or connected microphone, and a built-in or connected camera.
- Be calling someone who also has FaceTime installed on their device.





A DEEPER DIVE



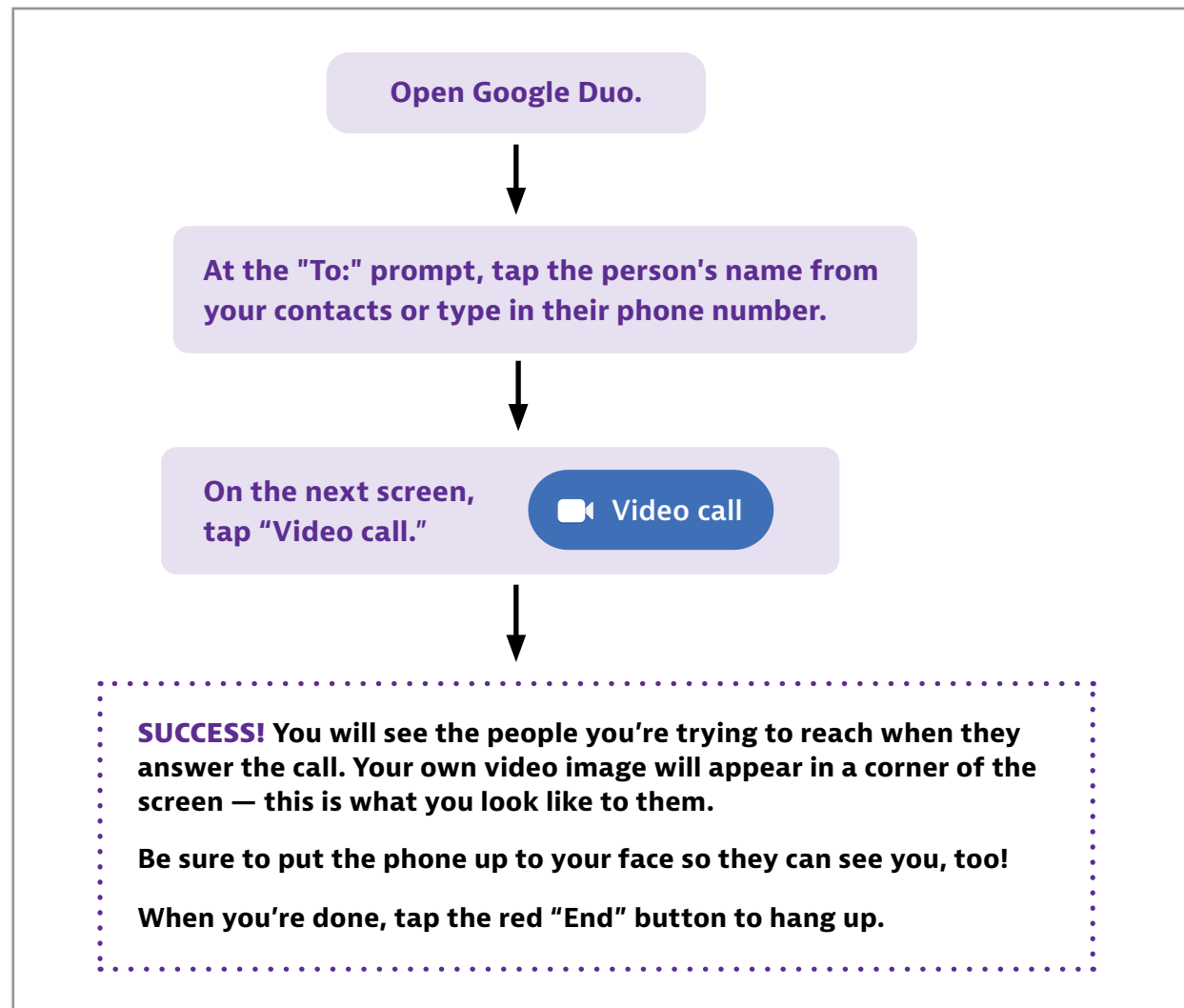
CHAPTER 1: Using Devices With Confidence

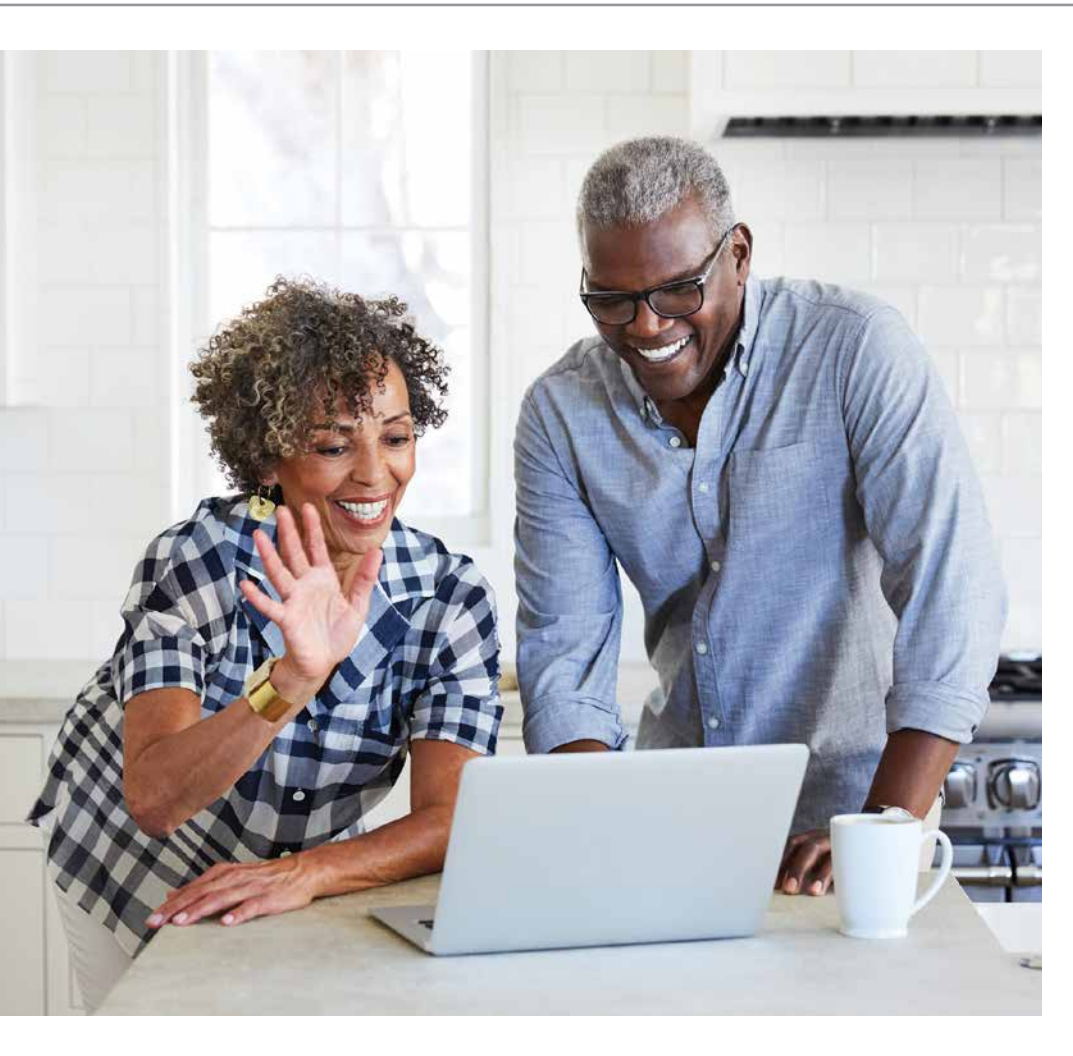
TRY IT YOURSELF: MAKE A VIDEO CALL ON AN ANDROID DEVICE

There are fewer steps to make a video call on an Android device, and it doesn't matter if the person you are calling has an Android or Apple device. As with most things, the more you try it, the easier it will get. With video calls, it's best to plan the call with the recipient ahead of time so as not to catch folks unaware.

BEFORE YOU GET STARTED

- Make sure you have the latest version of the Duo app. You can download it at <https://duo.google.com/>
- Make sure Duo has access to your camera, microphone and contacts. You can do this in Settings.
- Be sure you have updated your operating system recently.
- Be connected to the internet.
- Have a built-in or connected microphone, and a built-in or connected camera.





How to Make a FaceTime Call From an iPhone to an Android Phone

If you have a newer iPhone (XR, XS, 11, 12 or 13), you can make a FaceTime call to someone with an Android phone. But your iPhone must be updated to iOS 15.

1. Go to the FaceTime app.
2. If you're not signed in yet, you'll be prompted to do so. Input your Apple ID and password.
3. Click on "Create a Link." If you like, you can name the FaceTime link by clicking on "Add Name" and typing in your preferred title. Tap "OK."
4. Tap on "Share Link."
5. Click on "Join" and wait for your Android friend to join the call.

Of course, it's best to plan ahead and schedule a FaceTime call with your Android participant so that they can join you on the call at an agreed-upon time.

