Volume #4 - Issue #157
April 27th, 2018
This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to HomeCyberDefense.net to sign up.

How Safe is Your Personal Information

Another day, another data breach. Recent news about cybercriminals obtaining more than 5 million credit card numbers from high-end U.S. retailers joined a series of major hacks and online data breaches.

Unfortunately, the frequency of attacks on Americans' personal information has fostered a feeling of inevitability. In fact, according to results released today from a telephone survey conducted by The Harris Poll for the American Institute of CPAs (AICPA) of 1,006 Americans adults in the fall of 2017, nearly half of U.S. adults (48 percent) think it is at least somewhat likely identity theft will cause them financial loss in the next year.
While the survey finds that three out of five Americans (61 percent) have at least looked at their credit report, more than a third (35 percent) have never once checked. This is particularly alarming, as a majority of those who have checked their credit (66 percent) had to take steps with a credit reporting agency to correct inaccuracies, with the average being 13 specific corrections among those who have taken steps at least once. More distressing, those with a household income of less than $35K were found to be more likely to never have looked at their credit report than those with a household income of $100K+ (44 percent vs. 30 percent).

The frequency and scope of cyber-attacks has many Americans questioning the effectiveness of cybersecurity practices businesses currently have in place. In fact, eight in ten Americans (81 percent) said they are at least somewhat concerned about the ability of businesses to safeguard their financial and personal information, with two in five (40 percent) reporting that they are extremely or very concerned.

With security breaches costing U.S. consumers $19.4 billion of their own money, this may be a cause for action. The survey found four in five Americans (81 percent) said they've changed their behavior based on the threat of cyber breaches affecting credit card and debit card processing systems. Those changes include a majority increasing self-monitoring of credit and debit card accounts for fraudulent activity (56 percent), while about 4 in 10 are either using cash and/or checks more often (43 percent) or choosing to shop at locally owned stores more often instead of national retailers (40 percent).

A quarter of Americans (26 percent) said they have reduced their online presence, either turning off social media or visiting fewer websites because of concerns about data security. One in five (20 percent) have signed up for additional fraud detection or credit monitoring. Roughly 1 in 10 report they are switching their shopping to different national stores because of concern about data breaches (11 percent), placing a freeze on their credit (11 percent), or shopping online more often, because they feel like it is safer (11 percent). Five percent said they use alternative forms of currency.

Tips to prevent and mitigate the effects of identity theft:
Monitor your credit report & set protections. You can request a free credit report from all three major credit reporting agencies once a year, including TransUnion, Equifax and Experian. Additionally, some monitoring services allow you unlimited access to your credit information year-round. These services are there to help you spot inaccuracies, potential fraud and more on your credit report. This should also be done for children. Theft of a child's ID may go undetected for many years such that by the time they are adults, the damage has already been done.

Don't provide your Social Security number unless it's necessary. A space for it on a form doesn't necessarily mean that it is required. For example, your doctor's office may use a unique number issued by your insurance company to enter your claim but their form may have a space for SSN anyway. Don't be afraid to ask if they really need it.

Make sure your Wi-Fi network at home is secured with a password. A skilled data thief can access information on an unsecured network. Additionally, when away from home, avoid providing credit card or other personal information on unsecured Wi-Fi networks like those in airports or coffee shops.

Don't provide personal information in response to any unsolicited communication. Even if the caller, text or email claims to be from a bank or credit card company needing to "verify" your account to "prevent fraud."

If in doubt, call the number on your bank statement or the back of your credit card.

What to do if it happens? Act quickly to limit the damage. Call your credit card company and report it to them. They will close your card and issue a new one. File a police report to ensure that you are covered for any damages that you may incur. If your Federal return is affected, call the IRS 800-908-4490 and file Form 14039 **Identity Theft Affidavit.**

Thank you for subscribing to our email!

Home Cyber Defense Weekly
is a service of
House of File Technologies