My iPad® for Seniors

EIGHTH EDITION

COVERS
All iPads running
iPadOS 14

AARP®

Michael Miller

My iPad® for Seniors

EIGHTH EDITION

QUE®

Michael Miller

AARP®

One of the most common techniques used by identity thieves is called *phishing*. It's called that because the other party is "fishing" for your personal information, typically via fake email messages, text messages, and websites.

A phishing scam typically starts with a phony email or text message that appears to be from a legitimate source, such as your bank, the postal service, PayPal, or other official institution. Some phishing messages purport to be from someone you personally know, such as your manager at work or your pastor at church.

Most phishing messages purport to contain important information that you can see if you tap the enclosed link. If you tap the link, you're taken to a fake website masquerading as the real site. You're encouraged to enter your personal information into the forms on this fake web page; when you do so, your information is sent to the scammer, who can now steal your identity.

How can you avoid falling victim to a phishing scam? There are several things you can do:

- Look at the sender's email address. Tap it to view more detail. Most phishing emails come from an address different from the one indicated by the (fake) sender.
- Look for poor grammar and misspellings. Many phishing schemes come from outside the United States by scammers who don't speak English as their first language. As such, you're likely to find questionable phrasing and unprofessional text—not what you'd expect from your bank or other professional institution.
- If you receive an unexpected message, no matter the apparent source, do *not* tap any of the links included. If you think there's a legitimate issue from a given website, go to that site manually in Safari and access your account from there.
- Some phishing messages include attached files that you are urged to open to display a document or image. Do *not* open any of these attachments; they might contain malware that can steal personal information from your device. (Although malware isn't as much of a threat to iPads as it is to personal computers, you still want to avoid opening unexpected email attachments.)

Malware Threats

If you're a long-time computer user, you're probably familiar with the threat posed by computer viruses, spyware, and other malicious software (malware). Fortunately, due to technological safeguards built into the iPadOS operating system, the malware risk for iPad users is extremely low. So don't worry too much about malware on your iPad—but still remain vigilant, nonetheless.

Keep Your Private Information Private

Identity theft can happen any time you make private information public. This has become a special issue on social networks, such as Facebook, where users tend to forget that most everything they post is publicly visible—and often share information about birthdays, schools attended, pets' names, and even phone numbers.

None of this might sound dangerous until you realize that all of these items are the type of personal information many companies use for the "secret questions" their websites use to reset users' passwords. A fraudster armed with this publicly visible information could log on to your account on a banking website, for example, reset your password (to a new one he provides), and thus gain access to your banking accounts.

The solution to this problem, of course, is to enter as little personal information as possible when you're online. For example, you don't need to—and shouldn't—include your street address or phone number in a comment or reply to an online news article. Don't give the bad guys anything they can use against you!

Protect Against Online Fraud

Identity theft isn't the only kind of online fraud you might encounter. Con artists are especially creative in concocting schemes that can defraud unsuspecting victims of thousands of dollars.

Many of these scams start with an email or social media message that promises something for nothing. Maybe the message tells you that you've won a lottery or you are asked to help someone in a foreign country deposit funds in a U.S. bank account. You might even receive requests from people purporting to be far-off relatives who need some cash to bail them out of some sort of trouble.

The common factor in these scams is that you're eventually asked to send money (typically via wire transfer) or provide your bank account information—with which the scammers can drain your money faster than you can imagine. The damage can be considerable.

Gift Card Scams

Another popular scam consists of an email message that looks like it comes from someone you trust—such as the pastor of your church or an executive at the company you work for. The message asks you to go to a specific store and purchase some gift cards for that person. If you do so and provide the sender with the gift card numbers, you're out that cash.

Most online fraud is easily detectible by the simple fact that it arrives out of the blue and seems too good to be true. So if you get an unsolicited offer that promises great riches, you know to tap Delete—pronto.

Savvy Internet users train themselves to recognize these scam messages. That's because most scam messages come from complete strangers and often don't even address you by name. Most of these messages have spelling and grammatical errors because scammers frequently operate from foreign countries and do not use English as their first language. Con artists know their trade well, and even the smartest, most educated people can get scammed. Knowing what to look for is key.

If you receive a message that you think is a scam, delete it. In fact, it's a good idea to ignore all unsolicited messages of any type. No stranger will send you a legitimate offer via email or Facebook; it just doesn't happen.

>>>Go Further

WHAT TO DO IF YOU'VE BEEN SCAMMED

What should you do if you think you've been the victim of an online fraud? There are a few steps you can take to minimize the damage:

- If the fraud involved transmittal of your credit card information, contact your credit card company to put a halt to all unauthorized payments—and to limit your liability to the first $50.
- If you think your bank accounts have been compromised, contact your bank to put a freeze on your checking and savings accounts—and to open new accounts, if necessary.
- Contact one of the three major credit reporting bureaus to see if stolen personal information has been used to open new credit accounts—or max out your existing accounts.
- Contact your local law enforcement authorities—fraud is illegal, and it should be reported as a crime.
- Report the issue to AARP's Fraud Watch Network, at 877-908-3360.

Above all, don't provide any additional information or money to the scammers. As soon as you suspect fraud, halt all contact and cut off all access to your bank and credit card accounts. Sometimes the best you can hope for is to minimize your losses.

Shop Safely

Many people use their iPads to shop online. It's convenient, and you don't have to bother with driving to the store and dealing with all those crowds. It's been critical during the COVID-19 pandemic.

Despite the huge upsurge in online shopping, many users are still reticent to provide their credit card information over the Internet. It is possible, after all, for shady sellers to take your money and not deliver the goods, or even for high-tech thieves to intercept your credit card information over the Internet—or from a public Wi-Fi hotspot.

All that said, online shopping remains immensely popular and is generally quite safe. You can minimize your risk when online shopping by following this advice:

- Don't shop when using public Wi Fi. Although you can shop over any wireless connection, public connections (like the kind you find at coffeehouses and restaurants) aren't secure. It's possible for individuals with the right equipment to intercept public wireless signals, and thus skim your credit card and other personal information. While this sort of data theft doesn't happen often, it's better to make your online purchases over a safer private connection.
- Shop only at secure websites. Whatever you're shopping for online, make sure you're using a website that offers secure connections. A secure web address starts with https:, not the normal http:. A secure website encrypts the data you send to it, so even if it is intercepted by a third party, that party can't read it. Most major online retailers have secure sites.
- Don't leave your credit card number on file with online retailers. As tempting as it is to have your favorite retailer store your credit card info for future purchases, that also means the retailer has a copy of it on its servers—and anyone breaking into its servers can then steal your information. Instead, enter your credit card number fresh with each new purchase; it's just safer.

If you shop at major online retailers and follow the advice presented in this chapter, you're probably going to be safe. Same thing if you buy from sellers on eBay or Etsy; those sites have their own robust security mechanisms in place. If it's a retailer you haven't heard of before, check it out by looking it up on the Better Business Bureau or doing a Google search and reading online reviews; if the reviews trend toward the negative, shop elsewhere. And always, always shop from a merchant that offers a toll-free number for customer support, just in case something goes wrong.

Do all of these things and shopping with your iPad will be not only convenient but also safe.

Fraud Watch Network

AARP's Fraud Watch Network is a free and valuable source of information about online scams and fraud. Check it out at www.aarp.org/fraudwatchnetwork.

This page intentionally left blank