Second Quarter 2023

Do You Trust Your Phone a Little Too Much?

Most cell phones contain enough data to allow scammers to steal your identity, access your financial accounts to engage in credit card fraud or even empty your bank accounts. Passwords, PINs, passcodes, account information etc. are valuable currency for hackers. Using your personal phone for work could even give a hacker access to your company's data and networks.

Android devices tend to be more vulnerable to hackers, but iOS devices can also be hacked, and hackers don't have to steal your phone to do so. Fake Wi-Fi networks can redirect you to malicious sites. Phishing emails or texts can contain malicious links. SIM card swaps can transfer your phone number to the hacker's device and provide access to your accounts.

Some basic steps to protect your phone:

- Keep phone and apps updated.
- Use a Virtual Private Network (VPN) to create a secure tunnel between your device and the internet.
- Turn off Wi-Fi and Bluetooth when not in use.
- Avoid public charging stations. Use portable power packs if you need to charge while traveling.
- Lock your SIM card.
- Avoid downloading apps from third-party app stores.
- Keep your phone safe from theft.
- Use strong unique passwords.

For more information on fraud defense, read *Preventing Fraud Can Save You from Financial Disaster* in this newsletter.

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