WHEELER
Wealth Management

FLASH REPORT

Eric D. Wheeler, CFP®
Branch Manager, Wheeler Wealth Management
306 Middletown Park Place, Unit B · Louisville, KY 40243
P (502) 200-7225 · F (502) 473-6562

Foiling the Financial Fraudsters

Financial fraudsters are working overtime to target those of us with significant assets. *Even worse:* They're having far more success at parting us from our wealth than you might imagine.

The upshot: Just because you're "good with money" or careful in who you deal with when it comes to finances doesn't mean you won't be pursued by financial scammers—nor does it guarantee you'll avoid their traps.

With that in mind, consider some of the key ways you may be targeted—and what you can do to avoid these scams.

You're a target

Consider just how focused these criminals may be on you and your wealth: The affluent are 43% more likely to experience identity theft, according to research done by Experian and the Department of Justice.

The good news is that you can take steps to better protect yourself from financial scams and fraud. A good first step is to get a handle on the many ways the crooks are trying to get at you and your money—and the damage those efforts may cause.

1. Phishing and ransomware attacks. A type of online scam, phishing occurs when scammers impersonate a legitimate company using legitimate-looking emails or texts. You, acting under the assumption that the communication and the links in it are trustworthy, inadvertently share sensitive data with the crooks. Ransomware is a type of malicious software that encrypts your files in a way that makes them inaccessible to you, then demands a ransom for the "key" to get them back.

Ransomware has commonly targeted big businesses and large organizations, which of course have mission-critical technology and deep pockets. That said, small businesses are now the targets of 82% of ransomware attacks—likely because they're seen as easier prey with less adequate security measures.

2. Wire transfer fraud. This occurs when criminals fool you into wiring money to them. Often they do so by presenting themselves (via an email or a text) as a trusted individual or organization, such as a family member, a business partner or even a charity. One well-publicized example: Real estate investor and "Shark Tank" judge Barbara Corcoran was scammed out of nearly $400,000 after criminals pretending to be Corcoran's assistant emailed Corcoran's bookkeeper to wire funds to pay for a nonexistent investment property.

3. Account takeovers. This is a type of identity theft in which scammers get unauthorized access to an online account—for example, by setting up a legit-sounding public Wi-Fi network and using it to capture usernames, passwords and payment information.

AVOID GETTING SCAMMED

Armed with insights into how scammers might come at you and your wealth, you can start taking steps to avoid them or shut them down when they try to strike. Some ideas to consider:

1. **Check your "basics."** Secure your home network, use strong passwords and multifactor identification, and install anti-malware and other internet-security programs. Such plain-vanilla safeguards should form the foundation of your efforts.

2. **Slow down and use caution.** Many financial criminals demand that potential victims act quickly, creating a false sense of urgency to their pitch. That means one key move is to resist the urge to take immediate action, giving you time to dig deeper. Communicate this expectation to your financial professionals, too—advisors, insurance specialists, bookkeepers and so on. Tell them to double-check any financial transaction requests—especially ones marked urgent—with you directly.

3. **Verify requests independently.** Say you get an unsolicited email (or text or call) from your financial institution, the IRS, tech support, etc. demanding that you take action immediately. Rather than click on the link provided to you, call or email the person or company directly to determine whether the communication is legitimate.

4. **Root out impersonators.** Would-be online fraudsters often create fake accounts on social media that they use to gather intel they can use against you. Alert the companies if you see that someone has set up a profile claiming to be you, don't accept friend requests until you verify them as legit, and don't respond to requests from complete strangers.

5. **Separate your personal life from your business life.** Entrepreneurs should consider using different email addresses for family communications and business communications. This can help prevent a hack in one area of your life from spilling over into the other.

6. **Check in on your finances.** Review your financial statements for odd or unfamiliar transactions or any unauthorized activity. The same goes for credit reports and other statements that involve your wealth. This won't prevent you from getting scammed—but it can help you identify possible fraud and shut it down as soon as possible.

7. **Ask for help if you need it (or even think you might).** Even when people get scammed or worry they may be stepping into a fraudulent situation, they often don't tell anyone or reach out for advice or help. They fear that admitting they've been duped will make them look stupid or weak. Don't fall into that trap: If you think you're getting taken, enlist the help of the authorities, trusted advisors or others to review the situation and offer potential next steps.

8. **Consider hiring experts.** Fraud prevention firms catering to the affluent can build bespoke strategies designed to wall you off from financial fraud. Other services can monitor social media for scam accounts or posts that could threaten your wealth.

Note how many of the tactics to avoid getting scammed involve personal behaviors rather than high-end technology. Using both together can be more impactful, but it's important to remember that keeping financial criminals at bay can depend greatly on the actions you take—and don't take—when interacting with the world around you.