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!**

NATIONAL CRYPTOLOGIC FOUNDATION

WELCOME

National Cryptologic Foundation logo

Dear Reader,

Everyday cyber-attacks and cyber-fraud affect our lives.

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.

According to the 2023 FBI Internet Crime Complaint Center (IC3) Annual Report, the IC3 received 880,418 complaints with potential losses exceeding $12.5 billion. This is nearly a 10% increase in complaints and represents a 22% increase in losses compared to 2022. Investment fraud was once

again the costliest type of crime tracked by IC3. Losses to investment scams rose from $3.31 billion in 2022 to $4.57 billion in 2023—a 38% increase. The third-costliest type of crime was tech support scams. Victims 30 to 49 years old were the most likely group to report losses from investment fraud, while the elderly accounted for well over half of losses to tech support scams. (Internet Crime Complaint Center Releases 2023 Statistics, FBI, April 4, 2024).

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 clicking on links from unknown senders.

In the pages that follow you will learn the importance of taking care of your data, 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!

A digital version of this booklet is available free of charge on our secure website: cryptologicfoundation.org.

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

Laura C. Nelson
President & Chief Executive Officer

TABLE OF CONTENTS

AN INTRODUCTION TO DATA CARE

Creating data 24/7

Wait, what? The internet knows where we are when we use our phones? And other connected devices? Yes it does, 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 location as well as 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. Technologies that take us online 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 your online accounts and activities, and ends up filed in databases that companies and governments use to store information and behaviors associated with the way you use the internet.

Data care matters because all the data that circulates online about all of us as individuals is more than enough to build a detailed profile of anyone's identity. And it's not that hard to get hold of this data. Anyone with malign intentions, sufficient computer expertise, and some readily available digital tools can step into another person's identity and do bad things to that person or in that person's name. And the burgeoning presence of artificial intelligence in our online experiences only amplifies these risks. 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 how the principles and practices of good data care can help us more comfortably and confidently use online resources for all the good, convenience, and enjoyment they can offer.

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, shielded from AI manipulations, and accessible only to you and the people you want to see it. Just as we all strive to be active, informed stewards of our health,

finances, households, and general well-being, we should also be continuously learning and doing what is possible to use the internet safely and constructively.

That means understanding the best, safest ways to establish and manage online accounts, set up our devices to limit the release of personal data, and recognize and avoid the risks that show up on our internet-connected 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.

A simple, regular habit

Good data care can become a simple, regular habit, as familiar 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. 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.

> **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 in the margins to identify this kind of material. This information goes beyond the fundamental lessons of data care, and you can skip it without missing anything critical. And if you ever want to return to the book to learn more, the information will be there waiting for you.

Finding Trust in Online Accounts

→ **How online data security works.**

→ **Tips for building the best passwords.**

→ **How to manage all of your passwords.**

"I feel like my best passwords are already behind me."

To Go Online Is to Trust Online

From 2022 to 2023, the number of reported incidents in which American internet users' personal data was stolen, exposed, mishandled, or otherwise compromised nearly doubled, according to the Identity Theft Resource Center. The number of affected individuals totaled almost 350,000,000, or in other words, the equivalent of everyone in the country.

The good news is that this total represents a steep decline from the billions of people affected by data breaches of earlier years. The bad news is that data breaches remain notably underreported, and the true scope of this problem is almost certainly much greater than available statistics indicate. One estimate of the true dollar impact of cybercrime overall runs to $9.5 trillion for 2024, making cybercrime the third-largest economy of the world and more profitable than the global trade of all major illegal drugs combined.

Reckoning with such figures might make us conclude that the only safe approach to data care is to keep our data entirely to ourselves. 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 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 gets 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.

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 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 a digital handshake that signals 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.

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.

HOW TO BUILD BETTER PASSWORDS

Managing passwords is really hard. Even cybersecurity companies falter in this area. Okta is a company in the very business of managing and protecting online account credentials like userids and passwords. Nevertheless, in 2023 hackers secured an Okta employee's account credentials, introduced malware into the company's networks, and got hold of personal data for all the company's customer support users.