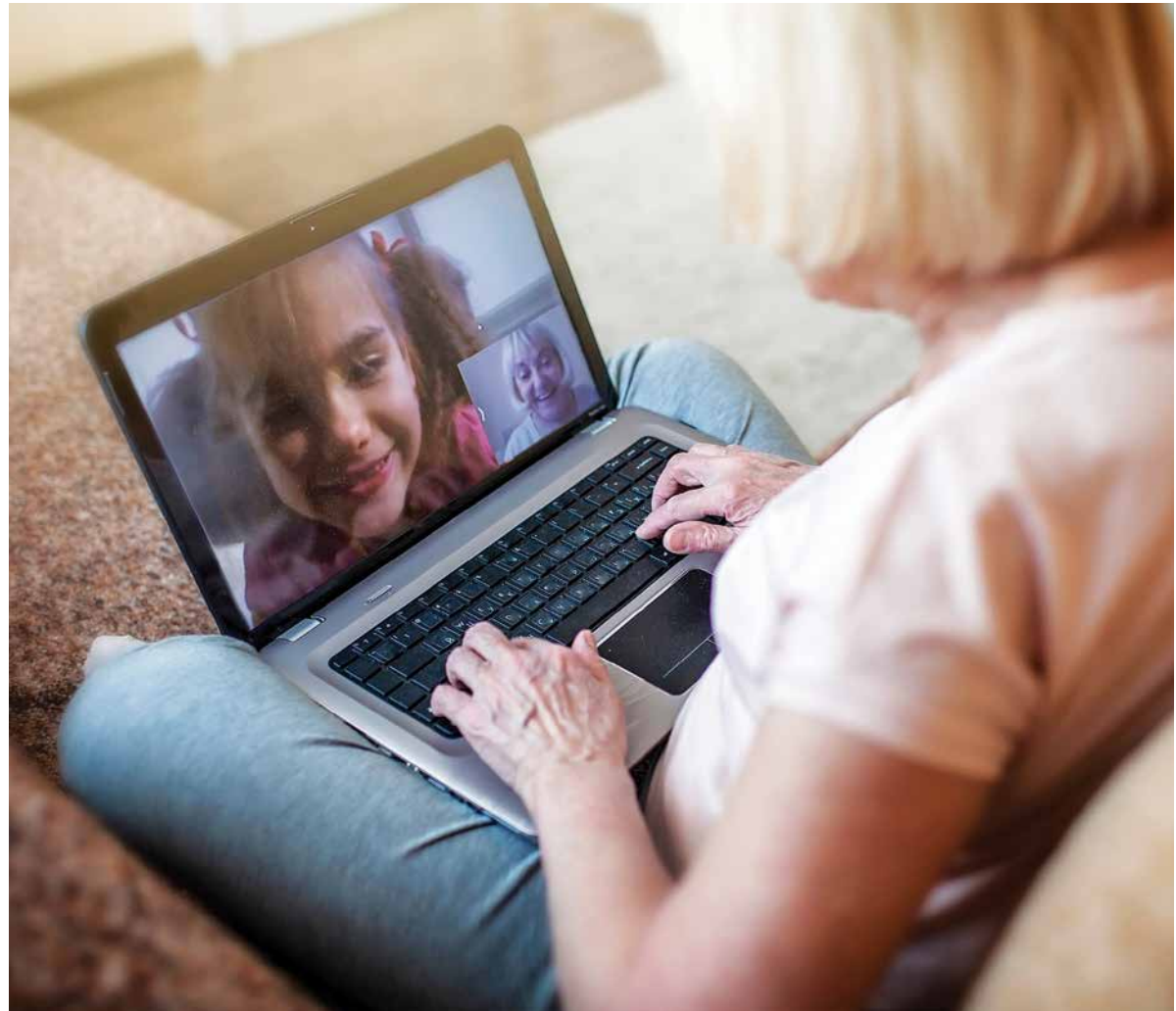
CHAPTER 1: Using Devices With Confidence

CHAPTER 1 TAKEAWAYS

1 We've come a long way since the rotary telephone. But for all the different personal technologies we use now, connecting with family, friends, and others over the "phone" remains a basic need.

2 Help with personal technologies is often there for the asking — from the store, from searching online, or from family members and friends.

3 Every time we go online, we share pieces of personal information, whether we mean to or not. "Data care" means taking appropriate steps to understand where our information goes and to keep it as safe as possible.



CHAPTER 2

Connecting Devices With Confidence

- Learn how to adjust your phone settings.
- Find safe ways to go online.
- Understand the perils of public Wi-Fi.



"Go into Setting, Privacy, Activity Controls, Web Activity, Manage Activity, and deselect Giant Snake."

Take Control of Your Settings

The devices we use now to communicate are different from that old rotary phone. They offer a huge range of choices for how we can produce, share, and store data. The good news is that all these choices give us control over what data we disclose when we go online. The challenge lies in making sense of these options, especially since instructions for how to do so can be scarce.

Get to know your settings

Take control of your data online in the “Settings” section of your device’s main menu. Settings are the controls for managing the operations and connections our devices can execute. Learning about on-device settings will make you ready to understand and

put to use the lessons in data care that follow with regard to connections, online accounts, and digital media.

Adjust the default settings

Every internet-connected device generates and transmits personal data derived from what we do and where we go online. You can choose to share more or less of this data by adjusting the settings that determine how a device interacts with apps loaded onto the device, as well as online networks available for connection. In almost every case, the “default” settings — how devices are set up to work when you take them out of the box

— enable sharing more data about our private lives and online choices than the devices require to work properly.

Since smartphones account for more than half of all web traffic, we will fo-

cus on settings for these devices. The terms and choices you will learn as you arrange settings on your smartphone, though, resemble those associated with computers, watches, smart speakers, and even internet-connected home appliances. Acquiring command of settings choices on a smartphone should give you confidence to delve into settings on these other devices as well.



APPLE DEVICE
SETTINGS ICON



ANDROID DEVICE
SETTINGS ICON



CHAPTER 2: Connecting Devices With Confidence

Start with passwords

The first and perhaps most important setting to consider on your phone is the one that controls who can unlock it. Depending on the kind of device you have, this setting might be called a “passcode,” “password,” “PIN,” “Touch ID,” “Face ID,” “fingerprint,” or something else along these lines. Whatever the term, the security principles in play extend to larger discussions of passwords that will come later in the book. For now, be sure to choose a strong, unique password for your device that you can easily remember, then keep it to yourself. This approach is the foundation for building and maintaining effective passwords for online accounts, as we will see in chapters 3 and 4.

In our real-life relationships, we put time, thought, effort, and feeling into assessing how much we can trust other people with information and objects

near and dear to us. With machines, the lines of communication and exchange are much more constrained. Alexa and Siri, for example, can quickly become unsatisfying partners in con-

versation when topics go beyond driving directions, requests to play music, or questions about the weather. To establish ourselves as “trustworthy” to computers, we use passwords to



verify that we are, in fact, who we say we are. Phones offer various approaches to password-like operations, but in all cases, they serve to “authenticate” our identity as an approved user of the device. On a phone, an authenticated user is typically “authorized” to access and manipulate all operations and data areas. With online accounts, questions of “authorization” get more complicated, but more about that later.

In the sections on the next pages, you will find more detailed instructions for security settings on Apple and Android phones. In any instance, be sure that passwords for your devices follow the basic rules vital to all passwords: Make them hard to guess, unique to each device, and known only to you. See chapter 3 for more information on how to build a strong password.

HOW TO CONTROL ACCESS TO YOUR PHONE

iPhone users

You might have set up access controls on your phone when you first got it. Even so, you can review them at any time to make changes or just explore the options more fully. First, go to “Settings” and scroll down until you see the word “Passcode.” It might say “Touch ID” or “Face ID” first. Then, you will be asked to enter your passcode. Once into the passcode settings, you will find many options for using security controls on apps and other phone operations, including changing your passcode. One choice involves using a password that uses four or six characters. As with passwords used for online accounts, longer means safer. So, at a minimum, set your phone’s passcode to the six-character option.

Android phone users

Android devices offer several levels of settings to control access to your phone. You will typically find them in the “Lock screen” page, which leads you to “Screen lock” options for deciding what level of security you wish to use. Newer phones can use fingerprints to authenticate your identity, which is safer than the more familiar pattern tracing, PIN, and password options. Note that facial recognition technology on Android phones does not offer the same kind of security or convenience as Face ID does on Apple phones, so it might not be the best choice for device security.

CHAPTER 2: Connecting Devices With Confidence

HOW TO ADJUST SETTINGS ON APPLE DEVICES

Look for a gray, gear-like object against a black background on your Apple phone screen to get access to Settings. Or just look for the word “Settings” (or “System Preferences” on a computer).

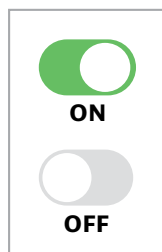


SETTINGS

Swipe down a couple of screen lengths to find the Privacy tab and click on it. With almost all the settings described below, a toggle switch in green means on and gray means off.



PRIVACY



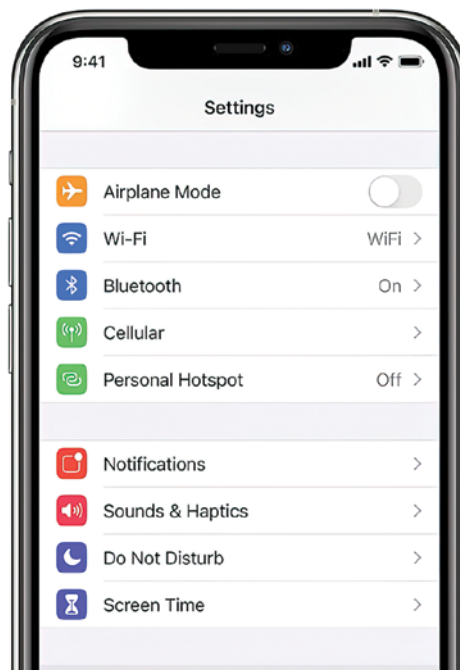
Once you are on the main Privacy screen:

1. Disable ad tracking.

Not only does ad tracking allow companies to gather large volumes of data about what you do online, it also allows them to sell this data to other companies. Turn this off now.

Here's how:

- **Settings** →
- **Privacy** →
- **Tracking** →
- **Allow Apps to Request to Track** (turn off so green button is white)



2. Restrict access to Location Services.

Think about how much where you go reveals about who you are, as you visit doctors, go in and out of stores, and take other kinds of trips out and about in the world. You can choose how much to share about your location for each app on your phone by clicking on **Location Services** and selecting among:

- Never
- Ask Next Time or When I Share
- While Using the App
- Always.

Some apps have legitimate need of your location data; many more do not. You can control them.

Here's how:

- **Settings** →
- **Privacy** →
- **Location Services** (choose an option that seems right)

3. Restrict access to other phone functions and tools.

After you settle on appropriate degrees of sharing Location Services, repeat the same exercise for **Contacts, Calendars, Reminders,** and so on down the list of other settings on this page. Turn off access for any apps that do not seem to need the type of information in question. When in doubt, turn things off more aggressively than less; you can always go back and ease up on things later.

Here's how:

- **Settings** →
- **Privacy** →
- **Contacts / Calendars / Reminders, etc.**

4. Reduce the amount of information you share while using a web browser.

Safari is the best browser for mobile use because it allows the greatest number of privacy choices. You can change the default search engine from the data sieve that is Google to something more private, like DuckDuckGo.

Here's how:

- **Settings** →
- **Safari** → **Search Engine**
(select DuckDuckGo for privacy)



5. Keep your web activity to yourself.

Prevent sites from cross-tracking where you go online.

- **Settings** →
- **Safari** →
- **Prevent Cross-Tracking**

Now, hide your IP address from trackers.

- **Settings** →
- **Safari** →
- **Hide IP Address** →
- **From Trackers**

Next, add an ad blocker to your phone as an extension from the App Store. There are many effective options, several of which are free (such as Ka-Block!) Choose the one you want and add it to Safari.

- **Settings** →
- **Safari** →
- **Extensions (under General)**

CHAPTER 2: Connecting Devices With Confidence

HOW TO ADJUST SETTINGS ON ANDROID DEVICES

Make your way to the All Apps screen on your phone and locate the single gear or cog wheel icon with the word “Settings” underneath. A short distance down the screen you will find the Privacy option. Inside this function you will be able to manage choices to do with how your phone shares data. So now:



SETTINGS

1. Review how apps access the rest of your phone.

The Permissions Manager is a tool for reviewing and determining what apps can see and do with other tools on your phone. Review each app and decide which options make sense for which apps, based on what they actually do.

