2023 · AM I AT RISK OF HAVING MY IDENTITY STOLEN OR BEING A VICTIM OF FRAUD?

WINDWARD
Private Wealth Management Inc.

CYBER THREATS	YES	NO
Do you use the same password to log into multiple websites? If so, consider making unique passwords for each website you log into or use a password manager.	☐	☐
Do you need to review if you are using two-factor authentication to log into websites?	☐	☐
Do you use common phrases, words, or personal information in your passwords? If so, consider making passwords that are harder to guess.	☐	☐
Do you share your login credentials with other people?	☐	☐
Do you need to update your browser, anti-virus software or operating system? If so, cybercriminals may be able to access your computer.	☐	☐
Do you receive unsolicited emails asking you to click on links or download attachments? If so, you may be subject to phishing scams, where you are lured into clicking links or opening attachments. Instead of clicking any links, navigate to the page on your own to avoid being redirected to a compromised site. Do not open any attachments.	☐	☐
Are images in emails set to download to your computer automatically? If so, consider turning this feature off as cybercriminals can use code embedded in images to gain access to your computer.	☐	☐
Do you share lots of your personal information on social media sites? If so, consider making your social media accounts private where possible. This makes it more difficult for anyone you do not know to see what you have posted. Some cybercriminals will look on these sites for key information (place of birth or mother's maiden name) that can aid them in resetting passwords associated with your accounts.	☐	☐
Have you received odd requests or links from friends or family? If so, consider calling the sender to verify the email before clicking anything in the email. The sender's email account may have been hacked and the email was not sent by the person you know. (continue on next column)	☐	☐

CYBER THREATS (CONTINUED)	YES	NO
Do you download apps to your phone? If so, consider researching all apps and/or app developers before you install them and give them permission to use your data. Cybercriminals can build legitimate-looking apps that can steal your data and monitor your phone's actions.	☐	☐
If you have minor children, do you need to take steps to protect them online? If so, check privacy settings on their social media accounts and talk with them about issues raised in this checklist.	☐	☐
If you are a business owner, do you need to create a cybersecurity plan for your business? If so, ensure that policies are in place for business operations (such as a confirmation call before electronic transfers occur).	☐	☐
Has your data been stolen because of a third-party data breach? If so, consider the following: ■ Freeze your credit by contacting the three major credit bureaus. ■ Change your password to any sites that had the same credentials as the compromised site.	☐	☐

COMMON SCAMS	YES	NO
Have you received calls from someone claiming to be from a government agency offering relief payments due to COVID-19? If so, this could be a scam. Do not provide them with any information.	☐	☐
Have you received calls asking for personal information? If so, call the business or organization back using a number you know to be accurate.	☐	☐
Have you recently met someone online, and they are asking for money even though you have not met in person? If so, they may be trying to take advantage of you. This is known as a romance scam. Do not provide them with money. (continue on next page)	☐	☐

2023 · AM I AT RISK OF HAVING MY IDENTITY STOLEN OR BEING A VICTIM OF FRAUD?

WINDWARD
Private Wealth Management Inc.

COMMON SCAMS (CONTINUED)	YES	NO
Have you received a phone call from someone claiming to be from the Social Security Administration? If so, they may be trying to convince you to provide them with your Social Security Number or bank account information. This is known as a Social Security scam. Do not provide them with any information.	☐	☐
Have you received a phone call, email, or text message from someone claiming to be from the IRS? If so, this may be a tax scam. The IRS does not contact taxpayers by phone, email, or text message to request or discuss personal or financial information.	☐	☐
Have you received a phone call from someone claiming to be a Medicare representative? If so, they may be trying to convince you to provide them with your personal information (including your Medicare number). This is known as a Medicare scam. Do not provide them with any information.	☐	☐
Have you received a phone call from someone claiming to be your grandchild and asking for money? If so, this may be a scam known as a grandparent scam. Contact family members and do not wire funds or otherwise transfer money without reliable confirmation that the caller is indeed your grandchild.	☐	☐
Have you unexpectedly won a sweepstakes, gift card, or lottery? If so, this may be a scam known as a sweepstakes scam. The scam may involve you having to pay a fee in order to receive the supposed winnings.	☐	☐
Have you received an email with a username and/or password of yours in the subject line? If so, the cybercriminal may have credentials from a single compromised website but claim to have access to all of your devices and accounts. This is known as a spearfishing scam.	☐	☐

OTHER ISSUES	YES	NO
Do you want to add a further layer of security and privacy to your online activity? If so, consider setting up a virtual private network (VPN) from a reliable provider.	☐	☐
Do you need extra support in monitoring your cybersecurity? If so, consider Identity Theft Protection services that can monitor your credit scores, new account openings, and suspicious activity on your behalf.	☐	☐
Do you need to review your Identity Theft Insurance Policies? If so, consider the following: ■ You may already have the coverage you need, as it may be included in your homeowners or auto insurance. ■ Fraudulent expenses purchased on credit cards may be capped to you at $50. ■ Be mindful of over-insuring yourself.	☐	☐
Have you been the victim of the above scams or other forms of fraud? If so, consider the following: ■ Immediately contact any affected financial institutions to report the fraud and contain your exposure. ■ If you lost money in a scam or were a victim of identity theft, file a report with your local police and the Federal Trade Commission. ■ Notify credit bureaus and other relevant agencies.	☐	☐