financial fitness

By **Jennifer Osgood**, Partner/Financial Advisor at Wagner Wealth Management

GUARDING AGAINST IDENTITY THEFT

TAKE STEPS TO PROTECT YOUR VITAL INFORMATION FROM BEING COMPROMISED

America is enduring a data breach problem. As many workers traded in the office for remote work, data security has been a focus for the public and private sectors. Between robocalls pitching low-cost health insurance, pretending to be the I.R.S., or offering "work from home" opportunities, the pandemic has seen scammers getting more creative than they've ever been.

Look for the "https" and the padlock icon when you visit a website. Not just the http – https. When you see that added "s" at the start of the website address, you are looking at a website with active SSL encryption, and you want that. A padlock icon in the address bar confirms an active SSL connection. For really solid security when you browse, you could opt for a VPN (virtual private network) service which encrypts 100% of your browsing traffic.

However, be especially careful when clicking on any links that you receive from an unknown sender. Many criminals have caught up, and use sites that seem valid by using the "https" prefix. Look to see what the email is asking for (example, demanding payment), and verify this by sending a separate email or calling the supposed contact to verify the validity of the email. Look for any misspelled words or incorrect links in the email. If you're more technically savvy, you can look at the original version of the email to see if it actually originated from somewhere else.

Check your credit report. You may have been the victim of identity theft or fraud, and not even realize it, until it shows up on your credit reports. Thanks to the Fair Credit Reporting Act (FCRA) you are entitled to one free credit report per year from each of the big three agencies: Experian, TransUnion, and Equifax.

Don't talk to strangers. Broadly speaking, that is very good advice in this era of identity theft. If you get a call or email from someone you don't recognize – it could tell you that you've won a prize; it could claim to be someone from the county clerk's office, a pension fund, or a public utility – be skeptical. Financially, you could be doing yourself a great favor. If an email looks like it could be legitimate, don't click on any links in the message or open attachments. Rather, go directly to the company or sender's website instead.

Use secure Wi-Fi. Avoid "coffee housing" your personal information away – never risk disclosing financial information over a public Wi-Fi network. (Broadband is susceptible, too.) Although a public Wi-Fi network at an airport or coffee house is password-protected – if the password is posted on a wall or readily disclosed, how protected is it? A favorite hacker trick is to sit idly at a coffee house, library, or airport and set up a Wi-Fi hotspot with a name similar to the legitimate one. Inevitably, people will fall for the ruse, log on, and get hacked.

Tax time can be a prime time for identity thieves. Their goal is to get their hands on your 1040 form and claim a phony refund using your personal information. You may realize you've been the victim of tax fraud if you can't e-file your tax return because of a duplicate Social Security number or if you receive a notice from the I.R.S. that talks about owing taxes for a year if you haven't filed.

Make sure when you e-file that you use a secure Internet connection. If somehow you just can't bring yourself to e-file, then think about sending your returns via Certified Mail. Those rough drafts of your returns where you ran the numbers and checked your work? Shred them.

The I.R.S. doesn't use unsolicited emails to request information from taxpayers. If you get an email claiming to be from the I.R.S. asking for your personal or financial information, report it to your email provider as spam.

If you have not received communication from the I.R.S. in the mail prior to receiving a phone call, it is probably fake. Also, the I.R.S. will not ask you to pay over the phone. They will direct you to an online payment portal on their official website. The real I.R.S. will not:

- **Be hostile**
- **Call to ask for immediate payment in any form, especially gift card or wire transfer**
- **Demand payment without the opportunity to appeal the amount**
- **Ask for your credit card number over the phone**
- **Threaten to bring in law enforcement if you do not pay**
- **Threaten to take away your driver's or business license or immigration status**

Wagner Wealth Management has offices in Greenville, Anderson and Oconee counties. Call us at 864-236-4706 or visit www.wagnerwealthmanagement.com to learn more about our firm.

Source: MarketingPro, March 2021
Taxslayer, April 2021
FTC.gov, 2021
IRS.gov, November 25, 2021
NextGov.com, June 19, 2019
Consumer.FTC.gov, 2021
AnnualCreditReport.com, 2021