Here's how:

- **Settings** →
- **Privacy** →
- **Permissions Manager**

2. Keep your lock screen free of private information.

Unless you restrict “sensitive notifications,” your phone will display them on your lock screen. Keep emails and texts about private subjects private.

Here's how:

- **Settings** →
- **Notifications** →
- **Sensitive notifications**

How ad trackers work



Think of an ad tracker as an invisible screen placed on top of a web page displayed on your device. Whenever you load the page or click anywhere on it, the tracker records your action — and possibly informa-


tion about your computer, physical location, other website visits, and more — for delivery to the company that placed the ad. Such personal data is often sold and resold among other advertising and marketing



3. Make sure your phone encrypts the data it stores while locked.

Most newer phones will automatically do this; older phones might not. Turning on this function can take a long time, though, so do it only when you will not be using your phone for a while. Tap “Encrypt phone” at the end of the sequence below if the option is available.

- **Settings** →
- **Security** →
- **Advanced** →
- **Encryption and Credentials**



companies to build ever-more-detailed pictures of who we all are as internet users. Take advantage of the blocking tools built into newer phones and computers to make your online tracks invisible to these prying eyes.

4. Choose a browser other than Chrome.

Since Android is a Google product, most every phone using Android as an operating system comes with the Google web browser, Chrome, already installed. And since Google makes its money by gathering online data from users, Chrome is designed to vacuum up all the user data it can to enable Google to serve up personalized ads to online users. Using any other web browser will help reduce the volume of data leaking out of your online comings and goings. You can limit the data that Chrome gathers and shares, though, from inside the program.

- **Open up Chrome**
- **Tap the three-dot menu next to the address bar**
- **Settings** →
- **Privacy and Security** →
- **Do Not Track / Always use secure connections**

CHAPTER 2: Connecting Devices With Confidence

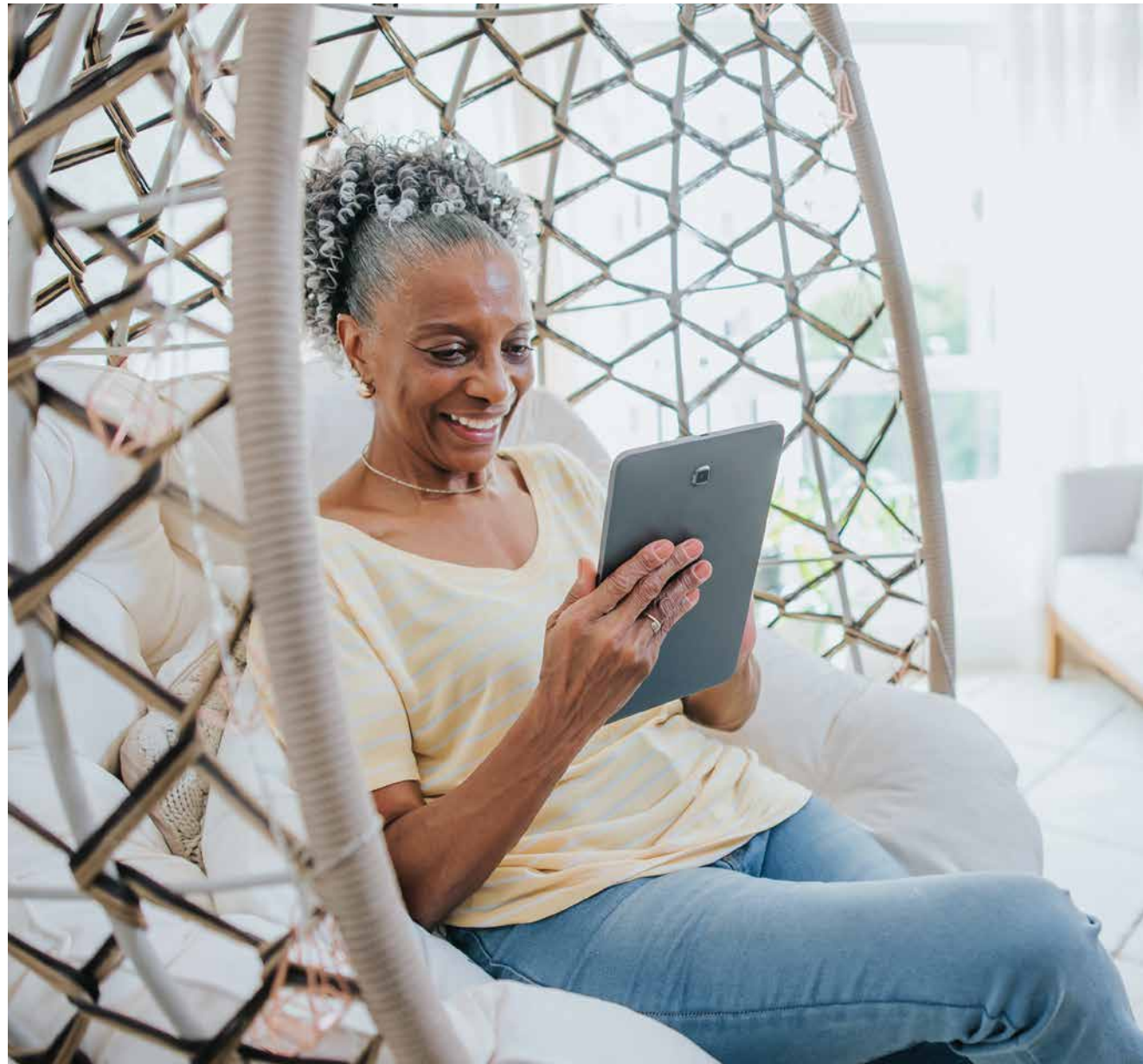
WHY IT MATTERS HOW YOU CONNECT

Now that you have learned about the volume and types of data your devices are sharing when connected to the internet, let's learn more about the connections themselves. The next part of this chapter will explore several kinds of online connections and the different levels of security they can provide — and they can be very different. Depending on how your device connects to the internet, you can feel almost completely confident that your data is being protected or almost certain that it is not being protected at all.

What is the most secure internet connection available?

Cellular data networks, meaning the connection on your phone.

THE NITTY-GRITTY: The connection between your phone and its cellular data network is among the most se-





secure links to the digital world. Data is encrypted and your identity is authenticated and protected, with all operations performed automatically by the network. Most phones run on networks with high levels of built-in security.

What about my computer's connection at home?

A wired connection to the internet is best ...

THE NITTY-GRITTY: The internet reaches you through a wire coming into your house that plugs into a modem that then plugs into a computer. The modem “translates” the outside, electrical signal into digitized information your computer can read and use to interact with other online digital devices. However, modems serve as relay stations, not protections, for data. Any built-in security in this ar-

range originates with the larger network of your Internet Service Provider, or ISP. Some do a better job than others of protecting data.

... But a home Wi-Fi network protected with a password is also good.

THE NITTY-GRITTY: Your home Wi-Fi network works much like a wired network, except a router sits between the modem and your devices. The router broadcasts a wireless signal that wireless-enabled devices can use to connect to the internet. The signal then goes back through the same wires that you use with a wired home connection. Using a security system called Wi-Fi Protected Access, or WPA, the router requires users to enter a Network Key, or password, to join the small wireless network it creates. The name of your home network, or

CHAPTER 2: Connecting Devices With Confidence

WHY IT MATTERS HOW YOU CONNECT (CONTINUED)

SSID (which stands for Service Set Identifier), and the password are found on a sticker somewhere on the router itself. Break-ins are rare but possible, either through a hack of the router itself or someone copying the SSID and Network Key information from the sticker and then logging on.

What if I need to connect to the internet away from home and don't want to use up data?

It's okay to use a public Wi-Fi network as long as it's protected with a password, but don't do any banking, shopping, or other activity that requires accessing personal data.

THE NITTY-GRITTY: Just as with your home router, the risk with password-protected Wi-Fi networks in public is a hack of the software inside a router. Router software attacks can take



many forms, but they all make data going through the router vulnerable to capture and exploitation. Especially appealing to hackers are routers in locations with the most users. Besides the risk of someone watching over your shoulder, this vulnerability is why you should avoid conducting personal business over a public Wi-Fi network, even if it features password protection.

What about public Wi-Fi that doesn't ask for a password?

Never use public Wi-Fi networks without any password protection.

THE NITTY-GRITTY: These networks are basically public data fountains. You can assume that any traffic going through an unsecured public Wi-Fi network is at risk. The National Security Agency, for example, warns, "Data sent over public Wi-Fi — especially open public Wi-Fi that does not require a password to access — is vulnerable to theft or manipulation." It goes on to use the word "malicious" three more times to describe the kinds of bad things that can happen on these networks. Avoid these networks if at all possible by turning off your Wi-Fi connection and just using your phone's cellular data connection to access online content.

A word about Virtual Private Networks, or VPNs.



A Virtual Private Network is an app or piece of software that sits on your device and encrypts, or otherwise makes unreadable, data going between it and an ISP. It can protect data in an environment such as an unsecure public Wi-Fi network — or not so much. VPN providers can retain records of your data, and some sell this data to third parties. In addition, using a VPN can reduce the speed at which your phone loads data. VPNs are most commonly used by people who travel a lot for business, with their company taking responsibility for managing and mitigating any security risks. In the hands of security professionals, VPNs can do good work. For the rest of us, the value might not be there.

The Can of Worms That Is Public Wi-Fi

→ Joining an unprotected public Wi-Fi network potentially opens us up to really bad stuff. Malicious, copycat networks are rife in places such as airports, hotels, and the food court. If you are checking your email in the lobby, do you connect to “MarriottGuest” or to “GuestAtMarriott”? Once you’re on the wrong network, hackers can redirect your data to fake websites — ones that imitate banks’ websites, for example — and trick you into divulging sensitive information.

→ You should use only password-protected public Wi-Fi networks or your phone’s cellular network. If that’s impossible, however, trust only websites that begin with “https” (the “s” is for “secure”), avoid downloading or clicking on anything remotely weird, and keep personal data off your screen.



