Guarding Against Identity Theft

Take steps so criminals won't take vital information from you.

Provided by DSA Financial Group

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.[1]

Tax time is prime time for identity thieves. They would love to get their hands on your 1040 form, and they would also love to 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 you haven't filed.[2]

Just make sure when you e-file that you use a secure Internet connection. When you e-file, you aren't putting your Social Security number, address, and income information through the mail. You aren't leaving Form 1040 on your desk at home (or work) while you get up and get some coffee or go out for a walk. 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.[2]

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.) It takes little sophistication to do this – just a little freeware.

Sure, a public Wi-Fi network at an airport or coffee house is password-protected – but 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.

Look for the "https" & the padlock icon when you visit a website. Not just 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.[3]

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 (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.[3]

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. This year, because of the increased issues with identity theft and fraud during COVID-19, these three agencies are also allowing weekly credit checks from now until April 2021. Checking your credit report weekly will not affect your ability to order your free annual credit report.[4,5]

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.

Raymond Dahlman may be reached at 281-724-8181, 8310 South Valley Hwy, Suite 300, Englewood, CO 80112 or r.dahlman@dsafinancialgroup.com.

www.dsafinancialgroup.com

Citations

1. FTC.gov, 2021
2. IRS.gov, November 25, 2021
3. NextGov.com, June 19, 2019
4. Consumer.FTC.gov, 2021
5. AnnualCreditReport.com, 2021