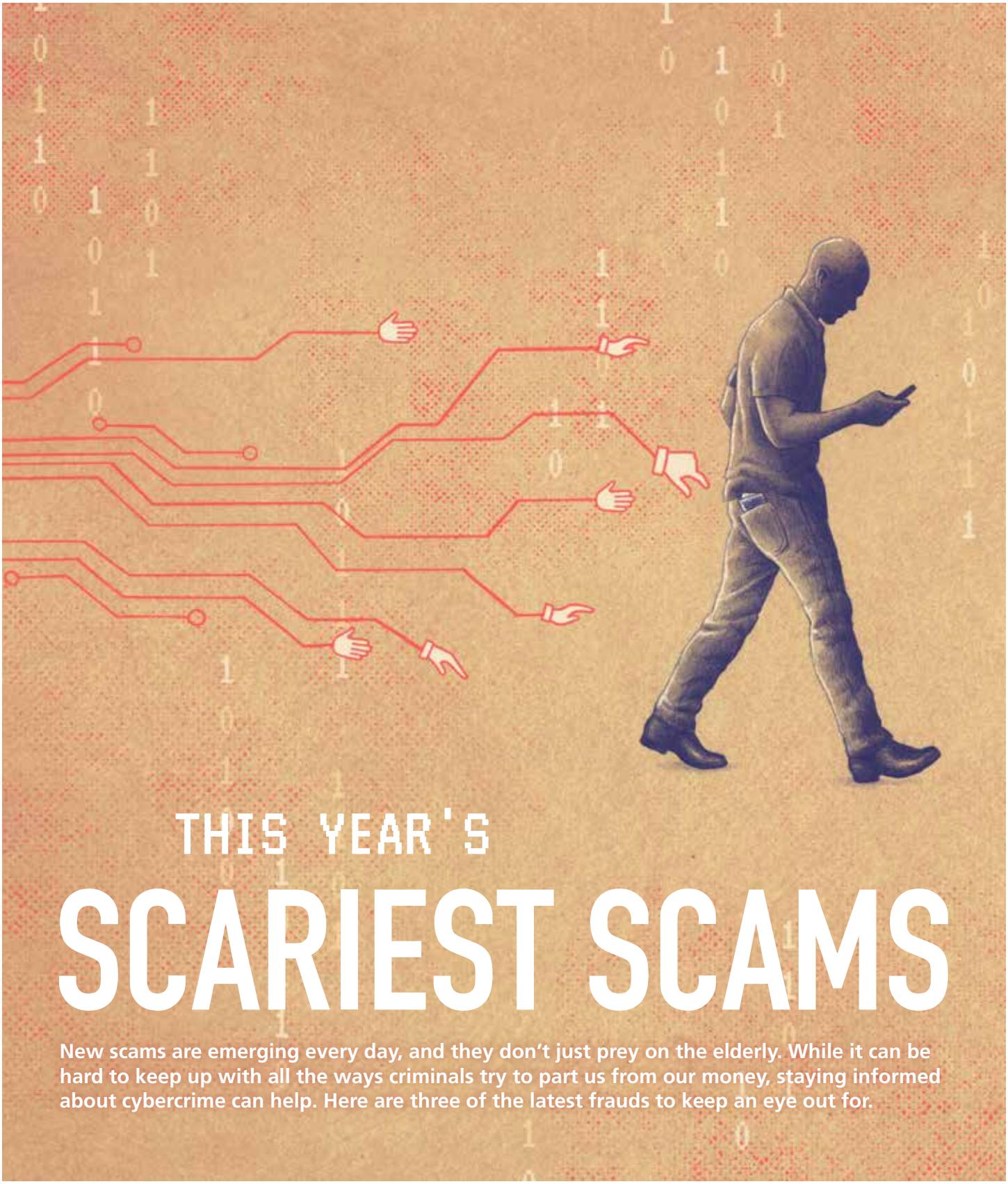


THIS YEAR'S SCARIEST SCAMS

New scams are emerging every day, and they don't just prey on the elderly. While it can be hard to keep up with all the ways criminals try to part us from our money, staying informed about cybercrime can help. Here are three of the latest frauds to keep an eye out for.

