Transcript - Staying Safe and Secure Online Podcast

Hi. This is Carol Kando-Pineda. I’m an attorney with the Federal Trade Commission, the nation’s consumer protection agency. One focus of my work is outreach to the military community, giving you tips and tools to avoid scams, watch your wallet, and protect yourself in the marketplace.

Today I’m going to give you some tips from OnGuardOnline.gov. That’s a cyber security site run by the FTC with its partners in the government and technology industries. Visit OnGuardOnline.gov to learn how to protect your personal information, secure your computer, and avoid Internet fraud. We all know the Internet can help us get information, entertainment, financial services, products from every corner of the world, more than ever before. But the Internet, and the fact that we can be anonymous, can also give online hackers, scammers, and identity thieves access to your computer, your personal information, and a lot more. But you can minimize your chance of an Internet mishap. To be safer and more secure online, make these seven practices part of your regular online routine.

First, protect your personal information. It’s valuable. To an identity thief, your personal information can provide instant access to your financial accounts, your credit record, and all your other assets. If you think no one would be interested in your personal information, think ahead. Anyone can be a victim of identity theft. In fact, FTC stats show that millions of people become victims every year. By the way, if you think your identity has been stolen, visit ftc.gov/idtheft to learn what to do.

So, how do criminals get your personal information online? One way is by lying about who they are to convince you to share your account numbers, passwords, and other information so they can get your money or buy things in your name. That scam is called “phishing.” Criminals send emails, texts, or popup messages that appear to come from your bank, government agency, an online seller, or some other organization that you do business with. The message asks you to click on a website or call a phone number to update your account information or maybe claim a prize or benefit. It might suggest something bad will happen if you don’t respond quickly with your personal information. In reality, legitimate businesses should never use email, pop-ups, or text messages to ask for your personal information. So to avoid phishing scams, don’t reply to those emails. Any email, text, or popup message that asks for personal or financial information -- stay away from it. Don’t click on the links in the message. Just delete it. If you want to go to a bank or a business’s website, type the address in your browser yourself. Don’t respond if you get a message, whether it’s email, text, popup, or a call that asks you to call a phone number to update your account or give your personal information to access a refund. If you need to reach an organization that you do business with, call the number on your financial statement or use a telephone directory.

Okay, so number two. This is good for any kind of business that you’re doing. Know who you’re dealing with. Know what you’re getting into. There are dishonest people in the bricks and mortar world and on the Internet. But online you can’t judge somebody’s trust worthiness with a quick gut check. It’s remarkably simple for online scammers to impersonate a legitimate business. So if you think about shopping on a site that you’re not familiar with, do some independent research before you buy. Alright, so, independent research, what does that mean? What should you do? If it’s your first time on an unfamiliar site, call the seller’s phone number so you know how to reach them if you need to. And if you can’t find a working phone number, take your business elsewhere. Type the site’s name into a search engine. If you find unfavorable reviews posted, you may be better off doing business with a different seller. You should also consider using a software toolbar that rates websites. These toolbars will warn you if a site has gotten unfavorable reports from experts or other Internet users. Some reputable companies provide free tools that may alert you if a website is a known phishing site or if they’re known to distribute spyware. Your security software may already have this feature. If so, become familiar with it and get in the habit of checking a site’s ratings before buying online.

Now, let me just talk for a minute about file sharing. It can give you access to a wealth of information: Music, games, software. Millions of people do it. This is how it works: you download special software that connects your computer to an informal network of other computers running the same software. Millions of users could be connected to each other through this software at any time. Very often the software is free and it’s easy to access. Okay, what’s the downside? It can have a number of risks. If you don’t check the proper settings, you could allow access not only to the files you intend to share, but also other information in your hard drive, like your tax returns, email messages, medical records, photos, or other personal documents. That’s a little scary. And you may unwittingly download malware or pornography labeled as something else. You could also download material that’s protected by the copyright laws, and that means you could be breaking the law. If you decide you want to use file-sharing software, be sure you read the end-user licensing agreement to be sure you understand and are willing to tolerate the potential risks of all those free downloads.

Okay. So that brings us to number three. Use security software that updates automatically. We’ve all got a million things to do and think about. You don’t want to be worrying about keeping your software active and current. At a minimum, your computer should have antivirus and anti-spyware software. And a firewall. You can buy standalone programs for each of these or a security suite that includes these programs from commercial vendors or from your Internet service provider. Now keep these things in mind. Some security software comes pre-installed in your computer. It usually works for a short time unless you pay a subscription fee to keep it in effect. It only works if it’s updated, so really, automatic is the way to go. Resist buying software in response to unexpected popup ads and emails, especially ones that claim to have scanned your computer and detected malware. That’s usually a scam. To get a list of security tools from legitimate security vendors, go to OnGuardOnline.gov. Once you confirm that your security software is up to date, run it to scan your computer for viruses and spyware. If the program identifies a file as a problem, just delete it.

