|  |  |  |
| --- | --- | --- |
| |  | | --- | |  |  |  | | --- | |  | |
| |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Identity Theft Can Happen to Anyone. Take These Steps to Protect Yourself.**  **Identity theft is the bane of the digital age. You need to know how to protect yourself and what can happen if you don’t.**  The success of identity thieves depends greatly on the steps you take to protect yourself. At stake is your financial health and your reputation. Once thieves rob your identity, they can empty your bank accounts, obtain medical care, steal your tax refund, and apply for loans and credit cards, all under your name.  **Keep your personal information private.** Social media is a great place to share information. However, that should never apply to personal information. If you share even innocent-sounding data, like your birthday, workplace, or phone number, you give thieves openings to attack your identity. You can protect yourself through strict privacy settings that prevent strangers from seeing personal information. In addition, you should omit personal information in your posts and tweets. Once that information is out there, you can never erase it.  **Limit your digital footprint.** That footprint includes items such as usernames, online searches, purchasing behavior, and electronic transactions. Protective steps you can take include deleting old accounts, browsing incognito, and removing yourself from data collection sites, which is something you can hire a service to do. Consider using a virtual public network (VPN) to protect your privacy as you surf the web and/or share files. When shopping online, use temporary virtual credit card numbers (available from card issuers or third-party services) to reduce your exposure to fraud.  **Avoid risky behavior.** This starts with using different passwords for different accounts. Keep all your passwords in a secure online vault so that you don’t have to remember them and change your passwords often. Never click on an unexpected email link, even if it looks safe, as doing so exposes you to a phishing attack. Instead, contact the email party by going to the supposed website through your browser. Never type your password or user ID into an unfamiliar sign-in screen.  **Monitor your credit reports.** The credit reports maintained by the three major credit bureaus (Experian, TransUnion, and Equifax) are available each year for free at AnnualCreditReport. com. By reviewing your reports, you can spot suspicious activity or unfamiliar accounts that indicate possible identity theft. Immediately dispute any mistaken data by directly contacting the credit bureau. Also set up your financial accounts to provide fraud alerts in real time. Consider subscribing to a protection service to help prevent and repair identity theft.  **Identity thieves can do a lot of damage.** Considering how much is at stake, the extra effort you extend to protect yourself is well worth it. Please contact me and we can discuss your options for a security review of your financial accounts and credit reports. Let’s stop the fraudsters in their tracks before they make you their next victim.   |  |  | | --- | --- | | |  | | --- | | [LET'S CONNECT](mailto:##AdvisorEmail##) | |  |  |  | | --- | --- | |  | Tracking #1-05068544 Expiration 11/23 | | | |
| |  | | --- | |  | |