Most people do as badly with their own passwords. The most-used passwords are clunkers like "123456," "qwerty," and "password." And people use them over and over for online banking, shopping, streaming services, and any number of other uses. Ugh. Passwords are the front lines of defense, 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.
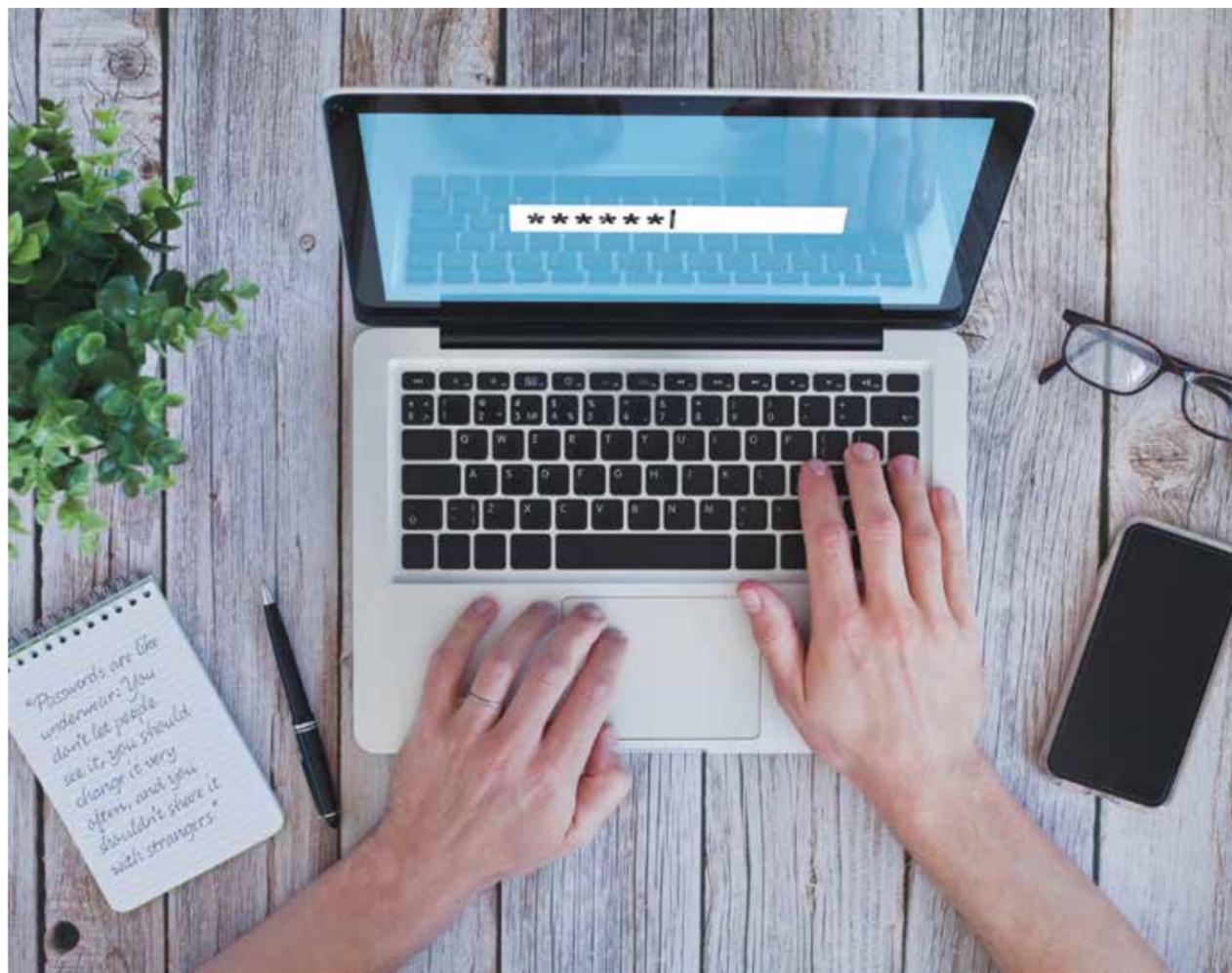
REPLACE LETTERS	ADD PUNCTUATION
	<, >, ?, /, *, &, ^, %, #, etc
a → @	
B → 8	**USE THE FIRST LETTER OF EACH WORD OF A FAMILIAR SENTENCE OR PHRASE**
E → 3	
i → !	*For example:*
o → 0	My kids are named Sue, Joe, and Michael.
s → $	*Becomes:* <Mkansj&M!>

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. "uptowNfuNk!2014" has 15 well-varied characters. Or, say, "hunG3r%Game$" for a strong, 12-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 the Marvel Cinematic Universe might use Avengers: Infinity War and its 2018 release to arrive at "20inF!war18" 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 "20inF!war18Amaz!" as a strong, long, memorable password for your Amazon account. Or "20inF!war18Elec!" 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.

How Secure Is My Password?
The #1 Password Strength Tool. Trusted and used by millions.
ENTER PASSWORD

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:
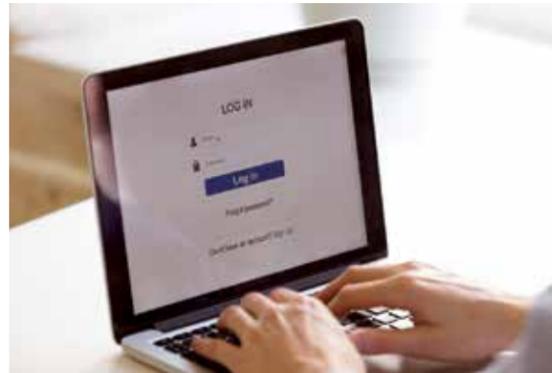
1. Use a different password for each account.

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 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

THE ONE SECRET TO STAYING SAFE ONLINE … DOES NOT EXIST

Because there's no single online shield, you must 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.
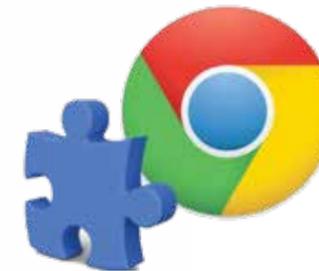
6. Keep antivirus and operating system software up to date, all the time.

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.

CHAPTER 1 TAKEAWAYS

1 Identity theft can happen to anyone. Every year, hundreds of millions of personal data records are compromised, and nobody can predict where the next security failure will occur.

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, online accounts, payment methods, and device updates can make using the internet a safe, enjoyable, and productive experience.
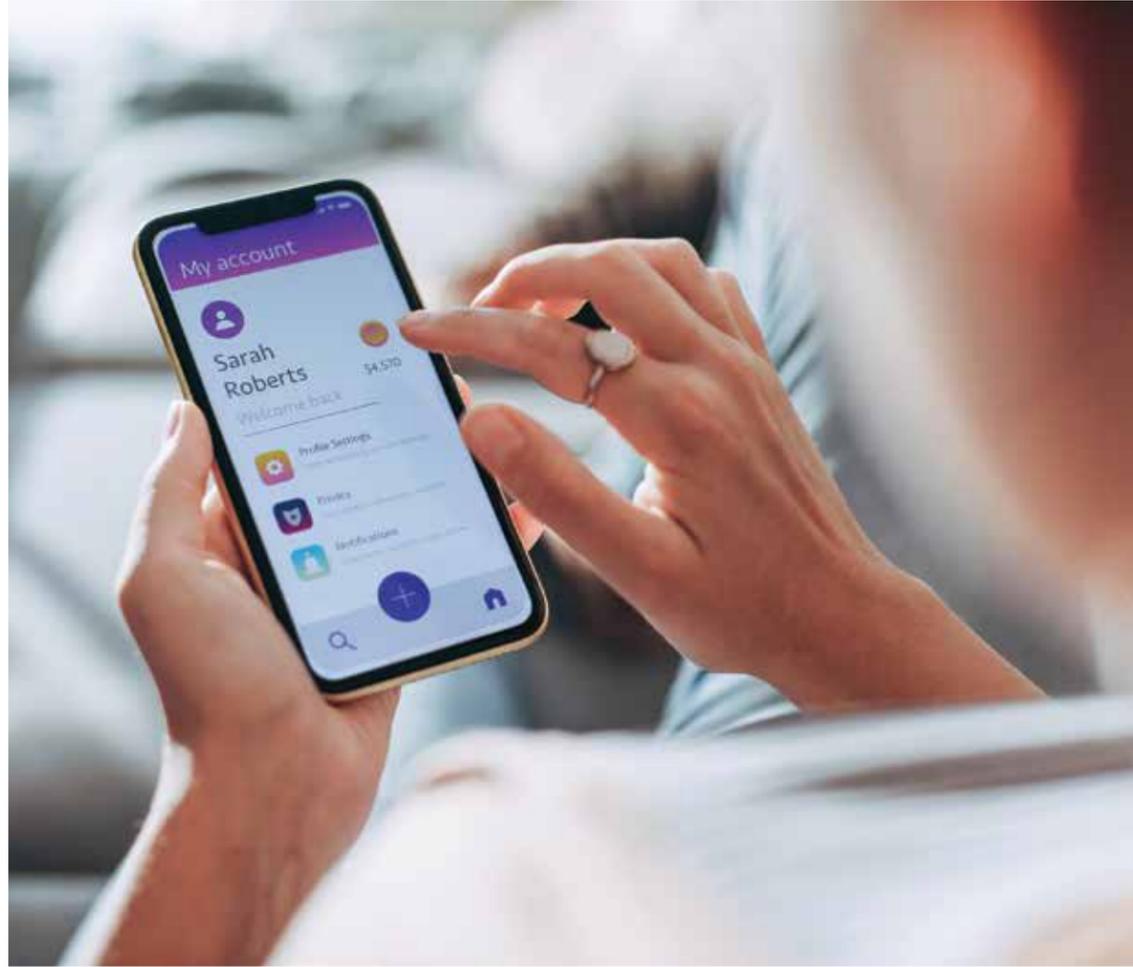
Connecting Devices With Confidence

