Ask McCaskill

FINANCIAL ADVICE STRAIGHT FROM THE EXPERT

"I have been receiving a lot of letters recently about a "global cybersecurity" incident that may include my personal data. What should I do?" D.H. – Ijamsville, MD

A: Unfortunately, you are correct. There was a global data breach recently that impacted government agencies, major financial institutions, and thousands of companies around the world. Most of these companies have offered complimentary (free) credit monitoring services and additional resources as a result of the breach, so I encourage you to sign-up for these benefits or reach out to them directly with questions.

In the meantime, here are some ways to protect your data and make you less vulnerable to a data breach.

Email scams are typically responsible for many data breaches you hear about on the news, but there are also risks associated with simple online activities that most of us engage in daily. We routinely send and receive email and instant messages and browse the internet, all of which could make us vulnerable to information security breaches. In fact, while performing these activities, you may unwittingly engage in some of the riskiest behaviors, including:

- Carrying sensitive information on a laptop when traveling or working on a laptop without a privacy screen when traveling
- Not deleting information on computers when it's no longer necessary to retain it
- Sharing passwords or using universal login credentials
- Connecting computers to the internet through an unsecure wireless network

- Using the same login credentials for multiple websites
- Using generic USB drives not encrypted or safeguarded by other means
- Losing a USB drive containing confidential data

The good news is that we can manage these risks by following these few sensible tips.

1. When you no longer need certain information, delete it from your computer.
2. When traveling, keep your computing devices physically secure, password protected, and encrypted (if possible).
3. Only connect to wireless networks you can trust. Connecting to free or random networks makes it easier for cybercriminals to capture and monitor your online activity.
4. Use different login credentials (usernames and passwords) for different accounts. Never use the same passwords for your work or bank accounts as those you use for your personal accounts (e.g., Facebook or Twitter).
5. Enable encryption or remote wiping on your mobile phone. That way, if the phone is ever lost or stolen, you can be sure that the information will be unreadable or unobtainable by anyone who gets their hands on your phone. Be sure to regularly back up your device so that no information is lost!

VISIT OUR NEW WEBSITE:

WWW.MCCASKILL-FINANCIAL.COM

FOR ADDITIONAL RESOURCES, FINANCIAL ARTICLES AND INFORMATION

To submit questions for future articles

Email to scott@mccaskill-financial.com or Call our office at 301.668.7366

MCCASKILL FINANCIAL