Threats to Your Data—and What You Can Do About Them

More than ever in this modern world, you are your data. And more than ever, that data is at risk. The bad guys are getting ever more creative with the tactics and techniques they use to scam, steal and sell your digital and physical information footprint.

All of this means you need to be ever more vigilant about protecting your data from threats that include the following:

1. Fraud and scams. It's pretty likely that you've experienced phishing or "smishing" attempts via email or text. With possession of your password or other login credentials, cyber crooks could attempt to access your bank and brokerage accounts (or your crypto wallet).

One recent trend has been to use generative AI to spoof the voices of people you trust. A bad guy might impersonate a loved one with remarkable accuracy and con you into wiring money with the ruse that someone you care about is in distress.

2. Identity theft. Your stolen identity also could be used for an array of other exploits—for instance, to file false tax returns and steal refunds. Or your pilfered ID might be used for medical fraud, with the crooks using your name to get hospital care, incurring big bills in your name. They could also use social engineering tactics to scam your friends and family members by posing as you.

And it's a major hassle to clean up a case of identity theft—just think of the mounds of paperwork and how many different agencies, banks and businesses you'll need to call.

3. Blackmail, extortion or worse. Stolen online data or physical media—sensitive emails, documents, photos, etc.—could be held for ransom, or used to extort or manipulate you with threat of exposure. If you're a person of a certain level of wealth or notoriety, such exposure could cause great financial or reputational harm.

Even worse, private information could be used in more dangerous exploits, such as attempted kidnapping or attacks, should bad actors discover your whereabouts by gaining access to your calendars, travel logbooks, smart home systems or even social media posts that indicate your location.

4. Business risks. Poor data protection habits could also pose a threat to business interests you may have. A hacked email account or a carelessly misplaced laptop could be bad news for your company if you're an owner, a C-suite leader, an investor or a board member, with cybercriminals gaining access to contracts, M&A details, intellectual property or other sensitive business information. If those documents were to be leaked and publicized, costly and time-consuming legal issues could follow.

Continued on back page

Steven C. Jackson, CWS®, CPFA™
Senior Vice President, Financial Advisor

Steven C. Jackson, Jr., CFP®
Senior Vice President, Branch Manager, Financial Advisor

Chalyda Dumayas, FPQP®, CWP
Senior Registered Financial Planning Associate

D|A DAVIDSON

JACKSON FINANCIAL ADVISORS
A member of D.A. Davidson & Co. member SIPC

301 N. Lake Ave., Suite 800 | Pasadena, CA 91101 | (626) 449-0330 | sjackson@dadco.com | dadavidson.com | JacksonFinancialAdvisors.com

Continued from front page

TAKING ACTION

The good news: There are more action steps than ever that are designed to thwart the criminals. Here's a list of some key areas to pay attention to and some steps you can take that are aimed at mitigating your risks

- **Online basics.** Most of these you should know and be practicing already. Don't click links in emails you don't recognize, and definitely do not open or download any attachments from suspicious-looking emails. Keep your social media sharing to a minimum—not everyone needs to know where you are at any given time. They don't need to know your address or your birthday either.

- **Device security.** Keep your software updated to make sure you've got access to the most recent security patches. Antivirus software is a good investment, particularly if you're using Windows or Android operating systems, and even for macOS users. Full-disk encryption tools such as BitLocker and FileVault aren't always necessary, but they offer a measure of protection should your device ever get stolen. And, of course, always enable two-factor authentication whenever it's available, and be sure to use an ever-changing set of unique alphanumeric upper- and lowercase passwords that incorporate symbol characters.

- **Identity protection.** If you're not actively in the process of financing a big purchase, it's worth considering freezing your credit with the three major bureaus—Equifax, Experian and TransUnion—to protect against fraud. Keep a close eye on your bank accounts and credit card statements, and be on the lookout for activity that's not yours.

- **Offline.** Protecting your paper trail is important. Shred sensitive documents such as financial statements, medical records and any credit offers that arrive unsolicited in the mail. Be careful with phone calls too. Don't give out any personal information unless you have initiated the call and it's to a verified number. And let calls from any number you don't recognize just go to voicemail.

Much about these protection efforts comes down to what are known in the cybersecurity world as "human factors." That said, there is some tech that can help—software and other tools that can protect your information online and off.

Some browser extensions offer a measure of protection with capabilities like content filtering that can block trackers and malicious code. Password managers help centralize your credentialing, with other capabilities including breach alerts and dark web scanning.

Two-factor authentication devices offer physical two-factor authentication, rather than SMS codes, which can be vulnerable to SIM swapping. Online, virtual private networks offer encryption that increases protection, especially on public networks.

Then there are the identity theft monitoring services that aim to keep a close eye on your credit activity and other footprints of your online presence, and will notify you of incidents such as dark web leaks or other suspicious activity.

For physical assets and files, you can avail yourself of any number of "smart" filing cabinets—many of which also bill themselves as fireproof—to store your important documents under the protection of numeric PINs and biometric technology. And when you don't want all that paper anymore, you can convert the pages into PDFs that are filed away in encrypted cloud storage. Then you can shred the originals.