

Protect Yourself Against Financial Scammers

It's unfortunate but true: During this period of economic uncertainty, one of the busiest "industries" has been financial scamming. But it goes on even during normal times, so you'll want to know what to look for and how to defend yourself.

For starters, just how widespread is financial fraud? Consider this: In 2019, more than 3.2 million fraud cases were reported to the Federal Trade Commission, with identity theft being the most common type of fraud, accounting for about one-fifth of the overall cases. And fraudulent new accounts (mortgages, student loans, car loans and credit cards) amounted to about \$3.4 billion in 2018, according to a study by Javelin Strategy & Research.

To prevent yourself from being victimized, consider the following suggestions. They are certainly not exhaustive, but they should prove useful.

- *Watch out for unsecure websites.* Make sure a website is secure before entering any payment or personal information. Look for sites that start with HTTPS, rather than those with just HTTP, which are not secure and can be hacked. But even a site with HTTPS can still be used by scammers, so, if you don't recognize the name of the company or group that's requesting your information, do some research to make sure it's legitimate.

- *Review your credit reports.* As mentioned above, the fraudulent opening of new accounts is a big source of financial scams. To be sure nobody has opened new accounts under your name, try to review your credit reports at least once a year. You can get them for free at AnnualCreditReport.com.

- *Follow up on fraud.* If you've already been victimized by having new accounts opened in your name, contact one of the three major credit reporting agencies (Experian, Equifax or TransUnion) and place a 90-day fraud alert on your credit file.

You might also want to file a complaint with the Federal Trade Commission, print it out and file it with your local law enforcement agency. And it's also a good idea to contact the fraud department of the financial companies where the thief has opened a fraudulent account in your name.

- *Be alert for suspicious links.* "Phishers" have gotten quite good at sending out messages that look like they're from reputable businesses. But if you examine these messages carefully, you can usually determine if there's something off about them. For example, no legitimate business will tell you, via this type of message, that you have to "correct your account" by providing additional information. And if you do hit the link provided and it takes you to a third-party site, you can be pretty sure it's bogus.

- *Resist "act now" offers.* If you get an offer via phone or online urging you to "act immediately" on an investment opportunity, discontinue the communication. No reputable financial advisor will ever try to force you to take such swift action, and if an investment is legitimate, it will be available tomorrow, next week and next year.

- *Use your shredder.* You probably have the option to "go paperless" with all your financial services providers, but, if you still do receive paper documents, be sure to shred them when they're no longer needed.

You save and invest for years to help achieve your long-term goals. Don't let any of your efforts be undone by financial fraudsters.

This article was written by Edward Jones for use by your local Edward Jones Financial Advisor.

Edward Jones, Member SIPC