When it comes to protecting yourself and your money from digital fraud, it may be easy to think it will happen to someone else. While it's true that many financial scams are designed to prey on vulnerable communities, such as seniors and new Canadians, a recent TD survey suggests that nearly three quarters of millennials also worry about becoming a victim of cybercrime.[1] This may be due to the fact that whenever it feels like the newest round of scams has been exposed and defanged, criminals step up their games and create fresh rackets. In 2016, the Canadian Anti-Fraud Centre reported on 30 different kinds of scams, and the Competition Bureau estimates that from January 2014 to December 2017, individual Canadians lost more than $405 million to fraudsters.[2] There are more every year. In many cases, emerging scams are variations of long-running predecessors, but others are new and ingenious. We asked two security specialists — Franklin Garrigues, VP of Digital Channels at TD and Jean Turnbull, VP of Financial Crimes and Fraud Management at TD — to guide us through three of this year's newest scams and tell us what to look out for.

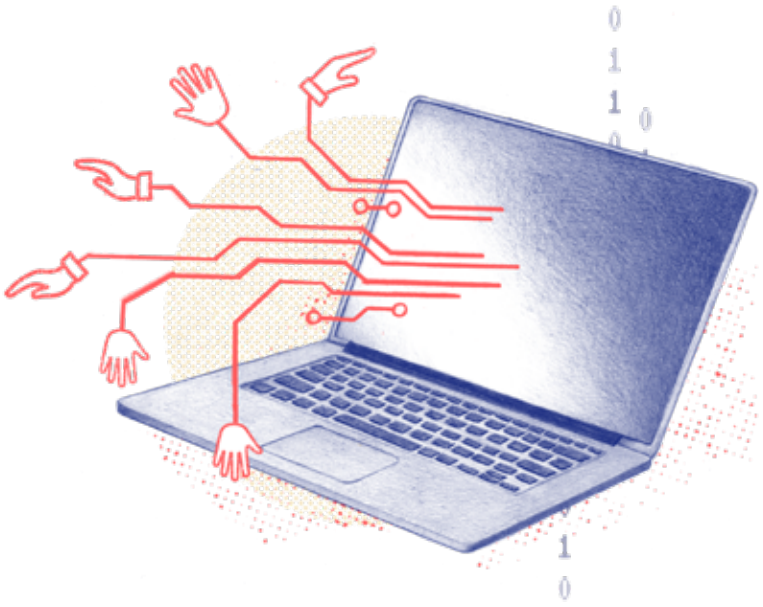
1. Don't Bank on These Apps

New malicious banking apps are increasingly being found on legitimate smartphone app stores, and they can increasingly look like the Real McCoy. In June of 2018, three fake banking apps were found on a popular app store, each promising an easy and convenient way for customers to increase their credit limits. Once installed, users were asked to supply their credit card login information in order to activate new offers. When they did, the information was leaked online to be accessed and used by others.[3]

How to Avoid it?

Garrigues says that using your phone's official app store is still one of the best and safest way to download an app. "Your bank's website may direct you to the correct

app on the store, rather than having to browse for it," he says. "Think twice about downloading an app from anywhere other than your phone's app store." Even then, it's good practice to spend some time reading reviews and examining the quality of an app and its description before download. Poor grammar and spelling errors can be an early flag that the application is probably not legitimate.



2. Cryptocurrency Cons

In August 2018, the U.S. Federal Trade Commission alerted consumers to a Bitcoin blackmail scam targeting men. Scammers have been sending email messages to men, often in affluent neighborhoods, insisting they have evidence of alleged affairs or indiscretions. They demand payments of thousands of dollars in Bitcoin or other alternative cryptocurrency in exchange for keeping quiet. The letter usually includes instructions on how to use virtual currencies to make a payment. Criminals want to be paid in Bitcoin and other virtual currency because it's harder to trace.[4]

How to Avoid it?