→ **Learn how to adjust your phone settings.**

→ **Find safe ways to go online.**

→ **Understand the perils of public Wi-Fi.**
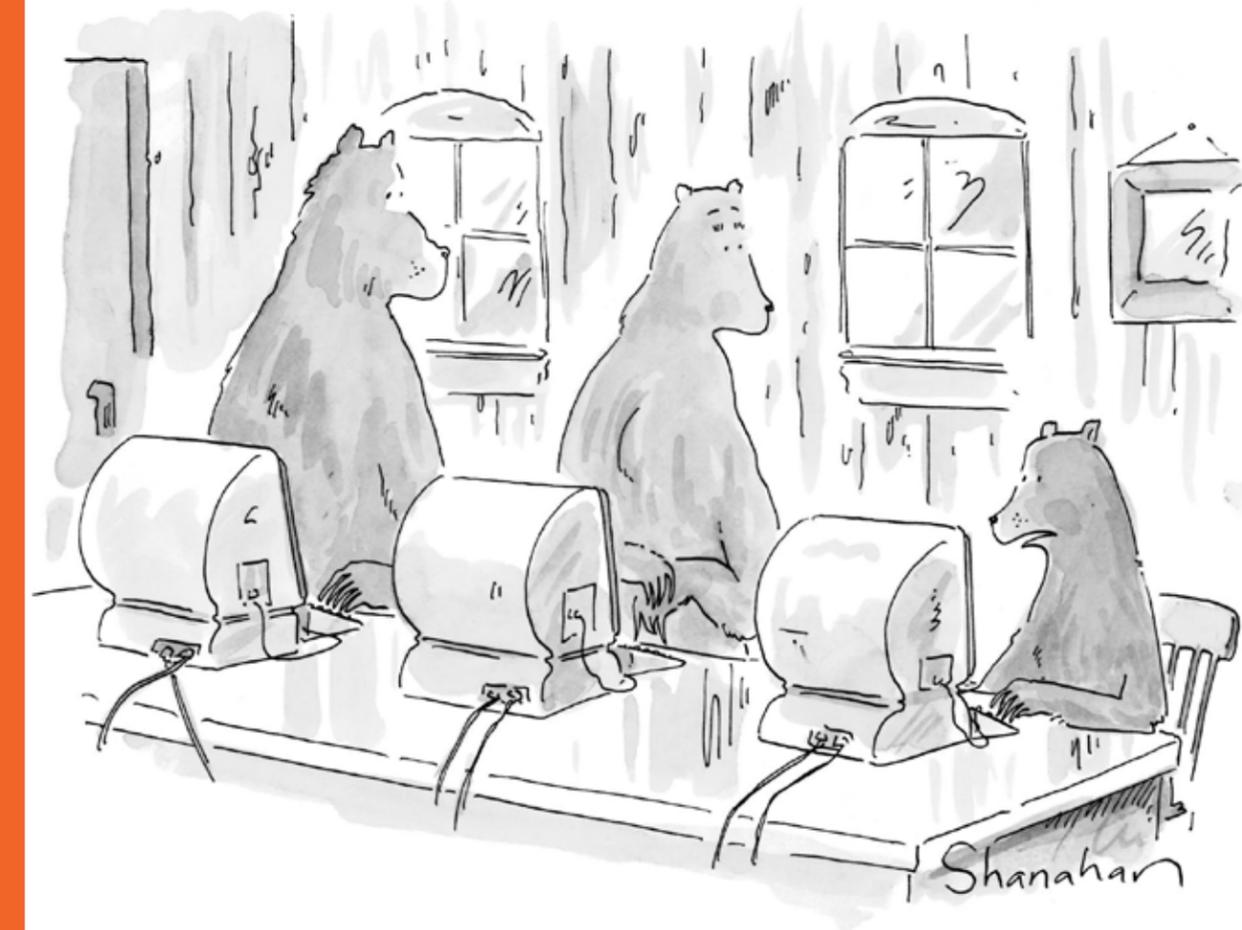
"Goldilocks added herself to our family calendar. Apparently, she's joining us for dinner tonight."

