

Steps to Help Protect Yourself from Financial Fraud & Scams

F

requently check your financial accounts and credit reports for suspicious activity.

A stolen credit card or hacked account can go unnoticed, so it pays to be vigilant. Most financial institutions will reimburse you for any stolen funds.



R

egister your phone number with the National Do Not Call Registry.

It's a free service managed by the Federal Trade Commission that is designed to help reduce the number of illegal sales calls you get.



A

ssure your passwords are secure.

Shoot for passwords that are 8-10 characters long with both capitalized and lowercase letters and at least one number and special character. Also, avoid recycling passwords among your online accounts.



U

tilize extreme caution when engaging with people online.

Scammers like to frequent social media, dating websites, Craigslist and other similar websites to reach potential targets. Be careful what you share online, even seemingly trivial information.



D

o online searches.

Type a company or product name into a search engine with words like "review," "complaint" or "scam." Or search for a phrase that describes your situation, like "IRS call."



Steps to Help Protect Yourself from Financial Fraud & Scams *(continued)*

S

Stay calm.

Scammers like to prey on people's emotions. They typically try to scare or trick you into believing something is scarce or a limited time offer. They use high-pressure sales tactics to get you to act before you can think.



C

Consider all unsolicited emails, calls, texts and letters a scam.

Maintain a healthy sense of skepticism. Don't click on links or open attachments in unsolicited email. Government organizations like the IRS won't call you, unless you ask them to call you.



A

Avoid sharing personal information with any person or business that you don't trust.

This includes banking and credit card information, your birthdate and Social Security number. Passwords should never be shared.



M

Make sure your online transactions are legitimate and secure.

Scammers have gotten better at imitating company logos, official seals, websites, email addresses, fonts and other details. Look for "https" in the URL and a small lock icon on the address bar. Steer clear of any site that asks for a non-traditional payment method.



S

Seek independent professional advice.

Before you provide personal information, send money or make an investment, talk to a financial adviser, accountant, or even the teller at your local bank. Not all scams are as obvious as the Nigerian prince with poor grammar and a severe allergy to money. An outside opinion can help reveal red flags you may have not noticed.

