https://www.unionleader.com/news/business/money_sense/marc-a-heberts-money-ense-protect-yourself-from-data-breaches/article_c3d18cc5-25c4-5630-a313-4820265a0844.html

Marc A. Hebert's 'Money $ense':Protect yourself from data breaches

Sep 26, 2020

DATA breaches periodically happen these days. The increase parallels the growing digitalization of today's world.

Once data is stolen, the impact can extend far into the future. So what should you do? Here are a few suggestions to help protect yourself.

Be aware of the various scams and ways that thieves could steal your identity. This is a big step in identity theft protection.

As a result of past breaches, most states now have notification requirements. If a breach involved your personal information, chances are good that you will be notified.

When you receive a notification, you need to determine what information was stolen. Was it your name and address? Your Social Security number? How is the company or organization dealing with the issue?

Some types of data pose more potential issues than others.

Make sure you have strong passwords. A combination of upper and lower case letters, numbers and symbols make good passwords. Don't use your name or birthday as part of the password.

Each account needs its own password. Obtaining one password shouldn't give a thief access to all of your accounts.

Use two-step authentication when available. In addition to a password, a text or email notice will provide you with an extra layer of security.

You are entitled to a free copy of your credit report from each of the three credit bureaus, which are Transunion, Experian and Equifax. It is wise to obtain these and review the data.

You may want to stagger obtaining the reports throughout the year. For example, obtain one in January, one in June and one in December. This will allow you to catch suspicious activity on an ongoing basis.

Once again, anything suspicious should be reviewed in greater detail.

Review your accounts carefully. Unknown activity should be investigated immediately. Call your financial institution if you notice anything out of the ordinary.

Limit your exposure by not carrying your Social Security card or more credit cards in your wallet than you need for a particular outing. If your wallet is stolen, a thief has less information to use.

Be aware of requests that you may receive asking for your data. You might be tricked into giving information via email, letter or phone. Never provide your data unless you are sure to whom you are giving it.

Using credit monitoring services is another option. These services track credit activity and will let you know if there are any changes, such as the opening of a new account. This could be helpful if you didn't open the account.

Consider putting a credit freeze on your accounts with the credit bureaus. Having a freeze in place prevents new accounts from being opened since the credit bureaus will not release data to lenders. Without the data, lenders can't evaluate your credit risk and, most probably, will not lend you anything.

Keep in mind that if you put a credit freeze on your accounts and subsequently need credit, you will have to lift the freeze. You will need to keep the pin numbers you were originally provided in order to unlock your accounts.

If you do become the victim of identity theft, you could consider putting a fraud alert on your accounts with the credit bureaus. A fraud alert notifies lenders that they must take extra steps to make sure it is actually you before they give you any credit.

Another step you could take is to make use of the tool that the Federal Trade Commission has developed to report identity theft and recover from it. See the website **identitytheft.gov** for further information.

Marc A. Hebert, MS, CFP, is a senior member and president of the wealth management and financial planning firm The Harbor Group of Bedford. Email questions to Marc at **mhebert@harborgroup.com**. Your question and his response might appear in a future column.

<]