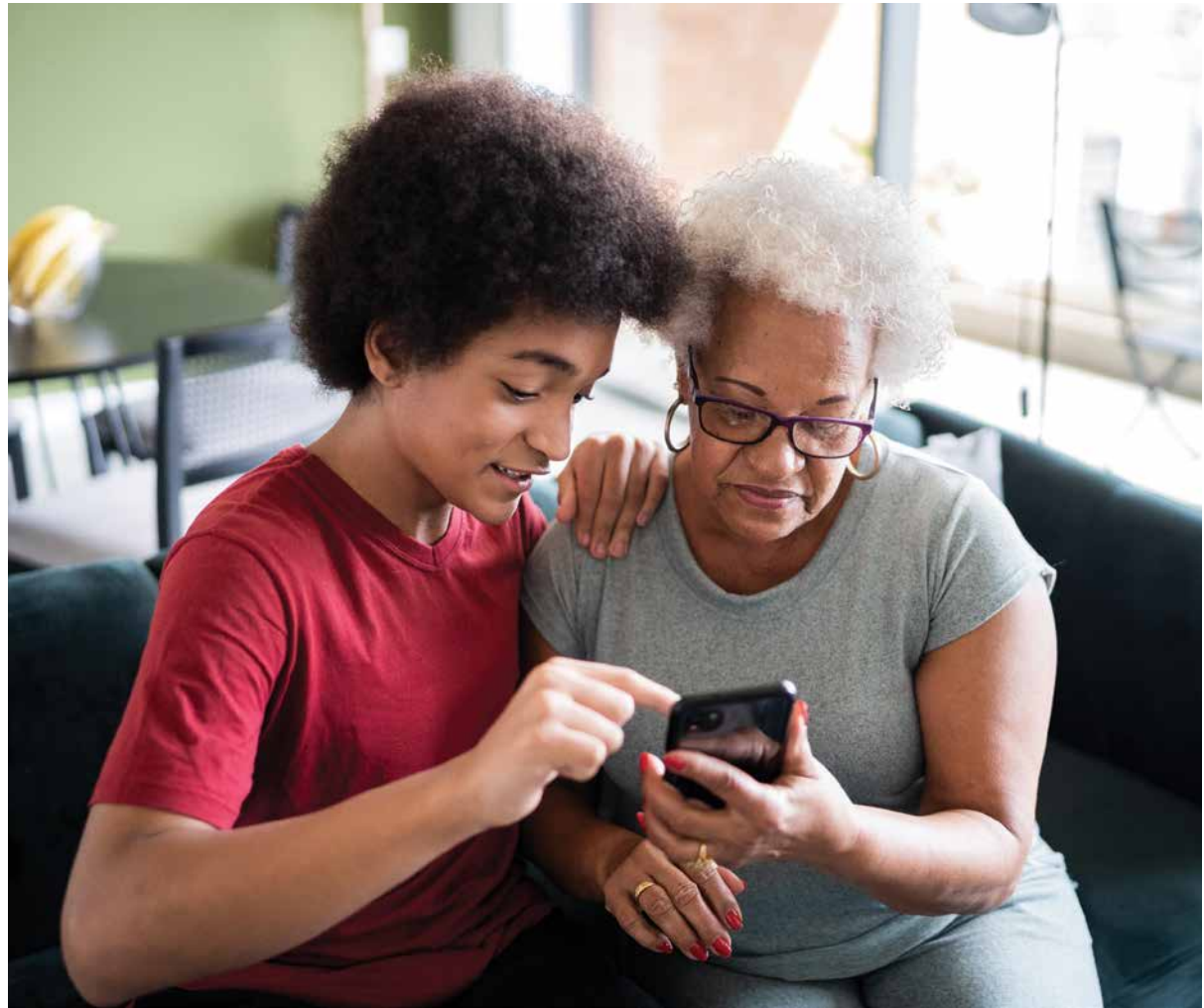
CHAPTER 2: Connecting Devices With Confidence

CHAPTER 2 TAKEAWAYS

1 Settings offer you many options for monitoring and controlling how your data is made visible and shared online. And once you figure them out on your phone, you should have little trouble figuring them out on other devices, too.

2 We connect our devices to the internet in many different ways. Wired connections are safer than wireless connections, but passwords can make wireless networks safer to use.

3 Unsecured public Wi-Fi networks present serious risks to your data. Avoid them, if at all possible.



CHAPTER 3

Finding Trust in Online Accounts

- How online data security works.
- Tips for building the best passwords.
- How to manage all of your passwords.



"You know, you can do this just as easily online."

An Internet Rife With Risk

In 2019 – 2020, one study found, almost half of all U.S. internet users became victims of online identity theft. Fully 47 percent of people endured the trauma of someone either opening up a fraudulent account in their name or having an existing account taken over. In more than half of these cases, the perpetrator turned out to be a family member or friend, heart-breaking though it is. Total losses for identity theft overall came to more than \$700 billion a year. Digging into the numbers that trace the scourge of online identity theft might make us conclude that the only safe approach to data care is to keep our data entirely to ourselves.



To go online is to trust online

The fact is, however, that deciding not to trust the internet with our data has become impossible. The ever-growing volume of tasks we carry out online through the many accounts we create means that our personal data ends up in the hands of many different kinds of companies, all with different approaches to handling it. Our banks, utility services, shopping sites, and news providers end up doing things with the personal data we give them that are difficult to track and impossible to contain. Even so, we put our trust in these companies and organizations to do the right thing — or at least not the

worst thing — with all the personal data we put into their virtual hands.

What to do to be safer

Whether this trust is misplaced or not, we can and should act to reduce the risk that our data winds up in the wrong hands or being used against us. In this chapter, you will learn many measures to protect yourself and the reams of personal data contained in online accounts. Passwords, of course, when built and used properly, provide a bulwark of protections, and you will learn several approaches to maintaining a robust, reliable online password system. You will also find other tips in the name of keeping online accounts working as safely as possible in your best interests.



CHAPTER 3: Finding Trust in Online Accounts

Trust, out of mistrust

Online accounts are, in fact, built on assumptions of mistrust. If the internet were a perfectly trustworthy environment, you could log into accounts with nothing more than your name. To get into your bank account, for example, you'd just enter your name into a box on the screen, and the bank's online system would let you check your balance, withdraw or deposit money, make a transfer, and so on. This approach might be convenient, but of course nobody would entrust their money to a financial institution that worked this way.



Trust is a two-way street

Instead, online bank accounts, and most every other type of online account, require users to prove they are who they claim to be before providing access to account data. To prove their identity, users provide information to identify themselves, typically a "userid," and then a separate piece of information that authenticates this identity. This separate piece of information is, of course, most commonly a password, the linchpin of online data security systems everywhere. Once an online data security

system matches a userid to a proper password, it authorizes the user to get into the system and act, within limits, to access the data in his or her account. All three of these operations — identification, authentication, and authorization — represent assumptions of mistrust, assumptions that people will seek access to data that is not theirs to do things they should not be doing. For online businesses to trust us as users, we need to jump through these hoops and prove, time and time again, that we are who we say we are.

A different kind of CIA

In turn, users must trust online businesses to handle personal data in the right ways. Users expect their data to be confidential, accessible only to them. They expect it to be reliably correct, to correspond to off-line reality with integrity. And they expect their data to be available





Look for the "S"

Online businesses signal their trustworthiness, and implicit commitment to the CIA triad, in various ways. One way appears in the very name of their website, which should start with the letters "https." The "s" stands for "secure," meaning that network data is encrypted into meaningless gibberish as it goes back and forth between user and system. And only the system can translate the gibberish into meaningful data. Trust can also originate with a business's reputation, a user's prior relationship with it, and persuasive representations of its approach to security. We should always monitor factors such as these to assess whether a business can be trusted to uphold the CIA triad and be a proper custodian of our personal data.

when they want access to it. These three principles — confidentiality, integrity, and availability — make up the so-called "CIA triad," a core principle of designing and managing online data networks.

Good passwords are your best defense

As we said, the password sits at the center of this environment of assumed mistrust. Successfully deployed, it acts as the antidote to mistrust, the clinching move in the digital handshake that signals a mutual trust between ourselves and the companies that hold our data online. But people are generally lousy at managing passwords, and companies are not always much better. The single most important thing people online can do to stay safer is step up their password game. Turn the page to find out how.

CHAPTER 3: Finding Trust in Online Accounts

HOW TO BUILD BETTER PASSWORDS

A 2020 hack of software company SolarWinds exposed sensitive data networks of thousands of high-profile companies and prominent government agencies. Hackers stole a critical company password to smuggle malware into a software update distributed to the company's large list of customers.

Most people online do as badly with their own passwords. The most-used passwords are such careless constructions as "123456," "qwerty," and "password." *Ugh.* Passwords are the front lines of defense for our data, and developing a plan for building and maintaining strong passwords is job no. 1 for effective data care.

1. Make them long.

Passwords should be at least **10 characters long**. Hackers use powerful computers to crack passwords, and they can figure out short, simple passwords in seconds or, at most, minutes.

2. Use a variety of ingredients.

A strong password contains upper- and lower-case letters, numbers, and special characters. Every different kind of character you use increases the combination space of the password, making it harder to crack.

REPLACE LETTERS

a → @
B → 8
E → 3
i → !
o → 0
s → \$

ADD PUNCTUATION

<, >, ?, /, *, &, ^, %, #, etc

USE THE FIRST LETTER OF EACH WORD OF A FAMILIAR SENTENCE OR PHRASE

For example:

My kids are named Sue,
Joe and Micheal.

Becomes: <Mkansj&M!>





3. Make them meaningful to you in some way.

A favorite song or movie title, creatively modified, can provide the basis for a long, strong password. "Aint2pRoud2beG!" has 16 well-varied characters. Or, say, "Char1ot\$ofF1re" for a strong, 14-character example.

4. Use a same-body/different-tail approach.

Develop a complex string of 8-10 characters that's meaningful to you. For example, a fan of old movies might use *Casablanca* and its 1943 release date to arrive at "19Ca\$a43" as the body. Then add a variable combination of other characters as a "tail" that relates to each individual account. For example, you could end up with "19Ca\$a43Amaz!" as a strong, long, memorable password for your Amazon account. Or "19Ca\$a43Elec!" for the account you have with your electric utility provider.

5. Test your password.

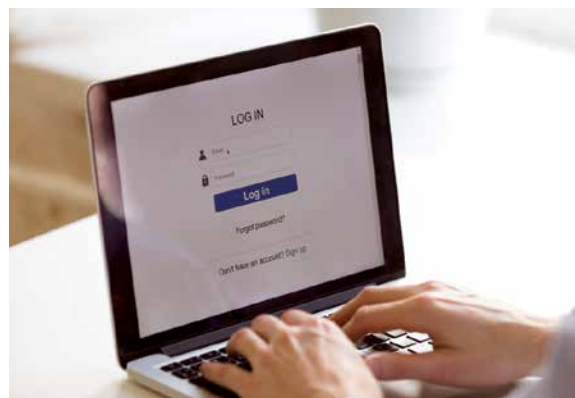
Whatever approach you choose for building passwords, make sure they are secure. Go to <https://www.security.org/how-secure-is-my-password/>, enter your password candidate, and see how long it would take to crack it. Try different combinations of characters to build safe, memorable, and manageable passwords.