Take Control of Your Settings

Even before we open an account online and willingly share data, we share data automatically just by using a device that is connected to the internet. Both the device itself and the way we connect to the internet enable personal information to travel beyond our control, often in ways we do not realize. However, taking simple steps to limit this flow of data is easy to learn, and in many cases, something you need to do just once. Especially with on-device settings, it can be a case of set-it-and-forget-it. Your phone itself will do work to protect your data as you text, talk, call for an Uber, shop online, and do

APPLE DEVICE SETTINGS ICON

ANDROID DEVICE SETTINGS ICON

all the other convenient and fun things that can be done on a mobile device.

Building confidence
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. Some time, effort, and the right kind of support can help you break through these challenges.

Get to know your settings
Take control of data automatically shared online in the "Settings" section of your device's main menu. Settings are the controls for managing the op-

erations and connections our devices can execute. Many people never even look at their device's settings, leaving them in the factory default positions. But learning about on-device settings is easy, and it's an effective way to limit the flow of data online.

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 focus 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.

Start with passcodes

The first and perhaps most important setting to consider on your phone is the one that controls who can unlock it. Generically dubbed a "passcode," this setting protects against unauthorized access to a device. It can

take the form of a four- or six-digit numeric code and can also be called a "password" or "PIN." Increasingly, devices use biometric security to guard against unauthorized access, pairing a passcode with other measures such as

"Touch ID," "Face ID," "fingerprint," or something else along these lines.

The most important element of choosing and managing a passcode is to use something you can remember or else store somewhere safe other

than on the device. For all the wonders of Face ID or Touch ID, sometimes you WILL need the passcode to access a device, such as after operating system updates. If you have forgotten the passcode after months of not using it, getting back into a phone, tablet, or laptop can be a huge, expensive, time-consuming hassle, if you can even do it all.

In the sections on the next pages, you will find more detailed instructions for security settings on Apple and Android phones. As with the passwords discussed in the previous chapter, the passcode you use with your phone should be hard to guess, unique to the device, and known only to you. Don't use your birthday or street address or any part of your actual phone number – let your passcode be its own, distinctive self, standing tall and on its own, unrelated to other important numbers in your life!

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 passcode that uses four or six characters. As with passwords used for online accounts, longer means safer. So consider setting your phone's passcode to the six-character option, but be sure to record it somewhere safe outside your phone in case you forget it.

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 passcode options. Note that facial recognition technology on Android phones can be less advanced, and thus less secure, than Face ID on Apple phones, so it might not be the best choice for device security.

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).
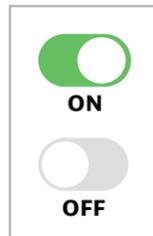
SETTINGS

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.
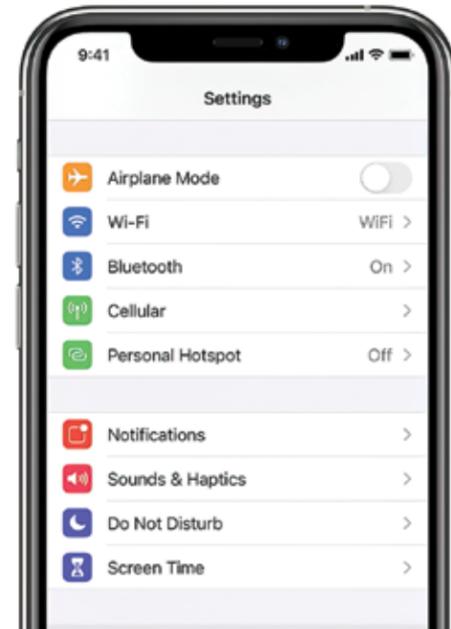
PRIVACY

ON

OFF

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 AdGuard, 1Blocker, or Wipr) Choose the one you want and add it to Safari.
- **Settings** →
- **Safari** →
- **Extensions (under General)**

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**

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**

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**

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 information 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 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.

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

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-

rangement 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 SSID

WHY IT MATTERS HOW YOU CONNECT (CONTINUED)

(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?
A public Wi-Fi network that requires a password is best. You should be cautious about 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. But on secure websites (look for the "s" after the "http" in the URL), as long as nobody is looking over your shoulder, even these kinds of transactions are okay if you need to do them in this kind of public setting.

What about public Wi-Fi that doesn't ask for a password?
In the recent past, public Wi-Fi networks not requiring passwords were easy to hack. But now, with websites widely encrypted and always-improving built-in network and hardware safety measures, the risks of open public Wi-Fi networks have greatly diminished.

THE NITTY-GRITTY: Before the nearly universal adoption of encrypted website development practices, public Wi-Fi networks transmitted user data in full view of anyone with the tools and desire to intercept and inspect this data. Things changed quickly, though, as users and administrators of such networks came to understand these risks. As long as you visit secure websites (the ones with "httpS" in the URL), use devices with fully updated operating software, and remain aware of people within view of your screen, these networks are safer than they used to be. However low the risk of the network, though, still be aware that you might be providing personal data to website owners with plans to misuse, or at least profit from, your data. Going online by way of a safe network does not necessarily mean your data is ending up in safe hands.

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 open 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.

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 Open public Wi-Fi networks can present risks to your data, but they are safer than they used to be. And you can almost always use your phone's cellular data connection to go online and avoid open public Wi-Fi altogether.

CHAPTER 3

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.

"It's free, but they sell your information."

Required: A Healthy Dose of Skepticism

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, not to mention AI
Unfortunately, this task is only be-

coming 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. 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. And the dramatic leap we have made into the age of artificial intelligence only amplifies these challenges. AI tools can boost the volume, variety, and persuasiveness of unreliable, even deceptive, content that comes our way online.

