OSBORNE PARTNERS
Capital Management, LLC

Effective Strategies to Protect Your Finances in a Growing Age of Scams and Fraud

By: Tom Piro CFP®, Enrolled Agent

July 2023

As financial scams become more sophisticated and believable, it is increasingly important to educate yourself and protect your finances.

Have you ever received a suspicious email, text, or phone call from someone saying they're calling from the Postal Service, another government agency, or a financial institution, asking you to provide confidential information or complete a survey? You're not alone. These are imposter scams designed to take money from you.

Imposter scams come in many varieties but work the same way. And unfortunately, these scams are becoming more sophisticated and believable. Scammers use high-pressure tactics to persuade unsuspecting people that they need to pay up or hand over personal information to quickly resolve an issue. Now with artificial intelligence, scams and fraudsters can take their scams to new levels.

For instance, a recent attempted scam made headlines in April. The scammer used a technique called "caller-ID spoofing." The scammer called a mother, claiming to have kidnapped her daughter. The scammer used artificial intelligence "voice cloning" to mimic the sound of her seemingly distraught daughter's voice. The scammer then demanded a $1,000,000 ransom in exchange for her daughter's safety.

Thankfully, the daughter was always safe, and the event was nothing more than an attempted scam. However, it reinforces the importance of being aware of scams like these and taking action to protect yourself. This is especially true, as the probability of your bank refunding your money is far from guaranteed. For instance, had the mother wired money to the scammer, it is unlikely her bank would have refunded her (even though she was under duress and a victim of a scam).

I believe the best protection against frauds and scams is to educate yourself. In this article, I'll share general best practices, along with the more important strategies and tactics that my family and I use to protect ourselves from scammers and fraudsters.

What I recommend, after reading the general rules, is starting and completing the "Simple Actions," which as the name implies, are quite simple. Then, move onto the "More Involved Actions."

Effective Strategies to Protect Your Finances in a Growing Age of Scams and Fraud

These are important steps to protect yourself but are still pretty easy. The "Advanced" section of recommended actions are things I do personally, but I recommend completing everything in the other sections before advancing to these.

General rules to protect yourself:

- **Be skeptical:** Be skeptical of too-good-to-be-true offers, or urgent situations, that just need some of your information. Verify that the entity contacting you is legitimate before giving out information. A quick web search of the agency or individual will go a long way. Same goes for emails.
- **Don't trust your Caller ID:** Scammers are pros at manipulating Caller ID systems to show the caller information they want displayed. Even if the Caller ID shows the name of an official organization, it does not guarantee that the person on the other end works for them.
- **Don't engage:** If you receive a call from someone urgently requesting security passcodes, account/ personal information, or money, this is a red flag. Don't spend any time asking questions. Hang up.
- **Never pay for a prize:** If someone informs you that you've won a prize, you should not have to pay any taxes, delivery fees, or insurance payments to collect it.
- **Call someone directly and have a family safe word:** If scammers have claimed to have kidnapped a loved one, call that person directly and have a family safe word.
- **Don't send a wire transfer or gift card:** These are all ways that scammers ask to be paid with urgency. And remember, if you are the person who clicks on "confirm wire transfer," it is unlikely your bank will reimburse you for money wired out of your account (even if you were under duress).

Simple Actions:

- **"Tap to pay" instead of swiping:**
  - ⇒ At the checkout counter, instead of swiping your credit card, place your card within a few inches of the payment terminal to initiate payment.
  - ⇒ Most credit cards use Near Field Communication ("NFC"), which is a short-range wireless technology that allows devices to communicate and exchange data by simply bringing them close together. NFC has a number of applications and is commonly used for contactless payments.
  - ⇒ This technique is currently among the safest forms of payment. Compared to magnetic strips that are more easily duplicated by hackers or thieves, it's incredibly difficult for a hacker to

recreate the one-time code that contactless credit cards create for each transaction. This makes contactless credit cards much more secure.

