

Staying Safe on Public Wi-Fi

00:01 Megan: Financial Wellness doesn't have to be hard, but it does take a little discipline and some good advice. At Golden 1 Credit Union, we're here to help, with unbiased financial advice and education. As a not-for-profit member-owned credit union, our main goal is to help you reach your goals, whether you're making a major purchase, starting an investment fund, or just looking to enjoy some peace of mind. Together we can be golden!

Hello and welcome to The Golden 1 Financial Wellness podcast. I'm Megan.

00:37 Daniela: And I'm Daniella.

00:38 Megan: Thank you so much for joining us on this festive day.

00:42 Daniela: I just love this time of year. Bring on the pumpkin spice lattes and peppermint cappuccino, all the family and friend time, social gatherings and merry making...

00:52 Megan: I couldn't agree more. The holiday season is officially in full swing, everyone is a festive mood, and holiday shopping is really ramping up.

01:03 Daniela: Yes, but this does also mean that people are often a little more distracted and less likely to be on the lookout for ID theft and other scams. We know that criminals excel at exploiting the hectic pace of the holiday season- from fake fundraising donations to lost packages and tight supplies of popular gift items. The holiday frenzy makes us all prime targets for cyber criminals. In fact, fraud attempts increase about 30% during the holidays.

01:31 Megan: Cyber fraud- on the rise- this isn't so shocking. The pandemic accelerated online shopping and other internet-based activities worldwide. The volume of personal information we're uploading to the web with each transaction increases the potential for data exposure. Each individual consumers personal information now resides on hundreds, if not thousands of servers across the globe. With that comes frequent data breaches and increased identity theft.

02:03 Daniela: That's why now is a good time to remind our listeners of how to stay safe online- particularly while using our mobile devices. You know... Like when we're standing in line at that coffee shop we seem to be visiting a little more frequently.

02:17 Megan: Let's start with being careful that we're not compromising security for the sake of convenience. Public Wi-Fi, like that at coffee shops and airports are popular targets for hackers because the online connection is unencrypted, insecure, or improperly configured. If you must use a public Wi-Fi, it's best to use a Wi-Fi hotspot that requires a password.

02:43 Daniela: And don't get public Wi-Fi sign-in confused with password level security. Lots of public Wi-Fi spots have sign-in pages. But it doesn't mean that their networks are secured. The sign-in pages are the legal fine print- outlining the terms and conditions of the page. They typically are just informing you how the Wi-Fi hotspot is using your data.

03:09 Megan: The best course of action, if you must use public Wi-Fi, is to get a virtual private network or VPN. A VPN is an inexpensive way to encrypt your data and stay safe even when connected to the airport and coffee shop Wi-Fi. A lot of businesses jumped on the VPN bandwagon when a growing number of employees started working remote.

When connected to a VPN server, your internet traffic goes through an encrypted tunnel that no one can see into- including hackers, governments, and your internet service provider. Companies use VPNs to connect to their employees to a local network at a central office. But VPN services are not only for businesses and their employees, but consumers can also get private VPNs for a small fee from their service providers. This helps keep their online activity private and ensure their internet experience is free from unwanted or outside interference.

04:11 Daniela: Another layer to public Wi-Fi security is to make sure the web pages your browsing are secure too. Try to stick to pages that begin with H-T-T-P-S rather than H-T-T-P. That extra "s" at the end stands for secure. So, remember to check the URL bar! While you're checking out that web address, look for a little padlock icon at the end of the URL. This symbol means a site is a secured with a digital certificate. Any information sent between your browser and the website is sent securely and can't be read by someone else while that information is moving from one browser to another.

04:52 Megan: Of course, you should also check your firewall and anti-malware regularly too. Firewalls are usually turned on by default on computers. But most smart phones don't have them enabled or installed. The same can be said when it comes to anti-virus and anti-malware software on computers and phones. Thankfully, a lot of VPNs come with these added layers of cyber protection already built in.

05:19 Daniela: We can't emphasize enough the importance of slowing down and being more vigilant this time of year. Accessing internet portals securely is important, but it's not going to stop all possible channels of fraud. Increased holiday shopping online is going to create a surge in fraudulent activities- like fake websites, scam emails and text messages from hackers trying to obtain your personal information to engage in some type of financial fraud or identity theft.

05:47 Megan: This just happened to me! Last week I received several text messages indicating that I was trying to make a large purchase from Amazon. Now, I have two little ones that often get a hold of my electronic devices. So, it's quite possible that they could have been trying to make a purchase. Instead of responding to the text message, I called Amazon directly and sure enough- there was no record of me trying to make any large purchase. Clearly someone was trying to initiate fraud or a scam... And this type of thing happens all the time.

06:26 Daniela: Oh, I know. Unfortunately, scammers and other malicious actors use things like emails, phone calls and text messages to lower potential victims and divulging personal information. I've had scammers wanting me to buy gift cards, send them verification codes and answer personal questions about my credit. Spam filters on your email box can help, but it won't eliminate all spam. So never open an attachment or click on a link from an unsolicited email. Cleverly crafted links can take you to a phony website set up to trick you into divulging private information or downloading viruses, spyware, and other malicious software.

07:06 Megan: Remember: Even emails sent from a familiar email address- like a friend or a family member may be a scam. Many viruses are spread by scanning a computer and then sending fictitious emails from you to your contacts. I've seen this countless times through email chains or on social media; the hacker starts posting content or reaching out to your friends and family claiming to be you to obtain their personal information. If this happens, it's important to change your passwords

Staying Safe on Public Wi-Fi

right away and notify your connections that your account may have been compromised.

07:47 Daniela: If you receive a call, email or text message from someone you don't know- never provide that person with any information, especially if they sound pushy or claim to be in an urgent situation. If you're suspicious about the validity of the call or online inquiry, reach out to the actual business or service provider directly to see if they are really trying to get a hold of you.

08:12 Megan: I know we've covered a lot of information, but I hope that everyone finds it helpful and has learned a thing or two about security on public Wi-Fi and how to stay safe around scammers and hackers- especially around the holidays.

And remember, if you haven't already done so, subscribe to the Golden 1 Financial Wellness podcast on Apple, Google, and Spotify to get more financial tips and insights. Plus, go to the financial wellness tab at golden1.com to find a ton of other resources like videos, interactive modules, and webcast. You don't even have to be a member to use them!

Thank you so much for joining us today. This has been Megan.

09:20 Daniela: And Daniela.

09:21 Megan: Wishing you financial health and happiness- and as always, reminding you to.

09:24 Daniela and Megan: Stay golden!

09:05 Megan: Hey Daniela, does this mean we can go get some coffee now?

09:08 Daniela: You know it. I just ordered a couple of Peppermint Mochas for pick up so we don't have to use the public Wi-Fi and can come back to the office to work.

09:15 Megan: Awesome, you're the best!

09:19 Megan: Golden 1 Credit Union is insured by NCUA.