Let’s talk a little bit about those specific softwares that I just mentioned. Anti-virus software protects your computer from viruses. It works by scanning your computer and incoming email for viruses, and then deleting them. Spyware software is software that’s installed in your computer without your consent. It monitors or controls your computer use. It may be used to send you popup ads, redirect your computer to websites, monitor your Internet surfing, or record your key strokes, which in turn can lead to the theft of your personal information. If your computer slows down, won’t shut down, or restarts or sends emails you didn’t write, spyware may be the culprit. So anti-spyware software helps you get rid of spyware and to avoid it. A firewall is like a guard watching for outside attempts to access your system and blocking communication to and from sources you don’t permit

Let’s talk a little bit about botnets. You’ve probably heard of these. Scammers scan the Internet to find computers that aren’t protected by security software. It’s like an open door to the rest of the Internet. They then install bad software, known as malware, through those open doors. That’s one reason why up-to-date security software is critical. You leave yourself way too vulnerable. Some spammers search the Internet for unprotected computers they can control and use anonymously to send spam. That turns them into a robot network called a botnet. That’s also known as a zombie army. The botnet is made up of many thousands of home computers that have these open doors and have been taken over by the bad software and they send emails by the millions. Most spam is sent remotely this way. Millions of home computers are parts of botnets and don’t even know it. So if you want to avoid malware, it can be hidden in free software applications, so be really, really careful about what you download.

Number four. Keep your browser and operating system up to date as well, and learn about their security features. Hackers also take advantage of Web browsers and operating systems that don’t have the latest security updates. Operating system companies issue security patches for flaws that they find in their systems, so it’s important to set your operating system and Web browser software to download and install security patches automatically. Again, automatic is the way to go. Just set it and forget it.

Number five, protect your passwords. Keep your passwords in a secure place and out of plain sight. Don’t share them on the Internet, over email, or on the phone. Your Internet service provider should never ask you for your password. If you share a computer, don’t allow a site to save your password online and keep you logged in and ready and waiting for the next person who sits down at your computer. Also, remember to log off when you leave your computer. You know, try to make it as hard as possible for hackers to guess your password. Use passwords that have at least eight characters and use numbers or symbols. The longer the password, the tougher it is to crack. So go with a 12-character password, not just an eight-character password. Avoid common words. Hackers can use programs that even try every word in the dictionary and they can do it within a few minutes. Don’t use your personal information, your login name, or adjacent keys on the keyboard as passwords. Change your password regularly, maybe every 90 days or so. And don’t use the same online password for each online account that you access.

Number six. Back up important files. If you follow these tips, you’re more likely to be free of interference from hackers, viruses, and spammers. But no system is completely secure. If you have important files stored on your computer, copy them on to a removable disk or an external hard drive and store it in a safe place.

Learn what to do in an “e-mergency.” If you suspect malware is lurking on your computer, stop shopping, banking, and other online activities that involve those user names, passwords, and other sensitive information. You’re just putting yourself at more risk. Malware could be sending all of that information to identity thieves. So, what should you do next? Confirm that your security software is up to date, then use it to scan your computer. Delete everything that the program identifies as a problem. You may have to restart your computer for those changes to take effect.

If there’s still a problem, you might want to call for professional help. If your computer is covered by a warranty that offers free tech support, contact the manufacturer. Before you call, write down the model and serial number of your computer, the name of any software you installed, and a short description of your problem. Your notes will help give an accurate description to the technician quickly. You may also need to pay for technical support. Many companies, including some affiliated with retail stores like Best Buy, offer tech support via the phone, online, or at their store or in your home. So generally, it’s going to be cheaper if you go with telephone or online help. It’s the least expensive, but you’ll have to do some of the work yourself. Taking your computer to a store is usually less expensive than hiring a technician to come to your home to repair your computer.

Once your computer is up and running, think about how the malware could have been downloaded, where it might have come from, and what you can do to avoid it in the future. Also, talk about safe computing with anyone else who uses the computer. For most people, that means talking to your teenagers. But really, anyone who uses that computer needs to know how to go on and use it safely and protect the computer. And if you do have kids in your life, go to OnGuardOnline.gov to order your free copy of Netcetera. That’s a booklet to help anyone talk to kids about safe computing practices as well as the things that they’re seeing and doing online. How to be good digital citizens, really. If you want to learn more, visit OnGuardOnline.gov. And if you think you were ripped off by an Internet fraud, file a complaint with the Federal Trade Commission. Go to FTC.gov/complaint.

And as always, you can go to Military OneSource for help. This free, 24-hour service is available to all active duty, guard, and reserve members, regardless of their activation status, and family. Consultants make referrals on a wide range of issues. Call 1-800-342-9647 or visit MilitaryOneSource.com.