How to protect yourself when your bank's online security fails

ROB CARRICK
PERSONAL FINANCE COLUMNIST
PUBLISHED MAY 30, 2018 UPDATED MAY 30, 2018

Lost money is the least of your problems if you're a victim in a data breach like the one that has affected as many as 90,000 Bank of Montreal and Simplii Financial clients.

Both banks say they will reimburse clients for losses. "I don't really have any concerns about that," said Sandy Boucher, a specialist in fraud and corruption investigations with Grant Thornton. "This is a reputational issue for them."

The much bigger risk is in any personal data that may be stolen by hackers. Both banks are still sorting out what personal information may have been taken. Depending on how severe the breach is, it's possible thieves could use the data to get access to other financial accounts you have and open new accounts at other financial institutions to borrow money in your name.

"Our first concern would be getting people who think they may be one of the 90,000 to start looking at their security everywhere else, apart from the bank," Mr. Boucher said.

Step one: If your account has been breached, or you're worried this has happened, see if you've used the same password and security questions for accounts at other banks or investment firms. If so, change those accounts immediately.

You're not supposed to use passwords multiple times, yet it happens all the time. "Security is inconvenient," Mr. Boucher said. "We all do those silly things where we use the same passwords to make things simple."

Step two: Go online and look at all your financial accounts to check for unauthorized activity. Mr. Boucher suggests you call your bank or investment firm if anything looks off.

Step three: Look at your credit report to see if there has been any unauthorized activity. Check with your bank or credit card issuer to see if it offers free access to at least some of this information – among those that do are Bank of Nova Scotia, Capital One and Royal Bank of Canada. Also check online lenders such as Borrowell and the website Credit Karma.

Look for new loans or mortgages set up in your name, and at inquiries made by lenders into your borrowing history. Either could be the result of thieves using your personal data to steal money. Mr. Boucher raised the idea of subscribing to an alert service via credit monitoring firms TransUnion or Equifax where you're notified if there are any changes to your credit report. However, these services can cost nearly $20 a month.

Step four: Look out for notifications that thieves are accessing other of your online accounts – social media, for example. You'd be notified about this via e-mails saying someone has tried to access your account from a different phone or computer than usual. Again, change your password if required.

Some people affected by the Simplii breach have reported that money was taken out of their accounts via unauthorized e-transfers. An additional risk is that your personal data is used to set up loans or mortgages that provide cash to thieves and leave you to pay up. The thieves who stole the BMO and Simplii data are asking for a ransom, but it's possible they could sell personal data to other thieves who will actually use it.

As last year's data breach at Equifax showed, hacking is a constant threat to businesses operating online and their customers. But this latest event involving BMO and Simplii is a shocker in a couple of different ways.

The focus on cybersecurity in banking has always been on the individual, not the institution. Mr. Boucher said individuals do need to watch for phishing e-mails that can either lock up your computer and hold it for ransom, or fool you into providing a login and password for a financial account. He also warns about fake public WiFi accounts that are designed to capture your private data.

Part of the branding of big banks – Simplii is owned by Canadian Imperial Bank of Commerce – is their image of impregnability. That's a big reason why the market share of purely online banks in Canada is feeble at less than 7 per cent, according to consulting firm McVay and Associates.

Mr. Boucher predicts that the security breach will make people more conscious of the risks of online banking. "I think it would be silly to say it won't have an impact," he said. "The reality is that pretty much anyone can be hacked."