**Truth can be a scarce commodity**
In all these areas, the fake and the fraudulent too easily crowds 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.
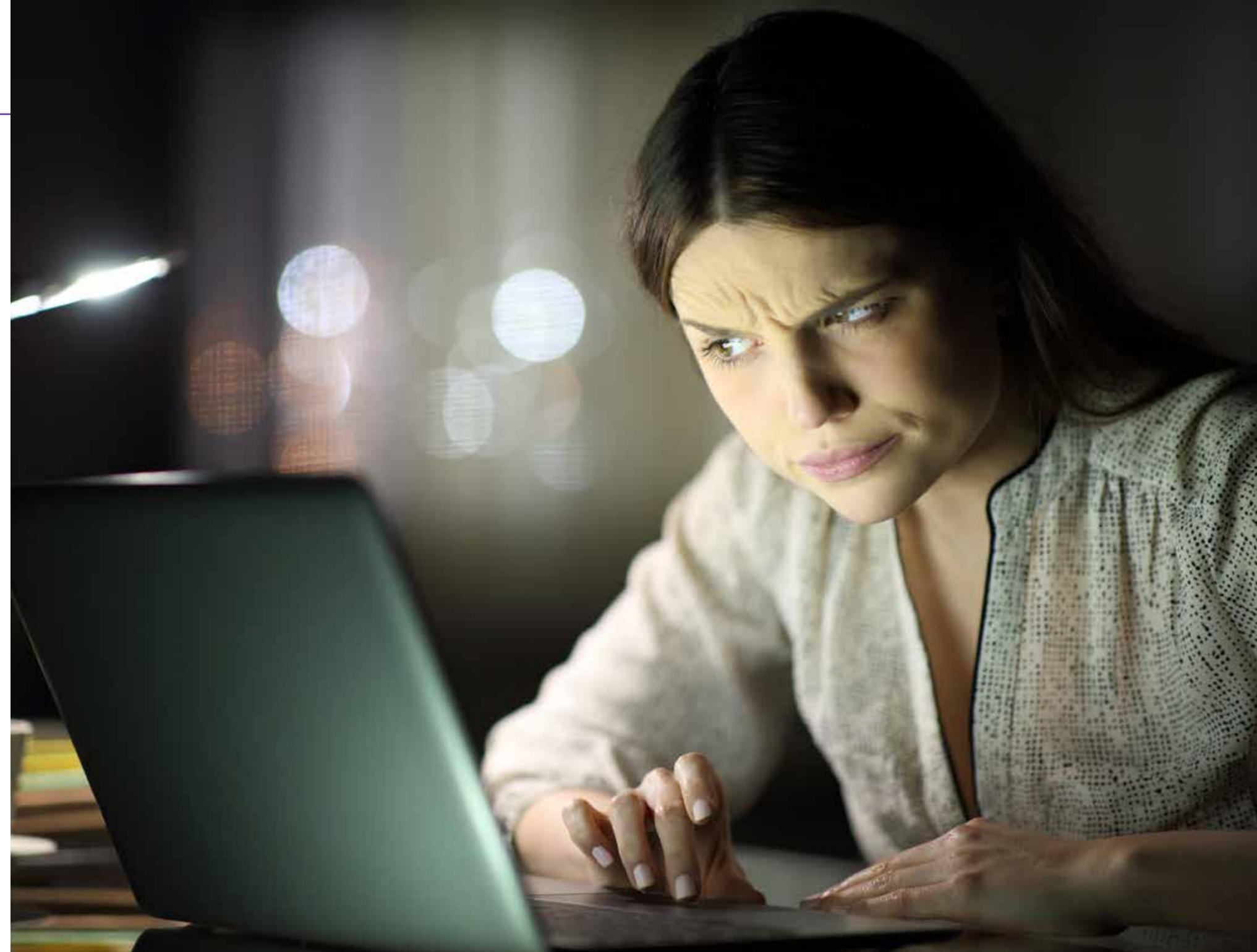
PHISHING: DON'T TAKE THE BAIT

"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.
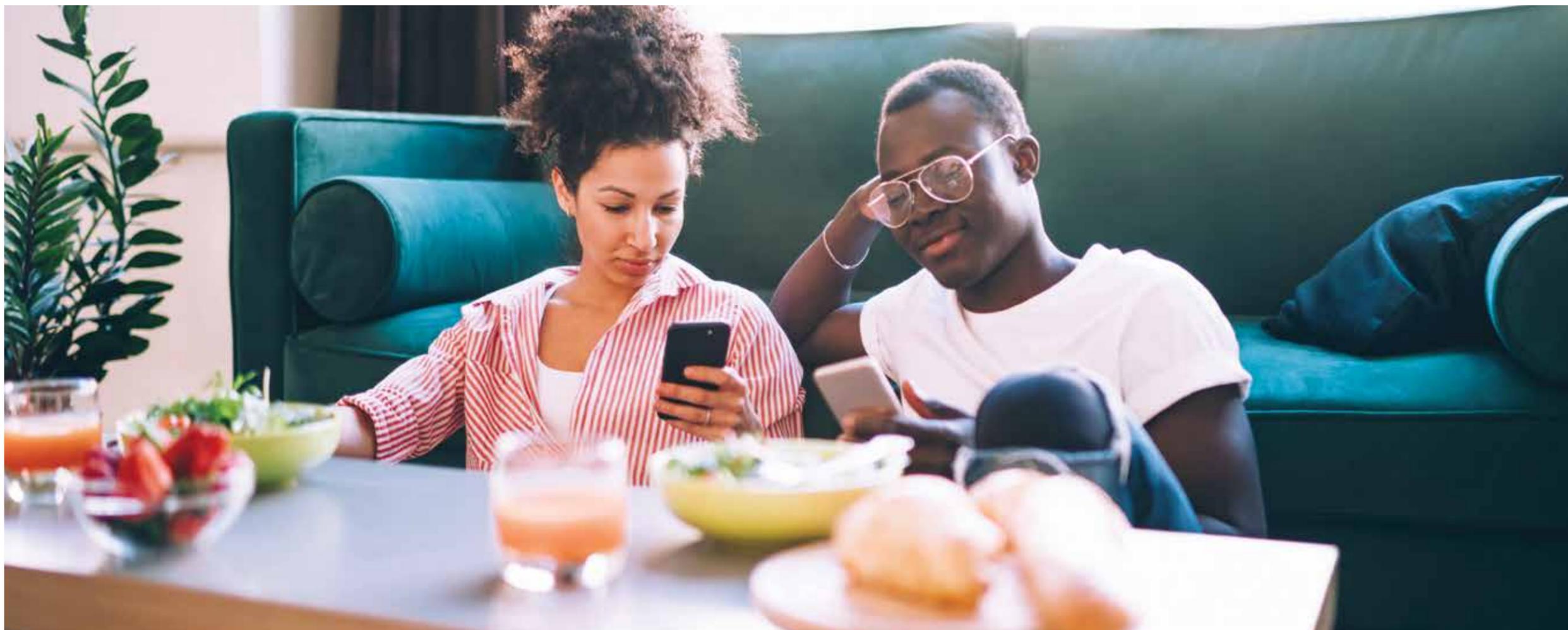
A few facts about phishing

1. Phishing is by far the most common form of cybercrime, by almost a four-to-one margin, according to the FBI.

2. Alarmingly 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.

4. AI makes it all worse. It can generate more individualized, persuasive personal details to get more people to click on things they shouldn't, automate and escalate campaigns to target many more users, and design emails to slip more readily past spam filters.