CHAPTER 3: Finding Trust in Online Accounts

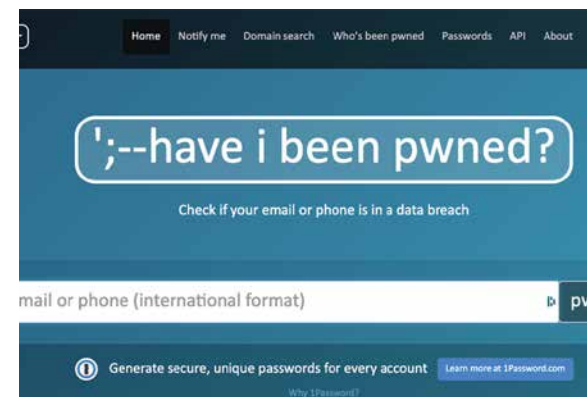
SMART PASSWORD MANAGEMENT

With the average person online trying to keep track of more than 200 accounts requiring passwords, the need to be smart and safe with them has never been greater. Once you settle on an approach to building passwords, you need to think about how to manage them:



1. Use a different password for each account.

An absolutely crucial measure, creating unique passwords prevents hackers in possession of information for one account from raiding other accounts as well. If someone logs into Netflix with your username and password, that's bad. But if you used that same password with, say, your Wells Fargo account, things could get much worse.



2. Check to see if your existing passwords have already been exposed.

Go to <https://haveibeenpwned.com/>, click on the "Passwords" tab, and enter your passwords to see if they have shown up in any data breaches. If they have, change them right away.



3. Use multi-factor authentication wherever available.

This security system delivers a one-time code to a device different from the one you are using to log into an account. You then enter the code from the second device into the first device to complete the authentication process that gets you into your account.



4. Store your passwords somewhere safe.

Hard-copy notebooks offer non-digital storage safety, but you still should secure the notebook from loss, intrusive eyes, pets, and other such real-world risks. Locked files on a computer or mobile device can work, but they can still be exposed to hacking under just the wrong circumstances.

Make Life Easier: Use a Password Manager

The simplest and probably safest solution is to use a password manager, a dedicated app for storing and/or generating secure passwords for all your accounts. The password manager is loaded onto your device as an encrypted piece of software, and it auto-completes login information whenever you try to access an online account. If you have manually saved a password into the password manager, the program will use it. If not, the password manager will generate a new, hard-to-break password for you and then save it for future use. All you have to do is build and remember a very-hard-to-break password for the password manager itself. The best password managers typically require a subscription fee, around \$50 per year. Examples include LastPass, 1Password, and Dashlane.



LastPass



1Password



Dashlane

CHAPTER 3: Finding Trust in Online Accounts

THE ONE SECRET TO STAYING SAFE ONLINE ... DOES NOT EXIST

Because there's no single online shield, you have to layer your safety measures on top of each other as reinforcements. That way, if one layer fails, another one, two, or three layers are in place to prevent further damage.

Use these tips and tricks to create layers in a security strategy to keep you and the data in your online accounts safer.

1. Download apps and programs only from trusted sources, like the App Store or Google Play.

And look at reviews as well as information from the developer about what kind of data is collected through the app. Some apps gather much more data than they need to.



2. Enter credit card information manually

instead of saving it with account data stored by a vendor or in your web browser. Storing payment information can be convenient, but it's risky. Hackers have tools to dig into data stored on our browsers, through bogus browser extensions, malware, or hoax email schemes. Better to spend the 30 seconds on manual entry now than the many hours it would take to recover from identity theft later.

3. Use one of your credit cards only for online purchases and nothing else.

If your financial data gets hacked, you'll have just one place to go to stop payments and seek recovery of any stolen funds. And never use debit cards — they offer much weaker buyer protections.



4. Avoid public charging stations, which can be hacked to gather data through a USB plug.

Travel with a portable charger, or at least use the transformer that came with your device.



5. Be wary of browser extensions in general, unless they come from a trustworthy source.

Adding dodgy software to your browser can expose all your online behaviors to third parties with bad intentions.



6. Keep antivirus and operating system software up to date, all the time.

These updates are often developed and delivered in response to newly discovered security risks. But install updates manually, rather than automatically, so that you have a chance to inspect any new piece of software loading onto your machine. Some of the worst data breaches have resulted from companies loading software updates booby-trapped to give hackers access to systems they should not be able to get into.

Do you wonder if your data has been leaked?

Most likely, it has. The largest data breaches involve billions of records. And the number of compromised online accounts is far more than the population of the entire world. So if you are wondering whether or not your online data has been compromised, you can be almost certain that it has. But you can check for sure by entering an email address, password, or phone number at the website <https://haveibeenpwned.com/>. Once you know which accounts are compromised, go make the changes you need to keep your data safer.

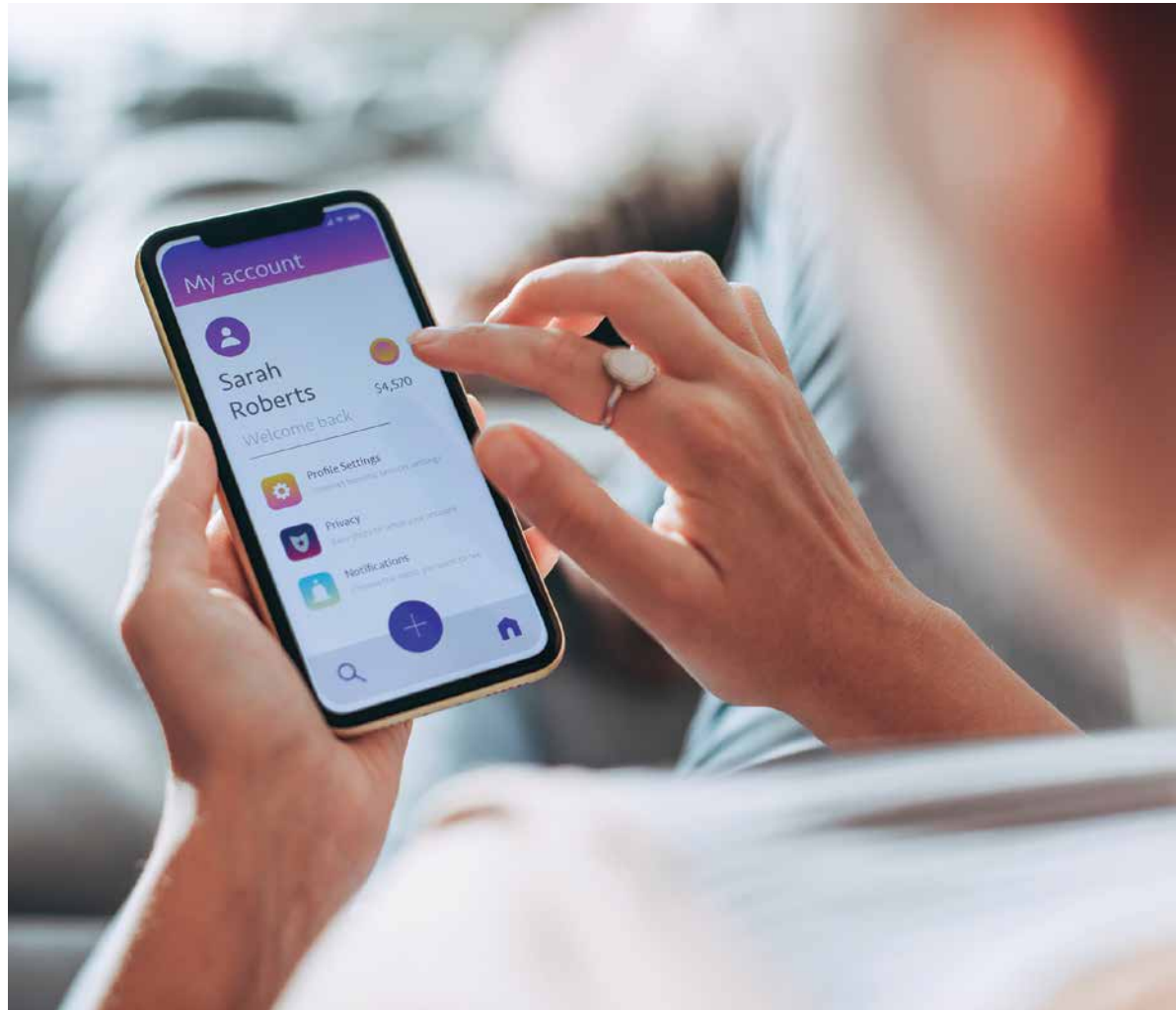
CHAPTER 3: Finding Trust in Online Accounts

CHAPTER 3 TAKEAWAYS

1 Identity theft can happen to anyone. Almost half of all internet users fell victim to it in 2019 – 2020, with annual costs of over \$700 billion.

2 Passwords should be the centerpiece of our data care protocols. They should be long, strong, and part of an effective management system.

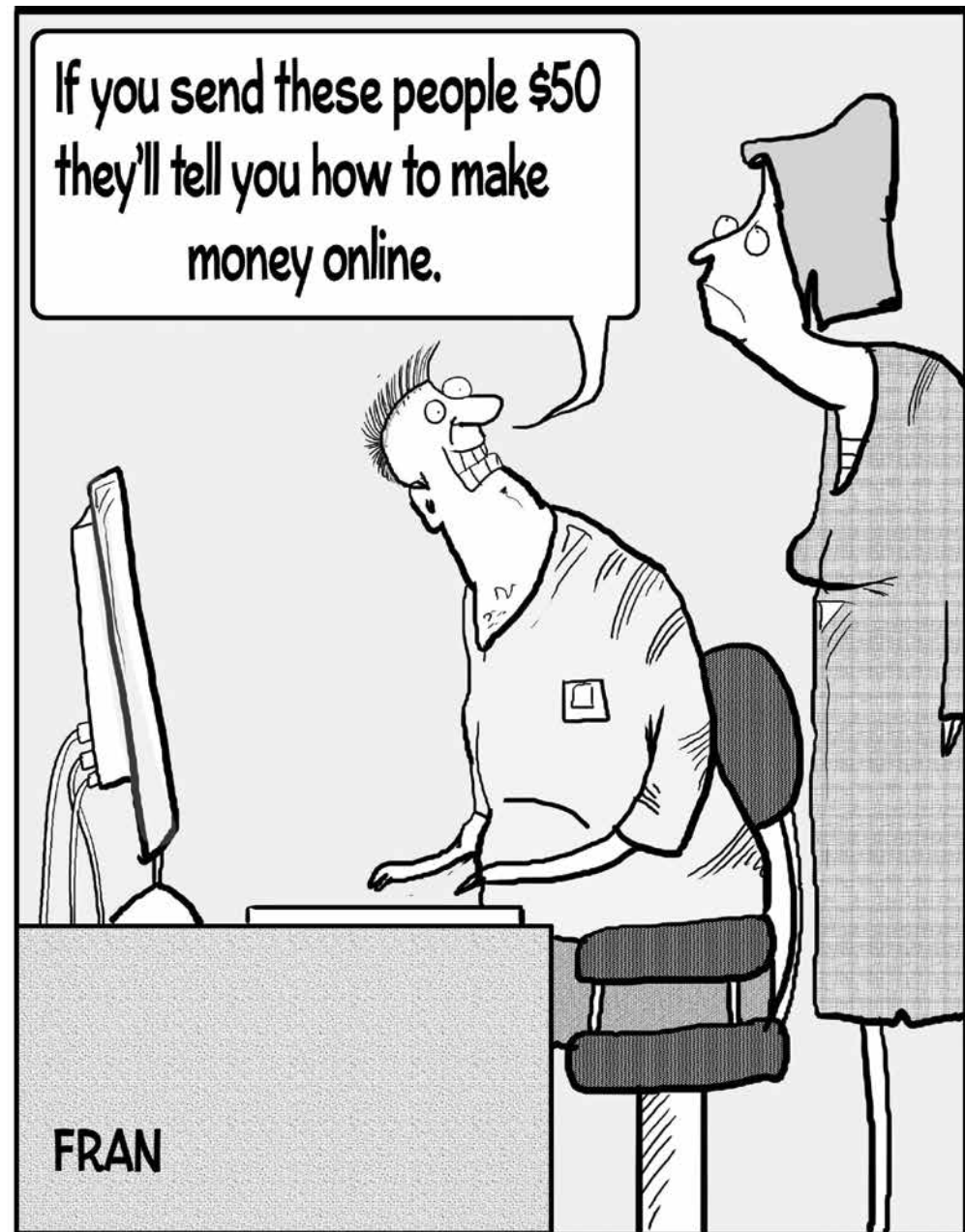
3 Effective data care means a layered approach to security. Informed, consistent attention to passwords, on-line accounts, payment methods, and device updates can make using the internet a safe, enjoyable, and productive experience.