"This is a typical con with a new tech twist to it," says Turnbull. "The cryptocurrency aspect makes it very hard to trace." If you do receive an email like this, it's best to ignore it and not respond. Turnbull warns not to send money to anyone you don't know, particularly in virtual currency. Remember that once funds are sent, they're gone, and you're responsible for that financial loss.

3. Shimming Sham

It was only a few years ago that "skimming," a scam in which false fronts are attached to ATM and point-of-sale terminals to capture the information on credit and debit cards, entered the general lexicon. Now comes "shimming," a similar but rare hack that targets the data contained in your card's embedded chip.

A paper-thin device is inserted into the slot of an ATM or point-of-sale terminal, giving fraudsters access to the private data on your card. In recent years, the RCMP have found shimming devices inserted in retail point-of-sale machines in British Columbia and Alberta.[5]

How to Avoid it?

Turnbull says this type of fraud is rare, in part because the chip technology in your card is already quite secure. The chip itself cannot be duplicated, though criminals can use the captured data to clone a duplicate card with a magnetic strip that can be used at points-of-sale that don't employ chip readers. While the odds of this happening to you are slim, Turnbull says "awareness is key and it's also a good idea to take preventative measures such as making sure that you are the one to swipe, insert or tap a card." Turnbull also points out that while you may limit your risk by using your card at "tap and go" contactless devices and ATM machines you're familiar with, it's always a good idea to monitor your accounts for suspicious activity. "Each payment method comes with its own risks," she says.

Be a Tattle-Tale

If you think you've been scammed, report it. Even though you may feel vulnerable and embarrassed, both Turnbull and Garrigues stress that authorities can only stop criminals with our help. The best place to report a scam is to the Canadian Anti-Fraud Centre, which works closely with local law enforcement agencies to help spread the word and alert others. By working together they can identify evidence and connections among seemingly unrelated cases. It helps too if you're diligent about keeping records, gathering all emails, text messages, financial statements and receipts to provide to law enforcement.

Next, Garrigues also states that you should notify your bank to cancel your card and issue a new one if you detect fraudulent charges. "Many banks have protection for customers who have been defrauded, depending on the type of fraud and how their information was compromised," he says, "so ensure you notify your financial institution if you believe you've been a target of fraud."

Garrigues also stresses the importance of maintaining the operating system of your phone and ensuring it's up to date. "Updates contain important fixes. And consider using anti-virus programs to help protect your devices," he says. If you suspect you've been the victim of scammers, you can also consider putting an alert on your file with a credit agency and your account will be scrutinized more closely.

Don't wait to report, time is of the essence when dealing with fraud.

— Denise O'Connell, MoneyTalk Life

[1]TD. Is your smartphone a friend or foe? March 8, 2018. https://newsroom.td.com/featured-news/is-your-smartphone-a-friend-or-foe. Accessed September 24, 2018.

[2]Competition Bureau of Canada. Fraud Facts—Recognize, Reject, Report Fraud. February 22, 2018 http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04334.html. Accessed September 24, 2018.

[3]International Business Times. July 30, 2018. Fake banking apps of 3 Indian banks used to dupe credit card owners. https://www.ibtimes.co.in/fake-banking-apps-3-indian-banks-used-dupe-credit-card-owners-776423. Accessed September 27, 2018.

[4]CNBC. 'I know you cheated on your wife.' Growing blackmail scam demands payment in bitcoin. January 22, 2018. https://www.cnbc.com/2018/01/22/growing-blackmail-scam-demands-payment-in-bitcoin.html. Accessed September 27, 2018.

[5]RCMP. Vigilant Coquitlam Retailer Stops High-Tech Shimmers. January 26, 2017. http://bc.rcmp-grc.gc.ca/ViewPage.action?siteNodeId=2087&languageId=1&contentId=49796. Accessed September 27, 2018.