PHISHING: DON'T TAKE THE BAIT, CONTINUED

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. Many 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.**

AI & phishing

Unfortunately, AI has made it harder to identify phishing emails. AI tools enable phishing emails that read more naturally, mimic real companies' communications more closely, and include more personalized content.

A sense of urgency

Phishing emails try to prey on our emotions and desires to make us click on links or download attachments we should avoid. Even though AI makes phishing emails more technically sophisticated and realistic, it can't make the content more plausible or credible. Phishing campaigns still must work to deliver attention-grabbing, unusually dramatic messages to motivate people to read and act on them. Look out for appeals along these lines that will generally seem too good, too bad, or just or too unlikely to be true.

USPS delivery address is wrong — confirm your address to receive package

Apple ID suspended: Please verify your details

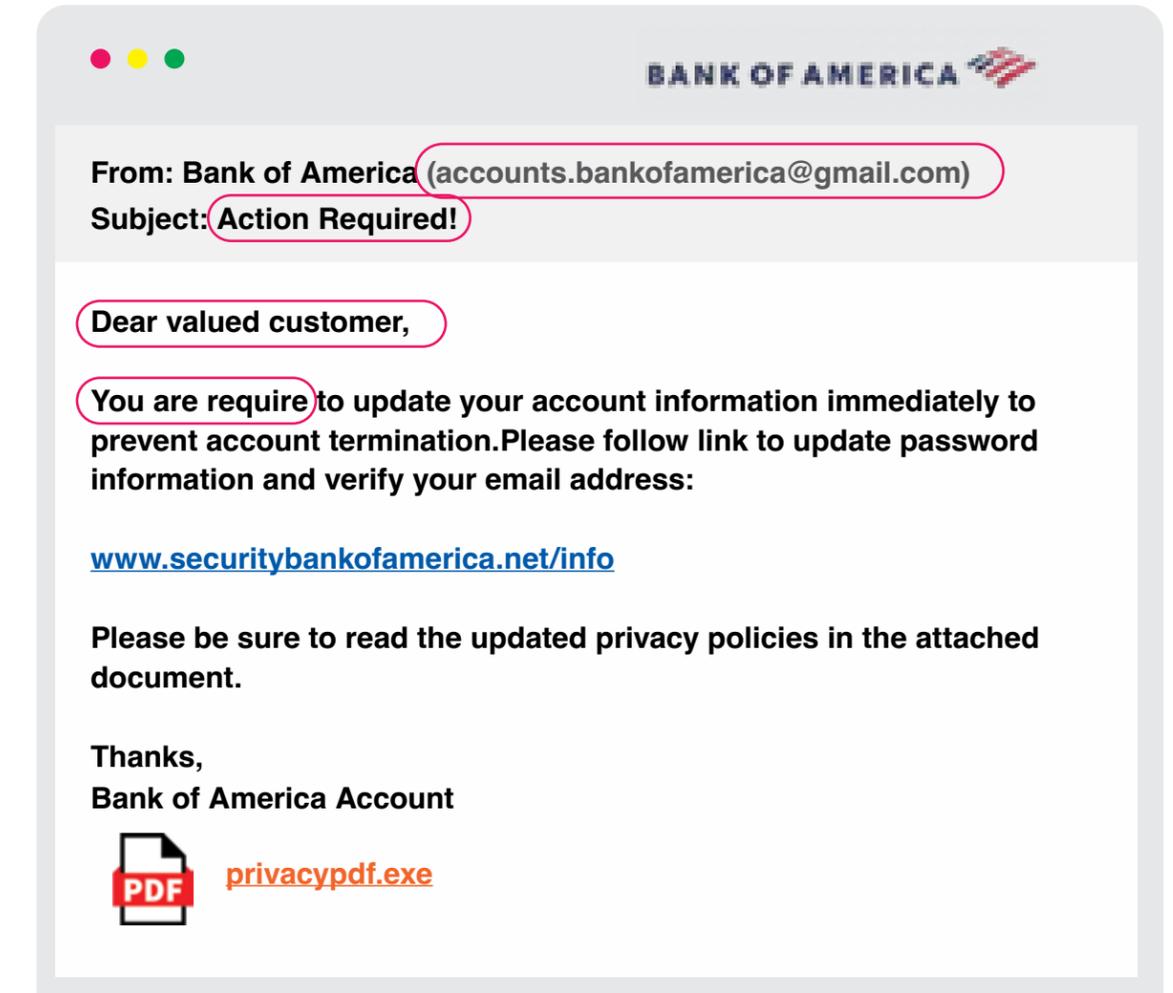*IRS overpayment notice — you have a refund waiting now!*

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.

Test your phishing-detection skills

Before the launch of ChatGPT and the ensuing flood of generative AI tools, identifying phishing emails was not that hard. The email at right shows what phishing emails, pre-ChatGPT, used to look like. The circles indicate clues to the fraudulent nature of the email.

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 page 41 for answers.

● ● ●   **BANK OF AMERICA** ⟪

From: Bank of America (accounts.bankofamerica@gmail.com)
Subject: Action Required!

Dear valued customer,

You are require to update your account information immediately to prevent account termination.Please follow link to update password information and verify your email address:

www.securitybankofamerica.net/info

Please be sure to read the updated privacy policies in the attached document.