CHAPTER 4

Protecting Yourself From Fraud and Scams

- How to spot phishing emails.
- The most common online and phone scams.
- What to do if you fall for a scam.



Required: A Healthy Dose of Skepticism

In the 1968 hit song “I Heard It Through the Grapevine,” Marvin Gaye reminded us to cast a skeptical eye on information in the public sphere: “People say believe half of what you see, son, and none of what you hear.”

In the digital age, this “half and none” standard might be too generous. Remember, wise data care practices do not stop with how we safeguard the personally identifiable information we give out online. Data care also means being a thoughtful, discriminating consumer of the information coming back in our direction. The online content we consume via email, social media, and news and information sources can go back and forth confusingly and quickly between trustworthy and not so

much. We must be able to tell the difference between what is false, deceptive, and malicious and what is true, reliable, and friendly.

Hoaxers and tricksters abound Unfortunately, this task is only becoming more difficult. Nearly every online information channel suffers



from worsening forms of information pollution. Our email inbox brings us more scam “phishing” campaigns every day. Social media platforms are rife with hoaxers and tricksters preying on our trusting nature. And news and information websites are littered with disinformation and misinformation that can endanger our health, rob us of money, and damage the foundations of civil society.

Truth can be a scarce commodity In all these areas, the fake and the fraudulent can crowd out the true. Unfortunately, an online truth detector does not yet exist. Instead, for consuming content, data care means bringing vigilant, skeptical thinking skills to everything we read, hear, and watch.



CHAPTER 4: Protecting Yourself From Fraud and Scams

PHISHING: DON'T TAKE THE BAIT

"Phishing" is a catch-all term for scams that come through email, text, shared video, or other personal communications channels. Designed to persuade people to give up sensitive account data, personally identifiable information, or simply money, these scams play on our emotions, especially fear, greed, temptation, and other states of mind that move us to make bad decisions.

In the case of phishing, the bad decision is usually to share personal information that allows criminals to get into data stores and networks that should be off-limits to them. With such access, hackers then infect computers with malware, lock up files and hold them for ransom, steal people's data or money, or commit other crimes that cost businesses and individuals billions of dollars every year.

A few facts about phishing

1. Phishing is by far **the most common form of cyber crime**, by almost a four-to-one margin, according to the FBI.
2. Alarming high percentages of people fall for scams — by one count, **over 20 percent of recipients open phishing messages**, and two-thirds of these click on links they contain.
3. One large study found that **95 percent of data breaches result from human error**, with the vast majority resulting from successful phishing campaigns.

An imperative of good data care is to use caution in providing information, especially in response to out-of-the-blue requests. Learning to spot phishing emails is a key first line of data care defense. Most phishing emails will reveal themselves as fake when you look at them closely.





Telltale signs of a phishing email

- Spelling and punctuation errors, as well as awkward formatting
- Language constructions that do not really make sense
- URLs that do not contain the name of the company behind the message
- Absent or invented information related to the person receiving the email.
- Unexpected or suspicious attachments, especially files ending with .exe.

Also, a sense of urgency

They often seek to generate a sense of urgency or excitement in the recipient.

You've won a \$100 Amazon gift card — act now to receive this limited offer!

Your Facebook account might be compromised — enter your username and password here to check!

Bank error in your favor — send us your account number to confirm!

Refinance now before interest rates go up — we will work with your lender so you don't have to!

Opening up messages like these tells the scammers that your email is real. Clicking on attachments or links can expose your computer to malware and compromise data on your hard drive. Whenever you get an email from an unfamiliar source, describing something too good (or bad!) to be true, with an attachment or link you did not expect, just delete it and move on.

CHAPTER 4: Protecting Yourself From Fraud and Scams

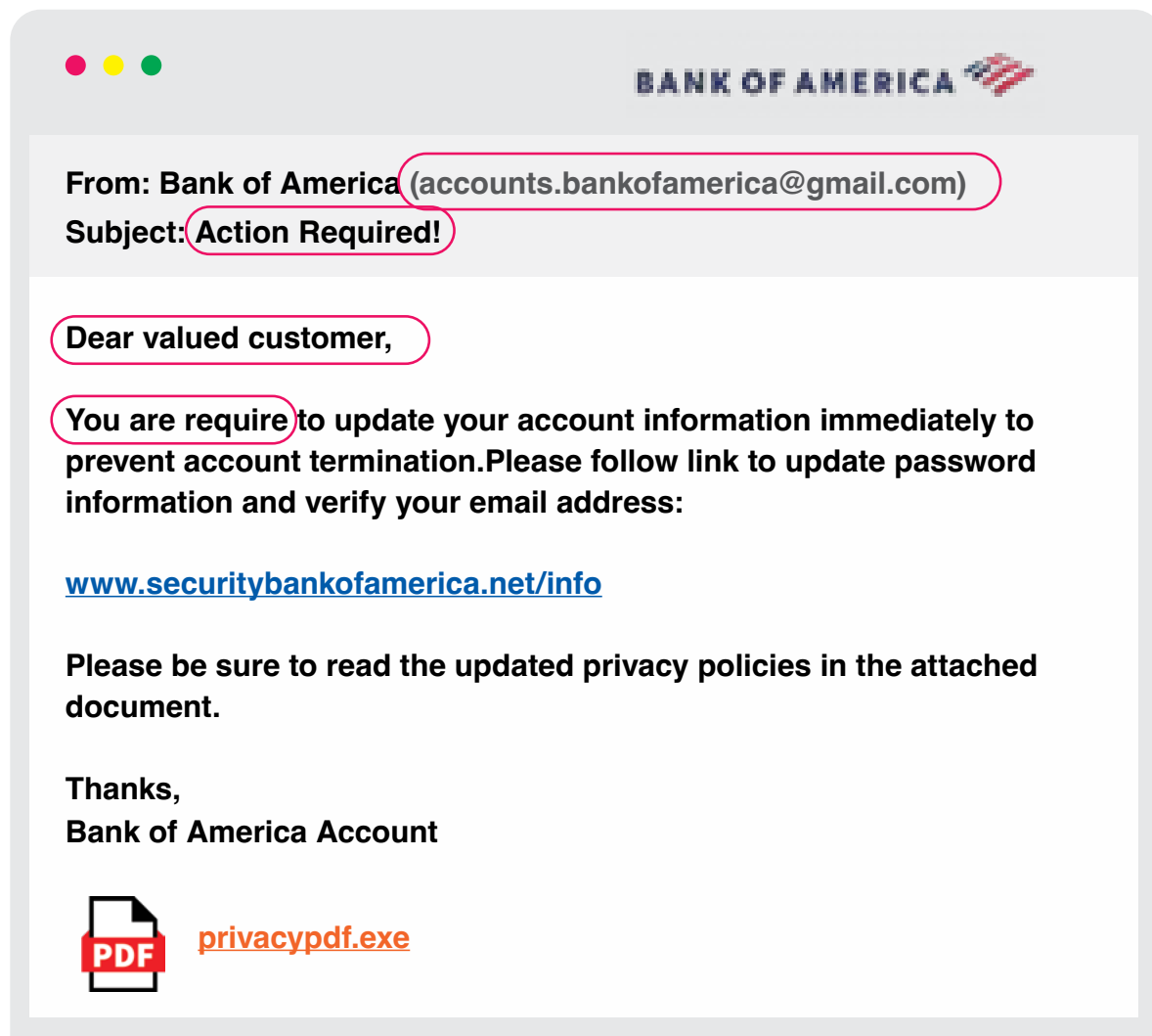
TEST YOUR PHISHING-DETECTION SKILLS

Look at the email at right and study the circled indicators of a phishing email. Then see how many more clues you can find that reveal the email as fraudulent.

1. **Email address of sender is not legitimate.** An email from your bank would not come from a gmail account.
2. **A sense of urgency in the subject line.**
3. **Generic greeting or salutation.** Your bank would greet you by name.
4. **Poor grammar or typos.**

What else can YOU find? Check the purple box on the next page for answers.

And finally, when you get a phishing email, you can often report it as spam or junk email. Look for a button on the screen with either of these terms to banish the sender from your inbox forever!





You can further develop your phishing-detection skills in various ways. A great place to start is <https://www.phishing.org/>, where you will find extensive, accessible, free guidance in identifying and avoiding

phishing scams. You can also select from any number of online phishing quizzes on other websites. These quizzes will walk you through how phishing emails are designed to trick and deceive. Don't worry about how well you

do — you can take these quizzes as many times as you need to become an expert at identifying phishing emails.

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

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

<https://phishingquiz.withgoogle.com/>

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

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

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

OTHER CLUES IN THE EMAIL

1. The logo at top of the email is low-resolution, blurry.
2. Space missing between "termination" and "Please".
3. Link doesn't look like legitimate website for Bank of America.
4. Generic signature.
5. The attachment ends in .exe.


