PFPG Fee-Only Advisors

PORTLAND FINANCIAL PLANNING GROUP, LLC

News & Views / September 2018

In this issue: E-mail hacking; new Medicare cards; top senior scams; job link

www.pfpg.com

Have you been hacked?

While the news about Russian election hacking dominates the headlines, everyday cyber-crooks are still diligently trying to part you from your money. If your e-mail account has been hacked, your friends and family may let you know that they've received e-mails from you that you never sent containing odd links or requests for money transfers. Your social media account shows posts you didn't post, or you can't log in at all. What steps do you need to take?

1.) If you don't have any **security software** on your computer – why not? There are reputable free versions of applications that can scan your computer for viruses (*Avast* for PCs, for example) and spyware (*Malwarebytes*). Run them and make sure your computer is clean, and repeat regularly. Also make sure the most recent security updates for your operating system have been installed, and set your computer to update automatically. If your techie skills aren't up to this, get professional assistance or the help of a trusted and knowledgeable friend.

2.) **Change your passwords** if you are able to log in to your account. Your e-mail provider or social media platform may have steps to help you regain control of your account if you can't. And be especially suspicious of any unsolicited emails directing you to reset your password on a vendor's website. This particular scam sends the recipient to a copycat website where a hacker can capture your legitimate log-in credentials.

3.) When you are back into your account, **check your address book and settings** to be sure that no new names appear in your address book, or your signature and "away" messages haven't been altered. Watch out for new "friends" that may have been added to your social media account. In fact, beware of whom you "friend."

4.) **Let your friends know what happened** (use the email Bcc line to keep their e-mail addresses private).

5.) **Update security questions** for any online accounts.

6.) If your online service (banks, financial accounts) offers **two-part authentication** (meaning they must provide you a code to enter before you can access your account), set that up.
As always, beware of unsolicited phishing e-mails that appear to be reputable business or government agency communications. Sometimes a misspelling will give it away – sometimes not. Never, never, EVER click on a link or open an attachment unless you are completely confident of the sender's identity and the reason for the e-mail.

New Medicare cards are on their way

Medicare is gradually issuing new cards using an 11-character ID made up of numbers and letters instead of the recipient's Social Security number, a move designed to lower the risk of identity theft. The card is free and will be delivered by mail to your home, so any phone calls asking you to pay a fee or trying to extract personal information in order for you to obtain the new card are scams.

As Maine goes. . .

The good news is that the Senior Safe Act, signed into law in May by President Trump, emerged from Maine's own Senior$afe program and gained bipartisan support in Congress. The Maine bill began as a collaboration among state regulators and financial and legal organizations to train banking and credit union employees about signs of elder financial abuse and alert the proper authorities. Bank privacy laws previously hindered reporting of suspected fraud. With the passage of the new act, bank employees can be provided training programs to recognize and report suspicious account activity without the fear of themselves or the bank being sued or fined. If you have an older friend or family member who you believe is being defrauded, read the AARP article "Spot Elder Financial Abuse" or check out the National Council on Aging's "Elder Abuse Facts" for a link to your state's adult protective services.

The bad news is that about 5 million older Americans from all walks of life are scammed each year. The top 10 scams targeting seniors, according to the US Senate Special Committee on Aging, are:

1.) IRS phone impersonators
2.) Robo-calls from phony marketers, charities, or government agencies using fake Caller ID numbers
3.) Lottery winnings where the "winner" must send a check to collect it
4.) Calls where the caller says "Are you there?" or "Can you hear me?" to prompt you to say the word "yes" (to authorize charges to credit cards)
5.) "Hi, Grandma, I need some money wired to me right away. . . and please don't tell my parents"
6.) Computer tech support/ransomware scams generated from clicking "pop-up" boxes on one's computer screen
7.) Romance/dating scammers
8.) Financial abuse by con artists, loved ones, caregivers, and trusted advisers
9.) Identity theft
10.) Grant scams purporting to be from the federal government

In addition, beware of: counterfeit prescription drugs on the internet; funeral and cemetery plot scams; phony anti-aging products; investment schemes (yes, there are still Nigerian con artists working the internet); and homeowner /reverse mortgage scams, including those who offer to have property value reassessed for a fee, or phony contractors who show up on your doorstep.

You should never give financial, Medicare, or Social Security information over the phone unless you originated the call yourself for a specific reason. If you receive a suspicious call, you can report it to the U.S. Senate's Special Committee on Aging's Fraud Hotline at 1 (855) 303-9470. For more resources, download the Committee's 2018 Fraud Book.

Cat: a tonic

If the above left you feeling a little stressed, here's a relaxing job opportunity to counter the effects. (Those allergic to cats need not read *fur*ther.)

Looking forward to autumn,

Thomas Rogers, CFP®
Brian L. Dietz, CFP®, CFA
Debra Yoo

Portland Financial Planning Group LLC | 511 Congress St., Suite 804, Portland, ME 0410