

TRANSITIONS

Wealth Management, LLC



QUOTABLE

Recently, "60 Minutes" highlighted a government study that says about 40 million Americans may have credit report errors. In the story, correspondent Steve Kroft effectively showed how time-consuming and expensive it can be for consumers to fix such errors.

Sam Richter recommends that consumers monitor the privacy controls on their social media sites, including Facebook, LinkedIn and Twitter. These settings must be checked regularly because firms are constantly making changes. A criminal who successfully hacks into a social media account could then seek more valuable financial account information using similar passwords.

"I've had a police chief tell me street crime is down because everybody is now filing false IRS returns," IRS Commissioner John Koskinen, who took office in January of 2014 said in an interview.

Who are you?...who who who who

News that hackers have stolen and published sensitive financial details of high profile individuals such as first lady Michelle Obama, Vice President Joe Biden and rapper Jay-Z serves as a good reminder that no one is 100% protected from having their identity stolen and credit wrecked. As your trusted wealth manager, we want to help you to have peace of mind around this rapidly expanding and troubling trend.

We are concerned with our clients' financial well-being and will be guiding you to be proactive in defending against identity fraud. In addition to regular credit report checks, one step that we recommend is that you purchase protection from services like LifeLock or IdentityGuard.

Lifelock, for instance, will send subscribers an alert as soon as someone has used their financial or personal information to apply for credit from retailers, seek a car or payday loan or even subscribe to a cell phone. It also lets subscribers know if someone has tried to change their address or sell their private financial information to others online. For about \$110 a year for basic service, Lifelock also can make the distressing circumstance of losing a wallet easier. It helps to cancel and replace credit cards, drivers licenses and Social Security cards, among others. Actify Inc. chief marketing officer Sam Richter told those attending the Financial Planning Association's Business Solutions conference in Chicago that even though these services don't work perfectly, wealth managers and financial planners should help their clients get protection for themselves and their children.

"When's the last time you got your 14 year old's credit report?" he asked. In fact, child identity theft is all the rage because criminals have realized it takes longer to detect cases when they have used the private information of, say, a three year old to open accounts and go on a spending spree. Some officials say it's close to a year before most of these cases are identified. You should be extra wary of giving out Social Security numbers of your children on health, school and other forms and even ask if they can use a substitute number, experts said. Shredding financial and health documents is also important.

To the many who have fallen victim to cyber-theft, they assumed it could never happen to them. But fraudsters have an arsenal of methods to help get their victims' personal information. Their goal is to make a profit off of vulnerable consumers. Fraudsters find online-related schemes appealing and effective because online access is a common form of financial activity and communication; it provides a layer of anonymity.

One area of fraud where there has been a significant increase is cyber-hacking. In this type of cyber-threat, an unauthorized person uses malware - such as a keystroke-logging or "keylogging" program - to take control of a victim's computer, often by secretly stealing their email login or online account(s) credentials. The fraudster then monitors the online activity(s) and identifies the company(s) with which the victim does business or communicates with.

One of the most dangerous security threats is the phishing attack or scheme. That is where criminals impersonate trusted institutions (established companies, government agencies, banking institutions, etc.) in an attempt to gain access to sensitive data, personal information and account number(s). Once the fraudster(s) obtain that information the cyber-fraud is easily committed.

To help prevent cyber-fraud and cyber-hacking, below are some recommendations and suggestions that may help your online account(s) from being compromised:

- Change all your password(s) periodically – every 3 months as an example
- Use special characters in place of letters – as an example use the '@' in place of the letter 'a' or a zero in place of the letter 'o'
- Use a combination of upper and lower case along with the use of special characters and/or numbers
- Use a different password for each online account
- Use a different email account for different 'types' of online activity – as an example have one email for bank account(s), one email for social media account(s), one email for online shopping, etc.
- Go directly to a website versus clicking on a link within an email to take you to a website
- Use secure websites – look for the 'lock' in the browser bar
- Keep the operating system, anti-virus and anti-malware/anti-spyware up to date on your computer; also keep the firewall on your computer turned on
- Log out of any sites that require a user name and password; don't just close the browser window; also turn the computer off – power it down
- Make sure your mobile devices (smartphones, tablets, etc.) are secure as well
- Do not use the names of your children or spouse in the user name or password
- Do not use any part of your social security number in the user name or password
- Do not use your birthdate in the user name or password
- Do not use your house number in your username or password
- Do not post to social media that you vacationing or will be gone for an extended period of time – that is announcing to the world you are vulnerable for theft
- Do not store your credit card details on website(s)

We have made this a top priority and encourage you to do the same. Transitions Wealth Management, LLC