CHAPTER 4: Protecting Yourself From Fraud and Scams

SCAMS: THIS TIME, IT'S PERSONAL

Scams can also take more personal forms than the high-volume, blast-it-out-widely approach that phishing represents. Initiating contact through social media or even by phone, scammers will seek to establish a personal connection and build trust with victims. Through multiple contacts, these “relationship-building” scams often require victims to provide sensitive personal data that criminals then exploit to extract money or secure other articles of value. Just as with phishing campaigns, the scams succeed by distracting or manipulating the victims with appeals to emotion. Good data care practice in these cases means NOT giving up personal information, even in the face of seemingly urgent, threatening circumstances. Remember that you always get to decide what you do, no matter what someone is telling you.



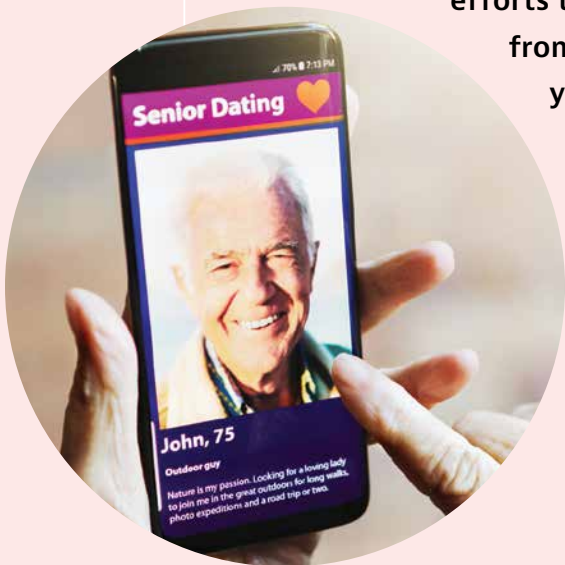
COMMON SCAMS AND HOW THEY WORK

SCAM	WHAT HAPPENS	HOW TO STAY SAFE
<p>Social Security, Medicare, and other government benefits</p> 	<p>The scam works by overwhelming you with claims of scary, immediate dangers, which you need to solve right away by providing sensitive, personal information to the person on the other end of the call.</p> <p>For instance, a scammer calls or emails asking you to verify your Medicare number, perhaps because of a change from paper to plastic cards or to add a chip to the card.</p> <p>Another scam involves offering you a less expensive plan or better benefits, but they need to know your Medicare number first. (They do not need this information in order to offer you a better plan.)</p>	<ul style="list-style-type: none"> → Hang up the phone. → Don't call any numbers left in a voice or text message or email. Call the customer service number of the agency itself and describe what is going on. You can trust the information you ask for more than the information people give you out of the blue. → Never, ever give out your account number, Social Security Number, or any other sensitive personal information unless you know the person asking for it is legitimate.

CHAPTER 4: Protecting Yourself From Fraud and Scams

COMMON SCAMS AND HOW THEY WORK (CONTINUED)

SCAM	WHAT HAPPENS	HOW TO STAY SAFE
Romance	<p>The scammer will seek to move a “relationship” quickly towards intimacy but at the same time resist meeting in person. And this scam, like others, depends on keeping it secret from your friends and family. Any efforts to isolate you from people in your life that you trust should set off alarm bells.</p>	<ul style="list-style-type: none">→ Look for the person’s profile on multiple dating platforms or through a general internet search. Often, the scammer will use the same name and picture on many different sites to carry on simultaneous scam campaigns.→ Never send money or personal information over the internet. If the relationship is real, you can always do these kinds of things in person, if you want to.→ Resist any efforts to exclude trusted friends and/or family from news of the exchange. They can tell you what might seem wrong about the situation.→ Be careful about what you post online about yourself. Even personal information that seems innocent or mundane can be used to draw you into something fishy.



BY THE NUMBERS



People age 50 and over are targeted more frequently than other ages for internet scams and hoaxes. In 2021, the FBI received over 165,000 complaints from online crime victims in this demographic, with over 90,000 coming from those 60 and older. Total losses among older victims came to almost \$3 billion, about 67 percent higher than the \$1.8 billion in losses racked up the year before, and notably more than younger victims' losses. Indeed, these figures surely understate the full extent of the problem, since many online crime victims never report their losses because of embarrassment, shame, or not knowing where to go for help with their plight.

SCAM

WHAT HAPPENS

HOW TO STAY SAFE

Family member in need

These scams exploit your concern for loved ones in combination with real pieces of personal information to get you to act quickly in an apparent emergency situation.



→ Hang up the phone and call your family member directly to make sure the person is safe. If you can't reach him or her right away, call another family member or friend to gather whatever information you can.

→ Never send money or give out personal information in response to a call like this. Once you establish what is really happening, there will be time later to help make things right.

→ Restrict access to personal information on Facebook and other social media platforms to friends and family. Scammers routinely gather personal information from public data on social media to make it sound as if they know you or your family members.

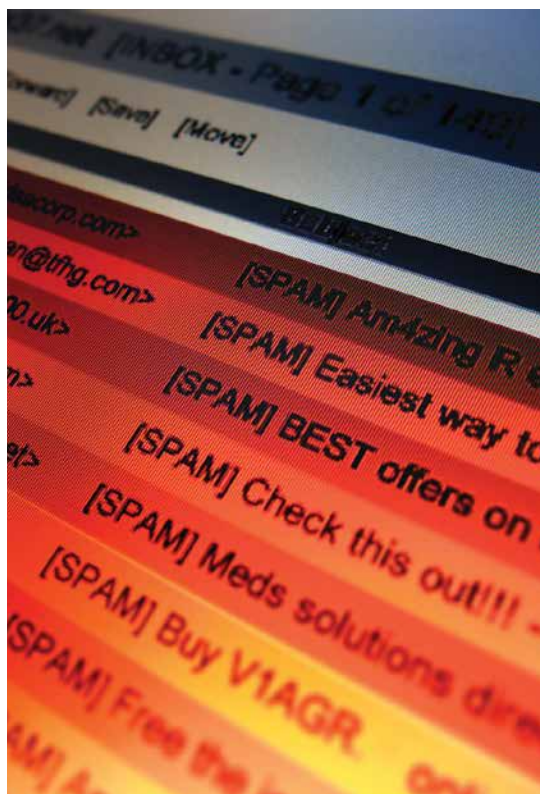
CHAPTER 4: Protecting Yourself From Fraud and Scams

COMMON SCAMS AND HOW THEY WORK (CONTINUED)

Other scams might involve offers of things such as:

- Prepaid home repairs never to be actually completed.
- Tech support for your computer to plunder data on a personal hard drive.
- Fake prizes that require financial account information to be claimed.

In many cases, these scams come packaged with persuasive personal details. They know your hometown, where you last vacationed, the names of your family members — all the kinds of personal information shared through social media profiles or found in publicly available records having to do with, for example, real estate transactions. Our lives are virtual open books on the internet, to a much greater degree than most of us can



quite imagine. It is no trick at all to compile a detailed biography of almost anyone who uses the internet to stay in touch with family and friends and carry on any kind of digital life online.

Don't just do something — sit there!

Often, the best response is no response at all. Keep your money and personal information and anything else of value to yourself. Unsolicited calls, emails, or rings at the door are often bogus and malign. Hang up or say no or walk away.

On your own schedule, consider how realistic or likely a scam scenario really is. Verify the offer or claim or request by calling the Social Security Administration or your bank or your family member. Investigate the dating partner on his or her profile and through your own online searches. Ask the questions you want to ask to find the answers you need so that you can check into what might be going on. Then decide what you want to do, if anything, when you are ready to do it.

IF YOU DID SOMETHING YOU WISH YOU HADN'T

Help is available to people who are victimized by scam artists.

Consider the resources below, depending on what happened to you:

Freeze your credit.

Contact all three credit bureaus to lock down your accounts and prevent anyone from doing something fraudulent in your name. Calling is the quickest way to start.

- Experian: 888-397-3742
- Equifax: 888-378-4329
- TransUnion: 888-909-8872

Contact the FBI.

Try either the local field office or the Internet Crime Complaint Center.

- Find a local office: <https://www.fbi.gov/contact-us>
- File a complaint: <https://www.ic3.gov/>

Get in touch with Fight Cyber Crime for immediate online support.

- <https://fightcybercrime.org/>

Call the National Elder Fraud Hotline.

- 833-FRAUD-11 (833-372-8311)
- <https://ovc.ojp.gov/program/stop-elder-fraud/providing-help-restoring-hope>

Ask for help from your local police.

NEWS YOU SHOULD'N'T USE

Even at the dawn of the World Wide Web, people were worrying about the quality and reliability of information available online. Experts at Forrester Research, a leading global market research firm that has long specialized in online communications, discussed the then-newfangled "information superhighway" in a 1997 *New York Times* article: "The good news is that everything is widely available. The bad news is that everything is widely available.... You used to spend hours getting the information you need. Now you spend hours verifying the information you have gotten."

If only people DID spend hours verifying the information they find online. But, of course, few of us do.

The principles of good data care, however, guide us to trust only what we can independently verify. Instead of just believing what you read or see online, check with people you trust, consider alternative viewpoints, and reserve a healthy skepticism for startling claims that are often meant just to get you to click on something before thinking twice about whether it is actually true or not.

CHAPTER 4: Protecting Yourself From Fraud and Scams

CHAPTER 4 TAKEAWAYS

1 Data care means safeguarding the information we give out online, as well as assessing information we take in for trustworthiness and reliability.

2 Scams and hoaxes come at us from many different directions online — always remember it's okay to walk away from, say no to, or just delete anything fishy.

3 Keeping a critical eye out for untrue and unreal claims online is a basic element of good data care practices.



TEST WHAT YOU'VE LEARNED!

The questions below all draw on the contents of this book. If you've read closely, or take the time to review before answering, you should be able to answer all of them with confidence. And if you get a few wrong, just go back to the chapter and look again to find the right answer. Learning about data care is an ongoing journey, and it's always okay to get help along the way.

