BNN Bloomberg

PERSONAL FINANCE
Technology
Jul 30, 2019

Pattie Lovett-Reid: 5 ways to protect yourself from a data breach

Capital One data breach hits 6 million Canadians

Pattie Lovett-Reid
Chief Financial Commentator, CTV
Follow | Archive

In one of the biggest-ever data breaches, a hacker gained access to more than 106 million Capital One customers' accounts and credit card applications earlier this year. Six million of them were Canadians.

Capital One said the hack, which it became aware of on July 19 but happened in March, is expected to cost the company between $100 and $150 million this year, primarily due to customer notifications, credit monitoring and legal support.

And while Capital One indicated it fixed the vulnerability and believes the information was unlikely shared or used for fraud, the company is still investigating.

The data breached includes credit card applications, names, postal codes, phone numbers, email addresses, birth dates and self-reported income. Drill a little deeper and it gets more personal – credit score, borrowing limits, balances, payment history and contact info. About one million social insurance numbers of the company's Canadian credit card customers were also compromised.

Capital One said it will notify people affected by the breach and will make free credit monitoring and identity protection available. This is a huge reminder that you can do everything right and still become a victim.

However, you can be sure the call to action for all of us will be to review our own personal data regardless of where you do business. But before you panic, let's not forget security is multilayered and institutions are also looking for areas of vulnerability in their systems.

When something like this happens it raises awareness and you don’t need to lose money. Here’s how you can make changes today.

1. Review your financial documents and accounts regularly. Check your credit cards thoroughly, review yours bills and question any unauthorized purchases or transactions. Capital One advises customers who notice unusual activity to contact the institution.

2. Set up real-time alerts. Most financial institutions offer real-time notification services that allow them to contact you in the event of a purchase or attempt considered to be unusual. You can put limits in place and chose how to be notified – email, text, or call – to validate.

3. Change your passwords monthly. Creating strong passwords is important. Coming up with obvious passwords such as your birthdate or initials do not pass muster. Studies have shown that more than 50 per cent of internet users use weak passwords. Be creative and make your passwords complex by using a random combination of letters, numbers and symbols that have no connection to you or your family. Some recommend a short sentence (for example: the sun is shining).

4. Keep your private information private. Don't share your passwords with family members and pay close attention to what sort of information you give out over the phone or online. A simple rule: do not provide your passwords or personal information to unsolicited callers. When searching new websites, to ensure its security, make sure there is a closed lock symbol at the bottom right of the screen. Web addresses that begin with “https” are generally secure, and if you click on the lock symbol on the bottom right, it will display the same “https” address.

5. Subscribe to identity protection. The bad guys' malware sneaks into private files, grabs your credit card and personal information, and sneaks out. There are numerous identity protection companies who will monitor your credit cards, and other data often for a fee. You can explore options via agencies such as TransUnion or Equifax.