ArchBridge Family Office

Are You Vulnerable to Identify Theft?

Imagine your identity as a puzzle. Each piece of the puzzle provides a hint to your identity. With enough of the pieces in place, one can ascertain the complete picture and assemble the rest of the pieces accordingly.

Whether in the physical or virtual realm, protecting your identity from bad actors requires keeping the pieces of the puzzle obscured enough so that the picture remains incomplete. In the physical world, you lock your doors and windows, place valuables and important documents in a safe, and avoid leaving behind obvious signs of being out of town, like a pile of newspapers gathering on your lawn. In the virtual world, this means ensuring the virtual pieces of the picture are protected just as well.

Currently, fraud committed against individuals online is rampant. According to the Aite Group, 47 percent of Americans experienced financial identity theft in 2020. Losses from identity theft cases cost an astonishing $502.5 billion in 2019 and increased 42 percent to $712.4 billion in 2020. According to consumaeraffairs.com, Internet of Things (IoT) devices – devices such as smart watches and smart home accessories – experienced more than 1.5 billion attacks in the first half of 2021.

While the cyber world can seem overwhelming and uber technical, there are some very simple steps you can take that will go a long way in keeping your identity secure. I've outlined three easy and effective steps to help protect your identity from bad actors online.

Step 1. As a first line of defense, ensure your Wi-Fi network is secure.

The increasing volume of people working from home over the past several years has paved the way for many criminals to steal personal information. Why? Their personal Wi-Fi networks aren't secure, which is akin to leaving every window and door to your home unlocked and wide open 24 hours a day. Fortunately, there are some simple actions you can take to better secure your information, so you don't become another FTC fraud statistic. The first line of defense is your connection to the digital world.

Give your Wi-Fi network an unidentifiable name.

If your name is Joe and your home Wi-Fi network is named "Joe's Network", there's an excellent chance that criminals will be able to link that network to you. It's the first piece of the puzzle that could provide them with information to steal your identity. If the criminals are successful in figuring out your passwords, they'll then have access to your personal information. Therefore, it's best to name your network something obscure so hackers can't associate it with you. Phrases from movies like "ThatsafactJack" or "Therainingspain" are hard to trace to a specific person yet easy for you to remember.

Always secure your networks with a password that is unique to you.

Another no-no is using the factory passwords printed on the labels of your modem and wireless router. A bad actor could use that relatively public information to connect to your network and have access to all

your data. Ask yourself, “do I know and trust the installer that my internet provider sent out? Would I willingly give this person my password?” If not, you should be sure to change the factory passwords to prevent the installer’s ability to sell or use your data. Additionally, if possible, set your router to generate notifications alerting you when a new device connects to your network.

If working while away from home, always confirm the name of the network with the provider.

Hackers are known to create networks that look like the one you’re trying to access, say, in a coffee shop or on a flight. Don’t assume that because its name is familiar means that it’s safe. Verify it with the network owner before logging onto it. Additionally, remember that once connected to a wireless network, the owner of that network can monitor all your traffic. Utilizing a VPN can mask some of this information, but nothing is impenetrable. The best practice if you are traveling and/or on a public Wi-Fi network, whether the connection is encrypted or not, is to avoid using credit cards or other personal information like your social security number.

Step 2. Be mindful about what you reveal on social media.

Social media can provide a treasure of clues to cybercriminals trying to piece together the puzzle of your identity. As a quick self-assessment, think of the last time you did a credit check or accessed a bank account and had to verify your identity. How many of your answers to your security questions could you get from your social media feed? Taking a cautious approach about what information you share can help keep your vital information safe from their clutches.

Don’t broadcast you’re away from home.

Just as you wouldn’t put a sign in your yard telling everyone you’re out of town, I recommend avoiding posting vacation pictures and travel stories while you are physically away. Also, don’t use the ‘check in’ option that alerts people to where are you. Why? This is akin to advertising to cybercriminals that your defenses are down. You may be spending more money than usual while on vacation and, if you’re traveling abroad or just “checking out,” you may be less vigilant about monitoring account balances and emails. Fraudulent charges won’t be as obvious and by the time you’re aware that you’ve been hacked, the trail to the criminal will have cooled.

Be wary of games and quizzes.

While some games and quizzes are completely innocuous, bad actors sometimes surface on social media in the form of tantalizingly fun ones. A few years ago, there was a popular app called FaceApp that would show your image at a certain age and allow you to post it on social media. While novel and seemingly harmless (if not slightly disturbing to see extra wrinkles in your visage!), the app was collecting names and photos and storing them on servers indefinitely. The Russian-based app company could turn around and sell that data to third party organizations, a scheme which the FBI labeled as a ‘counterintelligence threat.’ Whether it’s a serious threat to national security has yet to be proven, the point is that people who shared this information have no control over it once it’s on that company’s servers.

As a rule of thumb, think about what you would say about yourself in a large, crowded airport with a

microphone. My guess is that you wouldn't be rattling off your most private information. Be sure to act with the same caution when using social media.

Step 3. Be savvy about your passwords.

Because of rampant fraud, the need for impenetrable passwords is ubiquitous. Many people joke that their passwords are so good, even they can't access their pertinent information. Passwords are the keys to your most sensitive information and are a necessary evil, so I've detailed some ways you can use them smartly without making it to unwieldy for you to manage.

Don't be so obvious.

Think about your passwords. Do you use your kids or pets' names? Spouse's birthday? Maybe you think using your favorite vacation spot as a password will foil an identity thief. Think again. Be vigilant about variety. Maribeth Concannon, founder of Blink Solutions, a personal technology consulting firm, sees a common mistake individuals make in their personal digital security. "Some clients use the same simple password over and over – and once one account gets hacked it's a race to try to keep ahead of the damage to other accounts on other websites."

Instead of your birthday or a pet's name, which can easily be hacked, using a phrase or sentence is more secure. Consider what is probably the safest way to choose a password – using one that is algorithmically generated.

Enlist the help of a password manager.

Concannon says clients often seek her help in managing passwords because they have become unwieldy and difficult to remember. She recommends using a password manager, which is essentially a digital, encrypted vault and offers an additional layer of digital protection. LastPass, 1Password or Dashlane are all reputable password managers that offer both free and paid versions.

These three simple but effective steps can go a long way in keeping your private information protected. We recommend revisiting these steps regularly as a check-in to assure that you're safeguarded against a criminal solving the puzzle of your online identity. Vigilance is the best defense against any sort of crime. Just as you are cautious about leaving clues in the physical world that would give a criminal access to your home or possessions, be equally as attentive to your online security.

Zach Leeds
Principal

ArchBridge Family Office is an independent, multi-family office and trust company that advises 65 clients on more than $13 billion of investment assets and more than $15 billion of total wealth. Founded in 2002, ArchBridge Family Office provides holistic, high-touch client service including customized, independent investment management and a full range of family office and fiduciary services. The firm serves a limited number of clients with substantial wealth in order to maintain very low client-to-employee ratios. Visit archbridge.com to explore how the firm manages complexity with unmatched expertise and a Family, Forward focus.