Protect yourself from financial fraud and scams

RBC Wealth Management

While anyone can become vulnerable to financial scams, retirees and aging seniors have increasingly become new targets. The idea of a scam affecting you may be unsettling, but there are many ways to protect yourself. Recognizing these common scams, and how to avoid them, can help confirm you and your wealth stay safe.

Lottery/sweepstakes scams

These scams involve some form of financial windfall. First they tell you that you've won something or are eligible for money. Then they ask you to send money upfront to cover fees, taxes, tariffs and/or advance payments. Never send money to get money.

Romance scams

In this scenario, someone you've never met in person attempts to entangle you in an emotional relationship by frequently contacting you through a dating website or email. This "love interest" then asks for money to help them see you in person or move closer to you. That's the last you see of them. And your money.

Gift card scams

Gift cards work like cash and have become an easy way for scammers to steal money. The key to avoiding this type of scam is to remember that no reputable business or organization requests payment by gift card.

Government imposter scams

The scammer pretends to be an official with the IRS, DEA or other agency, often spoofing the phone number to look legitimate. They demand payment and create fear. These scams often involve gift cards or moving funds to a "secure treasury account."

Person-in-need (grandparent) scams

The scammer tries to contact you on behalf of someone you care about—a grandchild, for example—who is in trouble or needs money immediately. Always fact-check and confirm the story with another family member before sending money.

Computer tech support scams

A pop-up message, email or call tells you that your device is compromised and provides a link or phone number to call. The scammer then charges large fees to "fix" the non-existent problem or tries to gain access to your computer to steal your information.

Charitable giving scams

After catastrophic events like a hurricane or flooding, phony organizations pop up with the promise to help those in need. Before you make a donation, always check that the charity or company is legitimate. A reliable place to look is www.ftc.gov/charityfraud.

Internet investment fraud

While the internet is full of investment advice and legitimate investment sites, it's also home to many criminal schemes including "pump and dump" investments, pyramid schemes promising to turn a small investment into a big payday, and "risk-free" investment offers. Do your research, take your time and think twice before you invest in opportunities you found online. You can also report any "risk-free" investment solicitation emails to the Securities and Exchange Commission at enforcement@sec.gov.

Unsolicited sales calls

Cold callers may try to put you off-guard with kind words or by suggesting they've spoken with you or someone you trust before. Watch out for these tricks:

- High-pressure sales tactics
- "Once-in-a-lifetime" opportunities
- Investments in companies with amazing new technologies
- Callers who refuse to send you written information before collecting money

To stop receiving cold calls, add your name to the National "Do Not Call" Registry at (888) 382-1222 (TTY: (866) 290-4326) or www.donotcall.gov.

Phishing

Some criminals try to get your personal information by sending you emails saying they are from a reputable business or government agency. They then take your information to open fake accounts, make credit card purchases or wire funds. Never give your personal information, including Social Security number, over the phone or email.

Business email compromise

This is a scam where a fraudster impersonates a legitimate third party (such as a title company, contractor or attorney) or business executive to send fraudulent payment instructions. Because the recipient was expecting the payment instructions, or frequently receives instructions from the sender, they accept the instructions as authentic and initiate a funds transfer or give away sensitive information.

Having a trusted contact person is important

At RBC Wealth Management, if we think you may be a victim of fraud, we will contact you. Fast action can help resolve issues more quickly. A trusted contact person is someone you authorize us to contact if we are unable to contact you directly. This person should be someone you trust, such as a family member, friend or professional you depend on, like an accountant, attorney or trustee.

Your trusted contact person will NOT be an authorized party on your accounts, nor will we accept instructions from them that will affect transactions and/or change account information in any way. It's simply another way for us to reach you if we need to.

To add a trusted contact person to your account, contact your financial advisor with their name, address and phone number.

Knowledge is power

Con artists tend to target older Americans because they are more likely to have financial assets. In addition, many physical and emotional conditions due to aging can make them more susceptible to fraud and exploitation. As always, at RBC Wealth Management, helping you protect your finances is a top priority.

In addition to providing you information about rising or changing trends in financial exploitation, we are increasing our efforts to protect you from them. Our Client Risk Prevention group is providing robust, proactive training and resources to help every financial advisor work to prevent, detect and report any suspected financial abuse. If you have any immediate concerns, please contact your financial advisor.

What to do if you're concerned

If you suspect you or a loved one has been a victim of fraud or financial abuse, call your RBC Wealth Management financial advisor for immediate assistance and support. You should also:

- Cancel credit cards linked to your account
- Reset passwords on accounts and on email
- Contact local authorities or your state attorney general (if applicable)

Additional resources

The Federal Trade Commission includes an extensive library of educational content about fraud protection and filing a complaint on its website: www.ftc.gov.

The Financial Industry Regulatory Authority offers fraud prevention information and resources on its website: www.finra.org/investors/avoid-fraud.

The Securities and Exchange Commission has a wealth of practical consumer awareness information on its website: www.sec.gov/investor/pubs.shtml.

The FBI has a valuable library of information on scams and safety: www.fbi.gov/scams-and-safety.

21-04-03170_0410 (12/21)