Chapter 1

1. The data we generate online can reveal everything from the type of pet we own to where we take vacations. **True or False?**
2. Online data can be collected based on what we do with our phones, computers, smart speakers, digital watches, and cars we drive. **T or F?**
3. The internet knows where we are when we use our phones within about 100 feet of our precise location. **T or F?**
4. Data care involves learning about

and managing all the points of control that you have over your personal data. **T or F?**

5. Where can you go to get help with operating personal technology devices?
 - A. Online support from the manufacturer
 - B. Videos on YouTube
 - C. A trusted friend or family member
 - D. All of the above
6. What kind of phone(s) can you use to make a video call?
 - A. Android
 - B. iPhone
 - C. Touchtone
 - D. None of the above

Chapter 2

1. The default settings on our computers and phones are perfectly good for protecting our privacy. **True or False?**
2. On an iPhone, you can disable ad tracking and restrict location services to keep more of your online data private. **T or F?**

3. Of all the web browsers, Safari gathers the most data from its users. **T or F?**
4. The most secure internet connection is usually through your phone, using cellular data. **T or F?**
5. It's okay to use password-protected public Wi-Fi networks to do a little online banking. **T or F?**
6. Which of these personal technology devices allow you to choose settings that control how your data spreads online?
 - A. Smartphone
 - B. Desktop computer
 - C. Smart speaker
 - D. Internet-connected thermostat
 - E. All of the above
7. What kind of internet connection is the riskiest?
 - A. Wired connection at home
 - B. Wireless cell phone connection
 - C. Public Wi-Fi
 - D. Wi-Fi network at a friend's house

TEST WHAT YOU'VE LEARNED! (CONTINUED)

Chapter 3

1. Online identity theft is often carried out by other family members or trusted friends. **True or False?**
2. Your data has very likely been leaked somewhere online. **T or F?**
3. As long as you have a good password, you can use it over and over again for different accounts. **T or F?**
4. You can generally trust companies to handle your personal data with reliable security and care. **T or F?**
5. Using a password manager can be a good solution to building and managing strong passwords. **T or F?**
6. Which of these passwords is the strongest?
 - A. abc321pass
 - B. WoelsYou45
 - C. 4mYr!s@h0m
 - D. Fidos#0418
7. Which of these is NOT a good password safety practice?
 - A. Make sure your password

- remains secret.
 - B. Use a different password for each online account.
 - C. Save your passwords next to your computer.
 - D. Use multi-factor authentication when available.
8. What is the best way to stay safe online?
 - A. Verify the trustworthiness of anything you download.
 - B. Always enter payment methods manually.
 - C. Avoid public charging stations, which are easily hacked.
 - D. Keep antivirus software up to date.
 - E. All of the above.

Chapter 4

1. The most common form of cyber crime is phishing. **True or False?**
2. Two-thirds of data breaches result from human error. **T or F?**
3. You can safely open attachments that come with unexpected emails. **T or F?**

4. Which of these are signs of a phishing email?
 - A. An urgent call to action.
 - B. Grammatical errors or typos.
 - C. Impersonal greeting or sign-off.
 - D. URLs that do not match the name of the company.
 - E. All of the above.
5. If you are the target of a scam, you should:
 - A. Provide just a bit of information to see if it's real.
 - B. Exchange contact information to communicate more directly.
 - C. Keep it all secret from family members and friends.
 - D. Hang up and walk away.

ANSWERS

Chapter 1: 1. True; 2. True; 3. False; 4, True; 5. D; 6. A & B.

Chapter 2: 1. False; 2. True; 3. False; 4, True; 5. False; 6. E; 7. C

Chapter 3: 1. True; 2. True; 3. False; 4. False; 5. True; 6. C; 7. C; 8. E

Chapter 4: 1. True; 2. False; 3. False; 4. E; 5. D.

GLOSSARY OF TERMS



Android: The software that organizes data and governs operations on mobile devices made by companies including Samsung, Sony, LG, and Motorola.

Authentication: A process or tool used to confirm the legitimacy of a claimed online identity.

Authorization: Approval or permission for a user to get access to and manipulate data stored online, within limits defined by that user's status in the system.

Availability: The need for data and the system in which it is stored to be accessible and functional at all times needed for users' and owners' business purposes.

Browser: An application program or tool that displays web pages. Examples include Safari, Chrome, Firefox, and Internet Explorer.

Cellular data network: The communications system enabling mobile phones and tablets to connect to each other and to the internet.

Confidentiality: The condition of data being disclosed only to those who are authorized to view it.

Data care: The practice of managing and limiting the spread of personal information online to minimize risks of misuse and criminal exploitation.

Duo: The program Android devices use to make video calls.

Encryption: a translation of language in plain, conventional text into ciphered text requiring a key to decode and make legible.

FaceTime: The program Apple devices use to make video calls.

Identification: A name or label representing a user of an online data system, unique to that user but not sufficient to authorize access to data.

Identity theft: Theft enabled by a criminal impersonating someone else by using personally identifiable information stolen from online or physical data sources.

Integrity: Assurance that data stored online remains accurate and whole, corresponding to off-line realities and/or the owner's understanding of its completeness and correctness.

iOS/macOS: The software that organizes data and governs operations

GLOSSARY OF TERMS (CONTINUED)

on devices made by Apple, including both mobile and desktop devices.

ISP, or Internet Service Provider:

A company that provides customers with access to online networks and information.

Malware: Software designed to damage, invade, or otherwise exploit access to people's computers in illegal ways.

Modem: A device that converts electrical signals of different types into forms that various types of machines can use to transmit and receive information made intelligible to all.

Multi-factor authentication: A method of providing secure access to data that requires a code or special access to be delivered a device other than the one being used to view that data.

Network Key: A password used to gain access to an online data environment.

Phishing: The use of emails or other digital messages seeming to come from a trusted site or person that actually seek to trick the recipient into giving up sensitive personal data, usually meant to gain access to restricted data networks and records.

Router: A device used to distribute information to computers on a network based on requests from users.

Search engine: A tool for finding information online based on keywords or phrases. Not to be confused with a browser, which is a tool that displays web pages, a search engine, such as Google, DuckDuckGo, or Bing, is a website that provides you with search results. So, for example, using the web browser Safari, you can search the internet using the Google search engine.

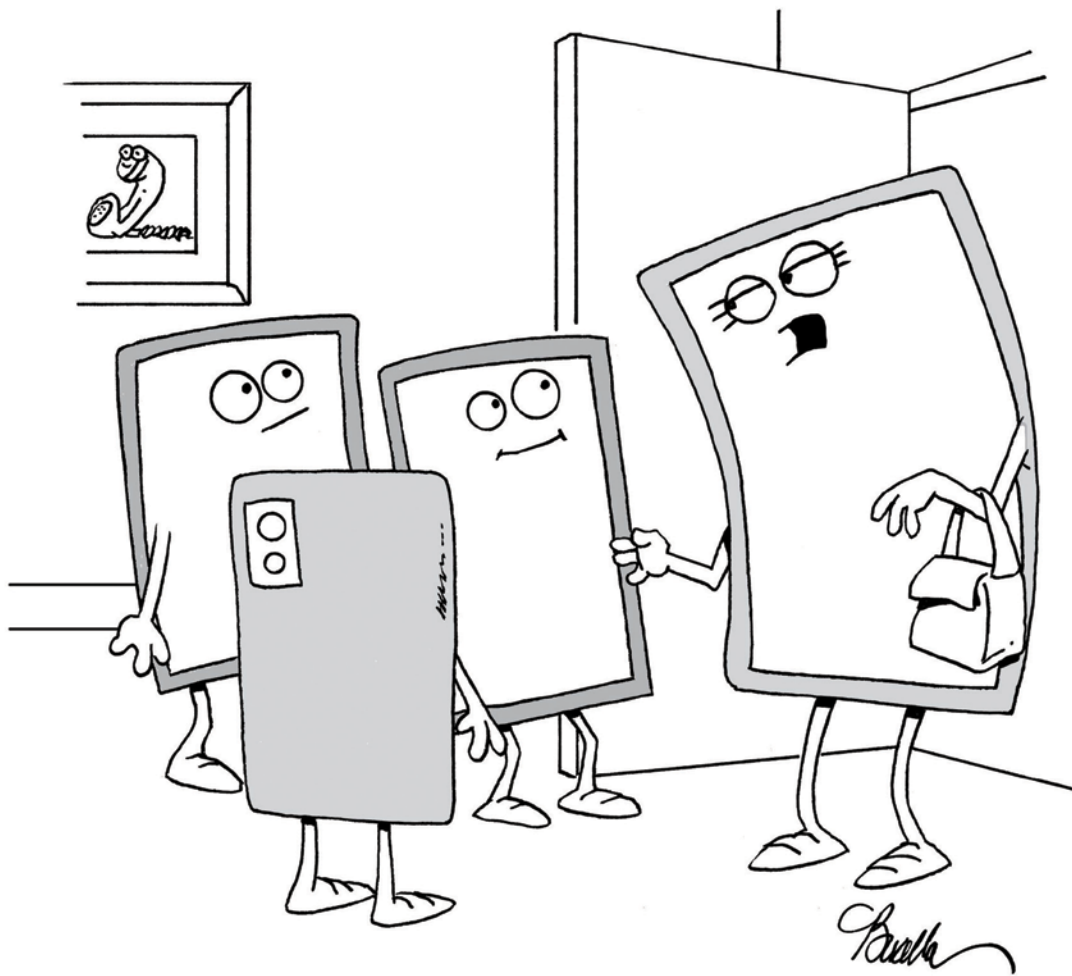
Userid: The identity or label by which a person is known on a computer system or network.

URL, or Uniform Resource Locator: The name of a website usually built to describe the contents or identify the organization associated with the website itself.

Virtual Private Networks, or VPNs: An app or piece of software that sits on your device and encrypts, or otherwise makes unreadable, data going between it and an ISP.

Web browser: A tool for accessing the World Wide Web or a local website. Examples include Safari, Chrome, Firefox, and Edge.

WPA: An acronym for Wi-Fi Protected Access, which is a security standard for computers with wireless internet connections.



"OK, now before we leave, did everybody charge themselves?"

Published by Start Engineering, LLC.

CEO & Founder: Robert F. Black

Creative Director: Stacie Harrison

Vice President, Learning and

Communications: Eric Iversen, Ph.D.

To purchase additional copies of this book please email Bob Black at bblack@start-engineering.com or visit our website shop at <https://www.cybersafeandsavvy.com/>

© 2022 by Start Engineering



CREDITS

PHOTOS All photos are from istockphoto.com except for: p.19, Stocky.com; p.29, Courtesy Samsung; pages 37, 46, 49, and 53, Getty Images; p. 38, Alamy Stock Photo; pgs. 43 and 45, Shutterstock.

CARTOONS All cartoons from Cartoonstock.com. Page 9 by KES; p. 21 by Ellis Rosen; p. 35 by P. C. Vey; p. 47 by Fran, p. 65 by Marty Bucella.

NOTES



Cryptology

Signals
Intelligence

Cybersecurity

THE NATIONAL CRYPTOLOGIC FOUNDATION

The National Cryptologic Foundation (NCF) was established in 1996 to support activities, displays, and artifact acquisition for the National Cryptologic Museum (NCM). Its mission has broadened to include a robust cyber education program and to deliver an innovation approach to solving cybersecurity challenges. Our support of the NCM remains a vital part of our mission, especially with our partnership with NSA.

National Cryptologic Foundation
808 Landmark Drive, Suite 223, Glen Burnie, MD 21601
Phone (443) 795-4498.
ncfinfo@cryptologicfoundation.org; CFC #31493

OUR CORE VALUES

Educate the public and inspire students to explore cryptology, STEM and cyber-related fields of study.

Stimulate and innovate by serving as a platform to bring big ideas to the table that support, educate and communicate with the public on the next generation of the cyber ecosystem.

Commemorate all “those who serve in silence” in the cryptologic mission with courage and distinction and whose contributions help enhance and preserve our way of life.