Let’s Talk Finances

Worry About Cybercrime? You’re Not Alone.

By Charles Schmalz
President of
East Wisconsin Savings Bank

Nearly a quarter of Americans, 23%, were victims of cybercrime in 2018. That’s down just slightly from the 25% who reported being targeted in 2017, according to Gallup's 2018 crime survey data. Survey respondents were more likely to say a household member has had their personal, credit card, or financial information stolen by computer hackers than report being victimized by any of eight other forms of criminal activity.

Gallup has previously found that Americans are more concerned about falling victim to cybercrime or identity theft than any other forms of criminal activity. Seventy-one percent of Americans worry about cybercrime and 67% about identity theft. The public's level of worry about these two types of crimes is substantially higher than worry about any other type of criminal activity and, based on their reported levels of victimization, is justified.

However, there are some steps you can take to reduce your chances of becoming a cybercrime victim.

Step up your password game. Many people use the same password for multiple accounts, which means that if your credentials are stolen for one account, all your accounts are in jeopardy. Do you really want to give criminals access to your bank account because you used the same credentials for your free online music account? It also helps to use very strong passwords on all of your accounts (especially if you still use the same password in multiple places). Do not use your name, birthday, or pet's name, as this information is readily available to many people, especially if you post it on social media. The best passwords are often derived from an entire phrase, rather than a single word, and incorporate letters, numbers, and special characters. For example, the song lyric "Don't worry. Be happy." can be transformed into this password: d0ntwry_Bhpy.

Beware of phishing scams. The dangerous thing about phishing scams is they don't rely on weak website or network security. Instead, they attempt to crack the human firewall: you. Phishing scams attempt to obtain personal information or plant a virus or malware on your device by sending a fake email requesting that information or instructing the recipient to click a link in order to reset their account. Never give out your personal information over the internet, phone, or via text message unless you know exactly who you're dealing with. If you receive a suspicious email from a business or charity and you're not sure if it's legitimate, close the email, open a new browser, visit their official website, and use the information published there to contact their customer service department. If you didn't initiate contact, it's always best to be suspicious.

Avoid using public Wi-Fi to buy. Shopping online may be convenient — especially during the holiday season when shoppers pack into the mall like sardines — but when you shop online, keep in mind that any purchases made via the web require transmitting your credit card and/or bank account information over the internet. Using a public Wi-Fi connection to do so puts that sensitive information at risk. Hackers can tap into unsecured Wi-Fi connections at hotspots like coffee shops and airport terminals to capture your information. If you're using a wireless connection to shop, be sure that it requires a password or WEP key. Websites that have additional security protections have https:// instead of http:// on all pages of the site, so watch for that, as well.

If you have questions about how to protect yourself and your family from cybercrime, check out the tips offered by the Federal Trade Commission at https://www.consumer.ftc.gov/features/feature-0038-onguardonline or talk to your local banker!