- **Protect & update your devices:**
  - ⇒ Keep your computer, smartphone, and other devices updated with the latest security patches and antivirus software. Enable automatic updates whenever possible.
- **Use only trusted networks:**
  - ⇒ Be cautious when using public Wi-Fi networks, like at an airport, coffee shop or hotel, as they can be vulnerable to hacking. Avoid accessing sensitive information or making online transactions while connected to public Wi-Fi unless you're using a secure virtual private network (VPN).
  - ⇒ An alternative to using public Wi-Fi networks is using your mobile phone as a hotspot. To do so, turn on your personal hotspot (usually found under your phone's settings), then connect your laptop/device to your phone's hotspot, and enjoy your secure internet connection!

More Involved Actions:

- **Get a credit freeze at the major credit bureaus:**
  - ⇒ One of my biggest concerns is the risk of someone opening a credit card or taking out a loan in my name.
  - ⇒ To prevent this, credit bureaus (Experian, TransUnion and Equifax) offer a credit freeze or a fraud alert to be applied by creating an account with them. This prevents someone from fraudulently opening a credit card or taking out a loan in your name, and you finding out too late.
  - ⇒ A credit freeze or a fraud alert does not affect your credit, and there is no fee associated with either option.
- **Use a password manager:**
  - ⇒ Password managers provide secure and encrypted storage for all your passwords, reducing the risk of unauthorized access and potential data breaches. By generating and storing complex, unique passwords for each of your accounts, you minimize the likelihood of successful hacking attempts or credential theft.
  - ⇒ Password managers also streamline the process of managing your passwords. They automatically fill in login credentials, eliminating the need to remember multiple passwords or

repeatedly input them. This saves time, reduces frustration, and encourages the use of strong, unique passwords across different platforms and websites.

- **Use Multi-Factor Authentication (MFA):**
  - ⇒ To further enhance your online security, I recommend protecting your account with a strong secondary measure, typically a single-use code. This is referred to as "multi-factor authentication," or MFA.
  - ⇒ Multi-factor authentication adds an extra layer of security by requiring a second (or even a third!) verification step, such as a unique code sent to your phone, in addition to your password. In fact, all of our systems at Osborne utilize MFAs.
    - ♦ See next section for taking MFA to an even higher level of security.
- **Secure your physical mailbox:**
  - ⇒ Always retrieve your mail promptly. Personally, I use a locked mailbox.
  - ⇒ Shred or destroy any documents containing personal or financial information before disposing of them.
    - ♦ At home, I have a simple $40 paper shredder, which is all I need to shred old financial statements or other documents with sensitive information.

Advanced Actions:

- **Use *Physical* Two Factor Authentication:**
  - ⇒ I personally use physical MFA. This offers the highest level of online security protection.
  - ⇒ It is different than the above MFA examples (which use text messages or applications), as it is a physical security key. Physical MFA can be a little dongle that you plug into a USB port or tap on your phone during account logins, as an enhanced level of security.
  - ⇒ Why are they so effective? Security keys protect you in two ways: First, there's no electronic authentication code for a hacker to steal. Second, physical MFA uses a security protocol to verify the website's domain during login, so they won't work on fake sites.
  - ⇒ Physical MFA keys typically cost between $25 - $50. I simply attach it to my key chain (it is about the same size as a thumb drive) and carry it with me.

Effective Strategies to Protect Your Finances in a Growing Age of Scams and Fraud

- **Research before making online purchases from new vendors and sellers:**
  - ⇒ Before making purchases from unfamiliar websites or sellers, research their reputation and read reviews from other customers. Stick to reputable online marketplaces and ensure that the payment process is secure.
  - ⇒ If something gets bad reviews, or doesn't feel right, walk away. (Remember earlier advice, "be skeptical").

I recognize there are other actions you can take to protect yourself from scams. However, for your time and money, these are steps I recommend and personally follow. Please feel free to reach out to us should you have any questions or would like to talk through the subject in greater detail. ■