How to Protect Yourself—and Your Money—From Hackers

September 21, 2017

You've probably seen headlines like this over the past few days:

Equifax® Says Cyberattack May Have Hit 143 Million Customers[1]

Every year, it seems more and more companies are falling victim to hackers. Even large organizations like Verizon®, Walmart®, and Target® aren't immune. But the recent cyberattack on Equifax is especially noteworthy. As one of the three largest credit-reporting companies in the United States, Equifax stores a *lot* of private information. In this case, names, addresses, birthdates, Social Security numbers and even driver's license numbers were stolen.

What can hackers do with someone's name, birthdate, address and Social Security number? The answer is chillingly simple: take the victim's identity and use it for themselves.

Fortunately, there are steps you can take to protect yourself.

What to Do After a Data Breach

In a situation like this, there are both reactive and proactive steps to take. Let's cover *reactive* steps first.

You may be asking yourself, "How do I know if I have personally been affected by Equifax's data breach?" Equifax has created a website, www.equifaxsecurity2017.com, where you can check if your personal information has been compromised. You can also enroll in a free credit-monitoring service provided by Equifax.

However, I would exercise caution before going there. The website asks you to provide the last six digits of your Social Security Number to perform the check. Given their recent history, it's reasonable to be wary of providing Equifax more personal information.

In addition, a report by the Washington Post suggests that "enrolling in the Equifax checker program … potentially restricts your legal rights. Buried in the terms of service is language that bars those who enroll … from participating in any class-action lawsuits that may arise from the incident."[2]

It's not my place to tell you whether to use the website or not, and indeed, the Federal Trade Commission's official position is that "if a company responsible for exposing your information offers you free credit monitoring, take advantage of it."[3] But whether you choose to use Equifax's checker website or not, there *are* additional steps the government suggests you take:[3]

1. Get a free credit report from www.annualcreditreport.com. Check for any accounts or charges you don't recognize.

2. Consider contacting your financial institution and placing a "credit freeze." This makes it harder for someone to open a new account in your name.

3. File your taxes as early as possible—before a scammer can. Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job.

4. Don't believe anyone who calls and says you'll be arrested unless you pay for taxes or debt—even if they have part or all of your Social Security number, or say they're from the IRS.

5. Watch for signs of identity theft. Warning signs include withdrawals from your bank account you can't explain, failure to receive expected bills, and merchants refusing your checks.

Changing your online passwords and signing up for a third-party credit-monitoring service are also prudent steps.

For more information, I recommend visiting www.identitytheft.gov.

Proactive Steps to Take

Whether your personal information was exposed or not, there are some basic steps *everyone* should take to protect their identity. Here are just a few:

- Delete your saved payment methods from online shopping sites. You will have to reenter your billing information each time you make a purchase, but it will protect your payment information if your account is breached or someone gains access to your login.
- Review statements and credit reports regularly. Look for unauthorized charges or small amounts appearing on statements. Check your credit report regularly. Federal law allows you to get a free credit report every 12 months to review. Make sure all information is correct.
- Don't make impulsive decisions based on fear. If you receive an email or phone call stating that it's from your bank or the government, and that you're in trouble, don't provide the sender with any personal information. Typically, the government will not contact you by email or phone. They will contact you by mail. Your bank will never ask you to provide information through email either. If you're concerned about the credibility of a call or email from your bank, contact the nearest branch and ask them.
- If someone contacts you saying they're a relative in trouble and need your help, ask them something that only your relative would know. Or ask a trick question that reveals they're lying, such as "How's your dog Scruffy? Did he get better?" when you know that relative doesn't have a dog. If they say, "Oh he's doing much better," then you know they're a fraud and you should immediately hang up.
- Keep all personal documents in a safe place. Don't carry them around with you, especially not your Social Security card.
- Don't open emails from senders you don't recognize, no matter how interesting the subject line.
- Choose a different way to pay. Many merchants accept alternative ways to pay for goods and services, including Google® Wallet, Apple Pay®, or PayPal®. These services provide an extra layer of protection because they keep your credit card information stored but do not actually provide it to retailers when you pay.
- Don't use your bank cards online unless the site is secure and reputable. Make sure you are purchasing from a reputable company and website. Don't trust a site just because it claims to be secure. Use credit cards so you can dispute the charges if something goes wrong. You can still be reimbursed for fraud on a debit card but the process often takes longer and your money is already gone.

None of these steps are foolproof, but by taking concrete steps to protect yourself, your identity, and your money, you make it much, *much* harder for hackers and scammers.

STEVE ROBBINS, CFP®
WEALTH MANAGEMENT FOR A FLOURISHING RETIREMENT

325 St. Francois Street, Florissant, MO 63031 • www.SteveRobbinsOnline.com • (314) 839-4600

Sources:

[1] Brian Womack, "Equifax Says Cyberattack May Have Hit 143 Million Customers," *Bloomberg*, September 7, 2017. https://www.bloomberg.com/news/articles/2017-09-07/equifax-says-cyber-intrusion-affected-143-million-customers

[2] Brian Fung, "By signing up on Equifax's help site, you risk giving up your legal rights," *The Washington Post*, September 8, 2017. https://www.washingtonpost.com/news/the-switch/wp/2017/09/08/what-to-know-before-you-check-equifaxs-data-breach-website/?utm_term=.de9d4617d81f

[3] "When Information Is Lost or Exposed," *Federal Trade Commission*, accessed September 8, 2017. https://www.identitytheft.gov/Info-Lost-or-Stolen