Second Quarter 2023

Preventing Fraud Can Save You from Financial Disaster

There are a lot of people out there who think they have just as much of a right to your money as you do. And they have no hesitation to hacking into your accounts or defrauding you in person. Your digital phone may be your greatest vulnerability. If you notice anything unusual happening with your phone - excessive data or battery use, poor or bizarre performance, unrecognized text messages or apps on your phone or apps opening and closing unexpectedly, it's time to get very worried.

There has been a tremendous surge in financial fraud, so once again we are cautioning clients, family and friends that they must take steps to protect their financial assets.

1. Understand what phishing attacks are and never ever give account numbers, login IDs or passwords in response to emails, phone calls, or internet alerts. Contact your financial institution, the IRS or whoever the contact claims to be directly to verify any suspicious contacts.
2. Use two or multi-factor authentication to log into financial accounts, credit cards, and companies such as Amazon or PayPal that have your payment information.
3. Only download verified apps from reputable websites, such as the App Store or Google Play.
4. PIN protect the SIM card in your phone. Do not allow a salesperson to change the SIM card or use a new one sent to you in the mail. Contact your provider if you have questions.
5. Set email and/or text alerts to monitor bank and investment accounts for fraudulent activity.
6. Use unique, strong passwords for each financial provider and change them periodically.
7. Do not save financial passwords on your phone.
8. Use your device's security functions to protect data – including the ability to track your stolen device, disable it and wipe it remotely.
9. Consider using a Virtual Private Network (VPN). With a VPN no one can see what you are doing online and no one will know who you are or where you live.
10. Don't share too much personal information on social media, such as vacation plans, major purchases, etc, that open the door for a fraudulent approach.

If you do nothing else, set account alerts! The sooner you can detect a problem the faster you can shut accounts and devices. Use both text and email alerts depending upon the importance of the alert.

Make certain your financial advisor verifies any transaction instructions with a personal contact and NEVER include account information when emailing instructions to your advisor.

Remember you have NO PROTECTION if your debit card is hacked. Once money is withdrawn from your account it is gone. Credit cards do have protection against fraudulent charges, but you need to understand the limits of that protection.

If you think you have been hacked, contact your banks, financial accounts, and credit cards to freeze your accounts. Close accounts with access to bank and credit card accounts such as Venmo, PayPal, Amazon, etc. Let trusted friends and family know you have been hacked and to alert them to watch for suspicious messages or activity. Delete programs you do not recognize or

from third party sources.

Don’t count on help from law enforcement or the government to recover funds lost to digital fraud. It is too prevalent and too sophisticated in many instances for their abilities to trace or identify the source.

Technology is a wonderful tool, but it can also be used against you. You are responsible to take steps to prevent hacking and financial fraud.

Brian R. Carruthers, CFP, CMT

BCA
BRIAN CARRUTHERS & ASSOCIATES

Your Conservative Advisory Firm Since 1990
301 Forest Avenue
Laguna Beach, California 92651-2115 USA
Telephone: 1-949-464-1900
www.gobcafunds.com
brian@gobcafunds.com