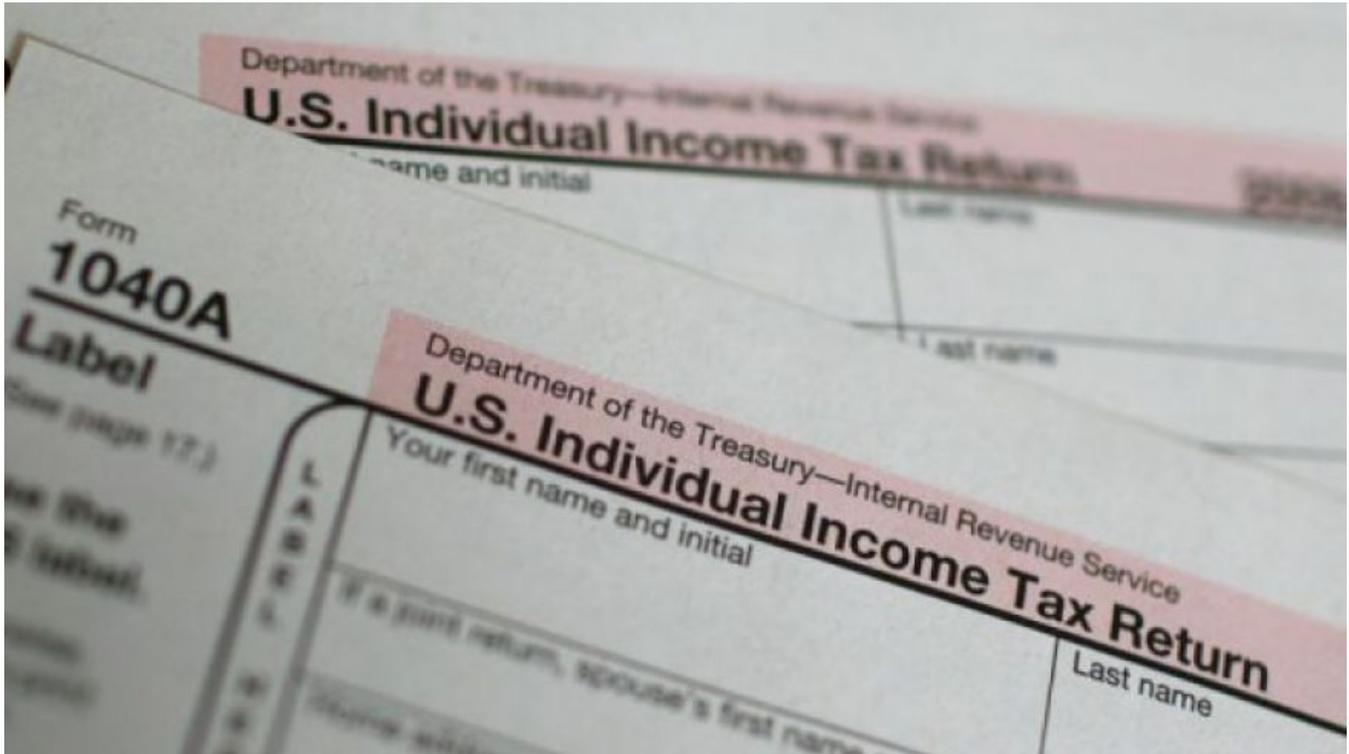


Are You 'Over-Exposed' Online? Lessons From IRS Hack

 foxbusiness.com/personal-finance/2015/05/27/are-over-exposed-online-lessons-from-irs-hack/

Kristin Bianco



According to the IRS, the cyber thieves who stole tax return information from 100,000 Americans via its “Get Transcript” application may have used social media to get in the door.

These criminals may have been able to figure out answers to security questions like the name of a first pet, or mother’s maiden name, using data that people readily share today with friends on social media sites, such as Facebook.

Are you "over-exposed" online? Here is advice from cyber security experts on how to keep your personal information from falling in the wrong hands.

Less is more (secure)

If one of your Facebook friends can answer your security questions, then you may be over-exposed, according to Alex McGeorge, head of threat intelligence at Immunity Inc., a cyber security firm based in Miami, Florida.

He said social media users should use privacy options to control what’s shared with friends and what’s shared with the public. The fewer people who know what you are up to on a daily basis, the more secure you’ll be.

“This is the new normal,” McGeorge said. “We need to start thinking defensively.”

Mobile and online defense

According to McGeorge, your phone is more likely to be compromised than a computer, not only because it can be stolen, but because downloading a poorly-coded application can make it vulnerable to an attack.

You can still enjoy the convenience of banking or shopping online, but he suggests using a dedicated credit card and bank account that has credit limits. For example, if you want to deposit checks or pay bills online, keep this account at a completely separate bank, from say, your savings and investment account. Also, use a separate credit card with strict controls and alerts for all online purchases.

McGeorge also said accounts with large balances -- like retirement or savings accounts -- should be accessed from the branch or over the phone, not online.

Monitor your credit reports

Chris Weber, co-founder of Casaba Security, a cyber-security firm based in Seattle, Washington, said consumers should get identity protection and credit monitoring for themselves and their children, from companies such as Equifax or Experian. He said it's important to protect children too, as their personal information may be found on social media and certain health-care websites.

And once you've signed up, keep an active eye out for any suspicious activity.

"It's an ongoing process. It's not like we make it secure and just walk away," Weber said.

Kristin Bianco is a financial news anchor and FOXBusiness.com contributor.