LAMCO ADVISORY SERVICES, INC.

HOW TO PROTECT YOURSELF FROM ONLINE IDENTITY FRAUD

By Mark Lamoriello, AIF® | President, Chief Investment Officer

We spend an absurd amount of our lives on the internet – whether for work, to shop, or to simply kill a few minutes perusing a social network. And, unfortunately, the internet can be a dangerous place; online identity fraud is the fastest growing crime now, and it has been for several years.

There is no way to completely protect yourself from online identity fraud. However, you can take steps to reduce your risk of online ID theft. By following a few best practices, it's possible to be safer online.

Verify the Security of the Website | The first step is to verify the security of the website you are using to make purchases or conduct other business. From your favorite shopping website to the website you use for email, you want to check to make sure it's secure.

One way to do this is by looking at the address bar at the top of the webpage. You should see a closed padlock image on secure websites. Additionally, you can look at the address itself. If an address begins with http instead of https, it's not secure. Look for that extra "s" before you enter a password or make a purchase.

Even secure websites can be hacked, but it's much harder. Double-check to see that the websites you use for banking, shopping, email, and other activities are secure. Some webpages only become secure when you need to enter a password or payment information. A good rule of thumb is to check for security before entering any information.

Create a Better Password | Next, get in the habit of creating better passwords. Following best practices can make it harder for hackers and scammers to get into your online accounts.

Here are a few tips for creating stronger passwords that are harder to crack:

- *Don't use the same password for multiple websites: If a hacker gets access to one site, he is likely to try that password on other sites. Limit damage by using unique passwords for different websites.*
- *Avoid connecting passwords to personal information: You might be surprised at what hackers and scammers can figure out by looking online. Don't create passwords associated with the names or birthdays of loved ones, or with your hometown, or other personal information.*
- *Make your passwords long: The longer the password, the harder it is to crack. You can use a phrase you like, or some other method to create longer passwords. Your passwords should be at least eight characters long, but there's nothing wrong with making them even longer.*
- *Combine letters, numbers, and symbols: Make sure to use different types of characters. Even if you use a phrase as the basis of your password, you can substitute numbers and symbols for some of the letters. This makes it harder to crack.*
- *Don't store your passwords in plain sight: If you save your passwords on your computer, keep them in an encrypted file. It's not a bad thing to write down your passwords, but make sure the list is out of sight. Write down the website, and, instead of writing the password, consider writing a clue to help you remember the password.*

Another solution is to use a service like *LastPass*, *Keepass*, or *1Password* that secures your passwords with a master password. Create a very strong master password, and then everything else will be taken care of for you.

Limit the Credit Cards You Use Online | Rather than using a different credit card at different online sites, consider choosing one card for online use. This way, you limit the damage to just one credit card if a website storing your information is hacked. Dividing up your credit card usage can also make it easier to know which accounts are affected if you do need to cancel a credit card after it's been compromised.

Another solution is to use an online payments system like PayPal to make online purchases. Your information is limited to one website, and you don't have to enter personal details and credit card information very often. The less information you share, the better off you're likely to be.

Be Stingy with Your Personal Information | The more you share online, the easier it is for scammers and fraudsters to steal your identity. Be stingy with your personal information. Items like your birthdate, high school graduating class, address, and family members provide fraudsters a starting place for creating fake accounts in your name.

Check your privacy settings on social media to make sure what you do share is restricted to fewer people. Finally, don't respond to emails asking for personal information and account information. Scams aimed at getting you to reveal information are common. The general rule is to avoid giving out account numbers and other information in response to an email request.

Monitor Your Accounts | Finally, stay on top of your accounts. Check your bank accounts and credit card accounts regularly. If there are suspect purchases, flag them immediately and contact the financial institution. The earlier you catch fraudulent purchases, the quicker you can resolve the issue and limit the damage.

Also, check your credit report at AnnualCreditReport.com every few months to check for loans and other accounts set up fraudulently in your name.

While there's no way to be completely safe online, your vigilance can reduce the chances that you will be a victim of identity theft.