# Make sure you button up your personal account security from thieves.

**Fred Dunbar**
**CLU®, ChFC®, RFC®, AIF®**

*We bring quality services to the shore, providing a "common sense" approach to pursuing our clients' financial goals for over thirty years.*

**Financial Planning* Asset Management* Investment Planning* Retirement Planning**

## COMMON ¢ENTS PLANNING

**1-800-647-0762**

**239 Baltimore Pike Glen Mills, PA • 6606 Central Ave. N. Sea Isle City, NJ**
**fdunbar@commoncentsplanning.com • www.commoncentsplanning.com**

*Securities offered through Commonwealth Financial Network, Member FINRA/SIPC. *Advisory services offered through Planning Directions Inc., a Registered Investment Adviser, are separate and unrelated to Commonwealth.*

**KEEP THE HACK OUTTA HERE**

By Fred Dunbar

"Complacency" is defined by Merriam-Webster as "self-satisfaction when accompanied by an unawareness of actual dangers or deficiencies." When we discuss cyber threats and cybersecurity, complacency can be dangerous to both individuals and businesses.

Recently in the news, there was a cyberattack in May on the Colonial Pipeline, which crippled the Southeast. Colonial Pipeline shut off gasoline supplies to much of the Eastern Seaboard, resulting in shortages particularly in the South, where there were long gas lines along with many service stations left with no gas. In June, there was an cyberattack on JBS S.A., which resulted in a huge disruption of U.S. beef operations and the payment of an $11 million ransom.

We look at large companies being attacked, and that might not generally resonate with us. These companies can usually pay the Bitcoin ransom request that the hackers demand to unlock their computer systems. We don't think of small businesses or individuals as being susceptible. However, nothing can be further from the truth. These cyberthreats have become commonplace, especially during the pandemic. With much of America working remotely throughout the past year-and-a-half, cybercriminals have had more opportunities to identify and exploit individuals' and companies' vulnerabilities.

Nas Benmederbel, director of security engineering at Commonwealth Financial Network, advises us on best practices to avoid common cyberthreats. Some of his do's and don'ts may be helpful in protecting you:

**MOBILE SCAMS**

- Do verify phone numbers by calling the institution/firm directly.
- Do utilize any phone scam identification services offered by your wireless provider. Contact them to see what is available.
- Don't open any links in text messages.
- Don't provide personal or sensitive information or passwords to incoming callers. Only give information to the company you are speaking with if you initiated the contact to their official number.

**EMAIL PHISHING**

- Do delete the email.
- Do verify the sender by directly calling the number from the company's official website.
- Don't give out passwords or personal information until you validate the request.
- Don't click suspicious links or open attachments.
- Don't forward or respond to these emails.

**MALWARE INFECTIONS**

- Do update your browser and operating system before using the internet.
- Don't open attachments without verifying them.
- Don't download software from untrusted sources.

**PASSWORDS**

- Do create unique, complex passwords of at least 10 to 12 characters, using a combination of uppercase and lowercase letters, numbers, and symbols.
- Do update your passwords regularly, at least every 90 days.
- Do use a power phrase that is easy to remember but hard to guess. For example, "I am Secure Today" would look like #1@m$3cur3T0d@y
- Don't reuse old passwords.
- Don't use the same password for multiple accounts.
- Don't use the "save password" feature.

Are you having trouble keeping track of all of your passwords? Consider using a password manager — essentially an encrypted digital vault. It stores your all of your passwords that you use to access apps and accounts on your phones, tablets, and websites. In addition to keeping your information safe, the best password managers will create strong passwords.

We recommend our clients change their account passwords regularly. When we ask when they last changed their passwords, amazingly some will say they never have. Does that sound familiar? Excuses we've heard: "It's too hard," or "It's too time-consuming." If you think changing your password is difficult, wait until someone hacks into one of your accounts. If someone steals your personal information, they will gain access to your bank, credit-card, and investment accounts. Perhaps you saw the 2013 movie, "Identity Thief." The comedy follows a businessman, Sandy Patterson (played by Jason Bateman), who travels from Denver to Florida to confront Diana (Melissa McCarthy), who has been living it up after stealing Sandy's identity. "Identity Thief" might be funny as a movie but not in real life, especially if it happens to you.

How can you help protect yourself against identity theft?

First, review your credit report at least annually to make sure that all of your information is correct. Everyone is entitled to a free credit report every 12 months from each of the three reporting agencies: Equifax (888-766-0008), Experian (888-397-3742), and Trans Union (800-680-7289). If you find that your information is inaccurate, contact the appropriate credit rating agency to let them know that you're disputing the information. Do this in writing — either online or by mail. If you are including documents that support your claim, send them via certified mail. This way you have a paper trail to rely on if this investigation does not resolve your dispute. The agency usually must investigate any dispute within 30 days of receiving it, and you will receive a written response.

Another way to proactively help protect yourself is to contact credit-card companies to have them add alerts to your account(s). I have alerts on my credit cards, so I receive an e-mail or text each time they are used. Review your bank and credit-card account statements at least monthly. Today, many people pay all of their bills automatically online and never review the statements. It is important to regularly look for any suspicious charges or account activity that you do not recognize. If you discover any inappropriate financial transactions, contact your financial institution as soon as possible.

If you feel that your personal information has been exposed, consider adding a fraud alert and/or a security freeze. A fraud alert requires any creditor to take extra steps to verify your identity before extending existing credit amounts or issuing new credit in your name. To add a fraud alert, contact one

of the three aforementioned major rating agencies, and they will pass this request to the other two rating agencies. A security freeze prevents new credit-card accounts from being opened in your name. Once you establish a security freeze, creditors will not be allowed to access your credit report; therefore, they cannot offer new credit. Unlike the fraud alert, you must contact each of the three credit-rating agencies individually to place a security freeze. Keep in mind, if you go to buy something such as a home or new car or to rent an apartment, you will have to unlock the security freeze. There is generally a small fee to do this.

One last thing we recommend is to make a copy (front and back) of everything you carry in your wallet or purse. In the event your wallet or purse is stolen, you will have all the account and phone numbers so you can contact each company. This will save you a lot of aggravation by not having to guess what was in your wallet.

Now that you have taken steps to button up your personal security, lather up and head to the beach with your favorite beverage, book and chair.

Fred Dunbar, CLU®, ChFC®, RFC®, AIF®, is President of Planning Directions, Inc., a registered investment adviser, and Common Cents Planning, Inc. He also offers securities through Commonwealth Financial Network, member FINRA/SIPC. Advisory services offered through Planning Directions, and fixed insurance products and services offered by Common Cents Planning, are separate and unrelated to Commonwealth. Fred may be contacted at 800-647-0762, by e-mail at fdunbar@commoncentsplanning.com or by mail at 239 Baltimore Pike, Glen Mills, PA, 19342. He's always happy to meet with you "down the shore" at 6606 Central Avenue N. Sea Isle City, NJ, 08243.