Thanks,
Bank of America Account

📄 PDF **privacypdf.exe**

PHISHING: DON'T TAKE THE BAIT, CONTINUED

After ChatGPT was launched in late 2022, scammers quickly adapted generative AI capabilities to help them develop and send more realistic, persuasive phishing emails in much greater numbers. Within just one year, the volume of malicious phishing emails increased more than 10 times over! Even worse, AI-generated phishing emails look a lot more like real emails. They can incorporate information, names, and events personalized to the recipient's actual experience. They typically feature correct grammar and spelling. And they can present branding elements almost indistinguishable from a genuine company, organization, or government agency.

However, you can apply — and step up! — many of the same approaches to identifying old-school phishing emails to the task of identifying AI-generated phishing emails.

1. Look for the same kinds of social engineering approaches — urgency, emotional intensity, high risks or rewards identified, topics or events introduced from out of the blue.

2. The greeting will often still be generic, saying something like "Dear Customer" or "Hello User."

3. The email address and/or domain name shown in the email will be just a bit off – there might be an "o" instead of a "0" or an "l" instead of a "1" somewhere.

4. If the AI email is supposed to be coming from an acquaintance, look for slight variations in tone or vocabulary or other small details that feel wrong.

5. Attachments or links in emails you do not expect to receive are always suspicious — verify the trustworthiness of such elements with a real person in the real world before clicking on anything.

6. Look for internal inconsistencies among the subject line, text of the email, and any call to action being made. It might say "donation" in one spot and "purchase" in another, for example.

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. Don't worry about how well you do — you can take these quizzes as many times as you want.

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.

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.

In these appeals, as well, AI tools make the scams harder to identify and resist. They help scammers gather greater volumes of personal data to use in earning people's trust. Enormous volumes of personal information can be scraped from social media

accounts, business exchanges, or other sources of personal information saved to online locations open to inspection.

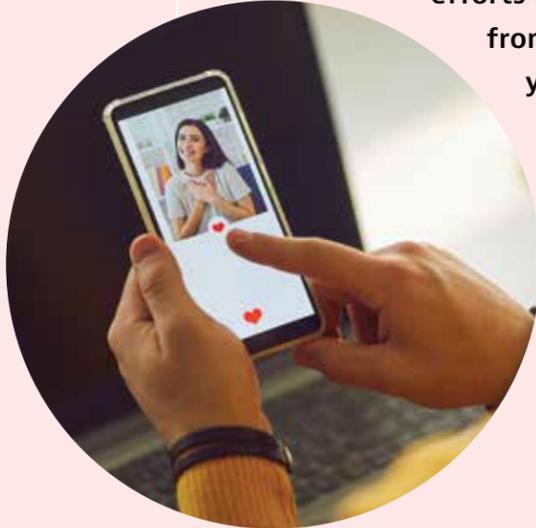Good data care practice in these cases means NOT giving up personal information, even in the face of seemingly urgent, threatening circumstances. Remember that you always get to decide what you do, no matter what someone is telling you.

COMMON SCAMS AND HOW THEY WORK

SCAM	WHAT HAPPENS	HOW TO STAY SAFE
Student loan debt forgiveness or reduction	The scam works by starting with an offer that might seem too good to be true. It could promise immediate loan forgiveness, lower monthly payments, or a limited-time offer for a special debt relief program. Combined with a short time window in which to act, the scam combines urgency with the prospect of relief from what is often a stressful financial situation. The scammer calls or emails with the offer and follows up with a request for sensitive personal information, like a Social Security Number, student loan account number, or bank account information. In exchange for a one-time fee or even a monthly payment, the scammer promises relief from current levels of debt. With information of this kind in hand, the scammer typically disappears, and any money provided is lost. In other cases, the scammer might even open up new lines of credit or take out new loans, leaving the victim even worse off.	➔ Hang up the phone. ➔ Delete the email. ➔ Don't call any numbers left in a voice or text message or email. ➔ Call the customer service number of the lender holding the loan 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.

COMMON SCAMS AND HOW THEY WORK (CONTINUED)

SCAM	WHAT HAPPENS	HOW TO STAY SAFE
Romance	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.	➔ 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.

| 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. A scammer impersonating a family member or reporting danger to a family member will call, asking for money or help of some kind in immediate fashion. The real personal information combined with possible danger to a loved one can add up to a frightening call to receive.	➔ 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. Many families establish a safe word or phrase that all members know. In a crisis situation, this shared word or phrase can verify the identity of the person on the other end. ➔ 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.

COMMON SCAMS AND HOW THEY WORK (CONTINUED)

More scams

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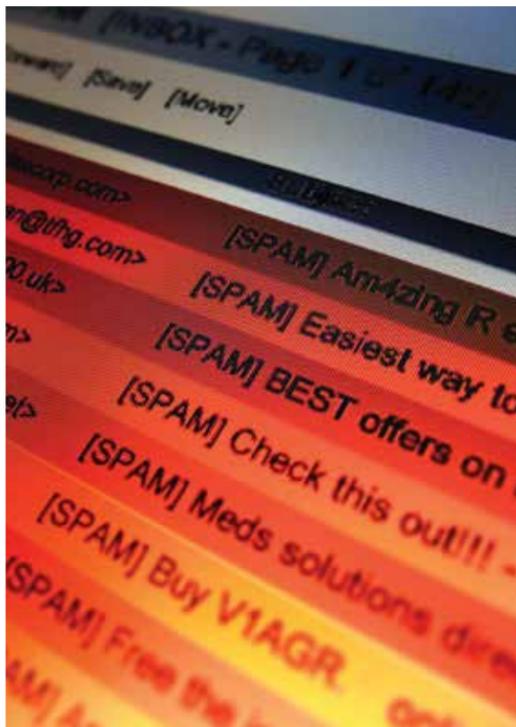
greater degree than most of us quite imagine. It is no trick at all to compile a detailed biography of almost anyone who uses the internet to stay in touch with family and friends and carry on any kind of digital life online.

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 request by calling whatever organization or person seems to be approaching you, whether bank, lender, government agency, family member, or whomever. 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.

