FINANCIAL POST

May 27, 2016

'With convenience comes vulnerability': What to do if you're the victim of financial fraud, and how to protect yourself

By Melissa Leong

Joan Cruz received a bizarre email from an acquaintance in November. He said that she had mistakenly sent him an email money transfer. The official-looking email asked that he click a link to accept the funds and input his banking information.

But Cruz had not sent him any money in the first place. Suspicious, she checked her bank account and found it empty.

"What the eff?" She thought. "There's got to be some mistake."

A fraudster had hacked into her account, cleaned it out and then went through her list of email money transfer recipients to try to victimize them.

"I was ashamed of it, then angry," says the 38-year-old Toronto artist and single mother. "I was scared that the bank wouldn't believe me. I thought, 'What if I can't get my money back?'"

With convenience comes vulnerability

The reality is that with our heavy reliance on our smartphones, our tablets and our computers, and with the country moving towards being a cashless society, the threat of cyber crimes and financial fraud has never been greater. Cruz is among the vast majority of us who bank online for its ease and convenience; according to the Canadian Bankers Association, more than three-quarters of us use online banking.

"With convenience comes vulnerability," says Kelley Keehn, personal finance educator and author of Protecting You and Your Money: A Guide to Avoiding Identity Theft and Fraud. "Especially with millennials, they're extremely tech savvy but their level of privacy and security knowledge is very low."

Millennials are extremely tech savvy but their level of privacy and security knowledge is very low

We've all likely engaged in some risky behaviour. For example, do you shop online? Have you used the same dedicated password for multiple sites? Do you download apps? Have you ever shared your social insurance number - perhaps in an email to a car salesman who is leasing you a vehicle, or an accountant who is preparing your taxes?

As for Cruz, where was her vulnerability? "Honestly, I have no idea," she says. A bank official suggested that she might have done some banking on her phone while connected to public wifi.

"The bad news is that a lot of people out there are trying to steal your money," says Tom Keenan, adjunct professor of computer science at the University of Calgary and author of Technocreep.

The good news is that if you didn't commit fraud, your bank will likely give you back your money, he adds. But you'll have to meet certain conditions set out in your security policy such as say, not sharing your password with your spouse or with any third-party financial aggregators, which can include popular budgeting apps like Mint.com.

Cruz's bank froze her account - as well as her acquaintance's finances - and spent a week investigating the theft. Luckily, in addition to returning her money, the bank also refunded her the interest that she accrued while she lived off of her line of credit.

To avoid being victimized, we could just use our smartphones to make calls and our computers to play solitaire, but it may be better to simply take the following steps to safeguard our money.

Do not click that link. You've gotten an email from a friend or co-worker saying, "Check this out," or "look at this photo of you," with a link. Delete it.

"There are links - we sometimes call them drive-by-downloads - you don't even realize that your computer has downloaded a program. Now your computer is vulnerable and someone can take over by remote control," Keenan says. "Once you get infected, the bad guys will start to look for things on your computer. They might find your 2015 tax return.... There's a treasure trove of identity theft information on most people's computers that really shouldn't be there."

If that isn't terrifying enough, Keenan also warns of ransomware where, after you click a link, a cyber criminal locks your computer and demands a ransom to release it. These attacks have increased dramatically in recent years and victims include everyone from a Calgary wine store owner, who shelled out $500 in bitcoin to free his computer, to a California hospital that could not treat patients when its network was locked.

Use caution when downloading apps. You may want to download a free Candy Crush app to help you beat an impossible level, but do your homework first. Keehn writes in her book that Android malware has been on the rise. Check out the reviews and the developer of an app before you download it. To be even safer, stick with well-known, popular apps. That way, you won't accidentally download a program that allows a hacker to watch your every move, text and email.

The bad news is that a lot of people out there are trying to steal your money

Remember that you're taking a gamble by sharing your financial passwords with any program such as a third-party aggregator. Doing so may nullify your security guarantee with your bank if you ever have money stolen. If the convenience is worth the risk, change your complex passwords frequently, always log out and perhaps set up another email address attached only to the aggregator. If it's not worth the risk, you can still use other budgeting and finance apps that don't require your personal information; you just might need to do a bit more work to populate your spreadsheets.

Consider paying for a strong anti-virus, anti-spy and anti-malware program for your mobile devices and your computer. Opt for reputable software to avoid nefarious programs masquerading as free anti-virus programs. Also, keep all of your software up-to-date. If all else fails, have an emergency safety mechanism - an app that will wipe all of the data from your phone if it's stolen.

Watch out when accessing public wifi. They're called evil twin hotspots. "A hacker may have set up a rogue access point … disguise it as Pearson Airport Free Wifi and people might connect to (it)," Keenan says. "The other possibility is to hack the service." Then they can watch all of the traffic. You can purchase virtual private network (VPN) software to encrypt traffic as an added precaution, he says.

Turn off your Bluetooth when you're not using it. Keehn references a 2013 warning from the Southern Alberta Better Business Bureau about hackers accessing texts, contacts and photos through Bluetooth wireless connections.

Consider identity theft insurance. Coverage can often be tacked onto your home insurance policy. It covers the expenses that you'll incur when dealing with the problem such as notarizing documents, loan re-application fees, credit reports and sometimes legal fees. Some insurance policies also include support where a case manager walks you through the process. Both Equifax and TransUnion provide credit monitoring that will alert you to any potential fraud.

Monitor your own activity and contact your bank immediately if something is awry. "You want to check your banking online as often as possible," Keehn says. "I check mine every day…. I've had my credit card compromised at least six times."