CHAPTER 3 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.
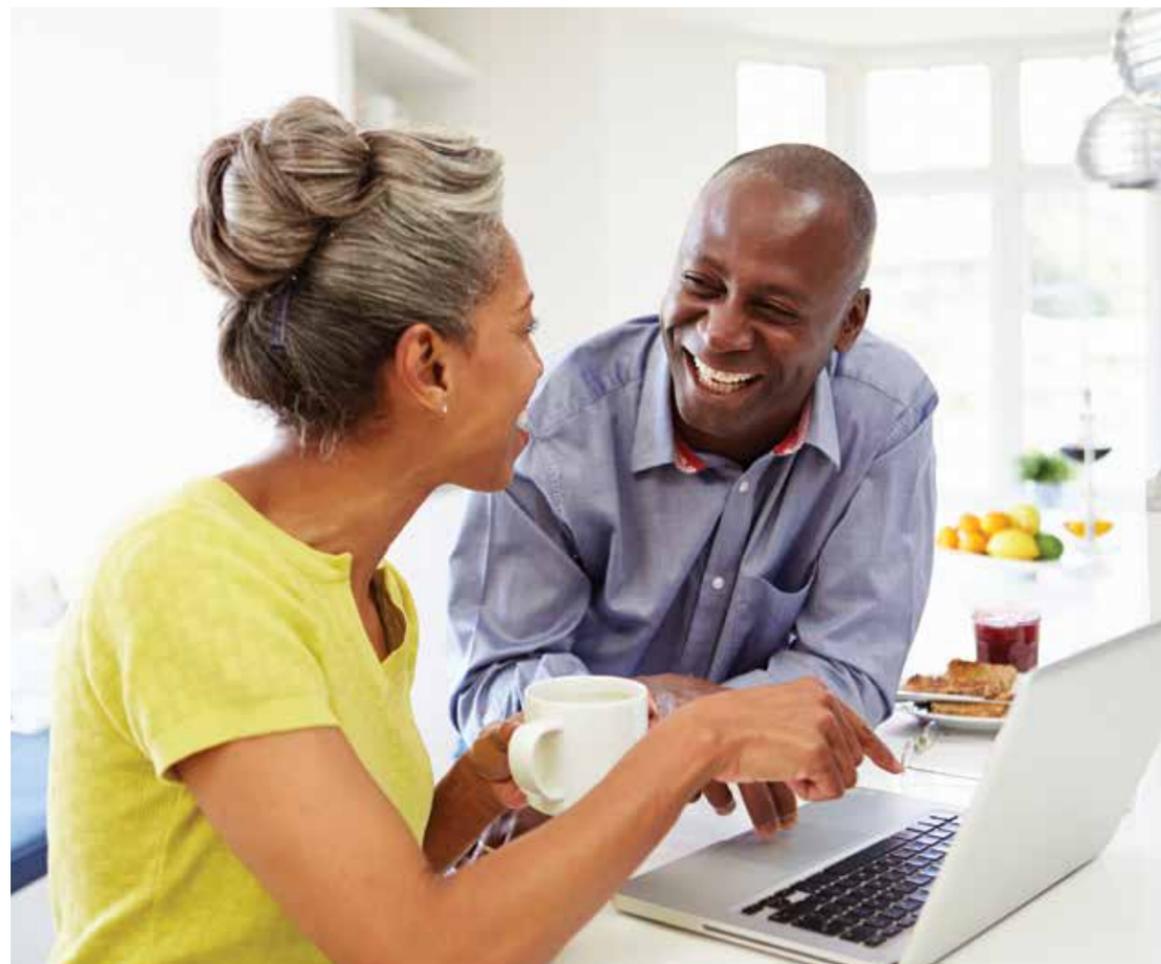
Artificial intelligence, or AI: The ability of computer systems to perform tasks that typically require human intelligence, like recognizing speech, learning from data, and solving problems. AI systems make use of large data sets, sophisticated programming, and powerful computing operations.

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

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

Availability: The need for data and storage systems to be accessible and functional any and all times users might want to use them.

Browser: An application that displays web pages. Examples include Safari, Chrome, Firefox, and Edge.

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

Cross-tracking: When companies record your browsing activity across websites to collect information about your interests and preferences.

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

criminal exploitation.

Encryption: A translation of plain-text language into ciphered text requiring a key to decode and make legible.

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

Integrity: Assurance that online data remains accurate and whole, corresponding to off-line realities and/or the owner's expectations of the contents.

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 people's computers in illegal ways.

Modem: A tool that connects computers to the internet by converting electrical signals into data that digital devices can read and use, enabling them to send and receive online information.

Multi-factor authentication: A method of providing secure access to data via delivery of a code to 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 seemingly trustworthy emails or other digital messages that actually mean to trick the recipient into giving up sensitive personal data and enabling 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. Examples include Google, DuckDuckGo, or Bing. You can access a search engine with a web browser, such as Chrome, Safari, Edge, or Firefox.

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.

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

Virtual Private Networks, or VPNs: An app or piece of software that sits on your device and encrypts data going between it and an ISP (Internet Service Provider).

WPA: An acronym for Wi-Fi Protected Access, a security protocol for encrypting data transmitted over wireless networks.

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. Your data has very likely been leaked somewhere online. **True or False?**

2. As long as you have a good password, you can use it over and over again for different accounts. **T or F?**

3. You can generally trust companies to handle your personal data with reliable security and care. **T or F?**

4. Using a password manager can be a good solution to building and managing strong passwords. **T or F?**

5. Which of these passwords is the strongest?
   A. abc321pass
   B. WoeIsYou45
   C. 4mYr!s@h0m
   D. Fidos#0418

6. 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.

7. 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 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

Chapter 3

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.

6. Scammers use AI tools to do which of the following things?
   A. Make phishing emails more individualized and persuasive.
   B. Automate scam operations to send out many more bogus emails.
   C. Scrape public sources of online information to harvest personal data about internet users.
   D. Replicate the look and feel of company or government emails almost perfectly.
   E. All of the above.

7. Of these examples of personal information, which do you think could NOT be found online?
   A. Your home address.
   B. Recent vacation destinations.
   C. Names of friends and family members.
   D. Your employment history.
   E. None of the above.

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

ADVANCING THE NATION'S INTEREST IN CYBER AND CRYPTOLOGY THROUGH LEADERSHIP, EDUCATION, AND PARTNERSHIPS.

★ NATIONAL ★
CRYPTOLOGIC
FOUNDATION

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