

# Seven tips on how to protect yourself from fraud

**Fraud has been around for a long time—we all know of a family member, friend or colleague who has fallen victim to a scam. According to the latest numbers from the Canadian Anti-Fraud Centre (CAFC) and the Competition Bureau, close to 90,000 complaints were lodged in 2016, and a total of \$91 million were lost to fraud.**

Here are testimonials from seven fraud victims, and our tips on how to detect fraud and prevent it from happening to you.

## **1. Don't believe every email or text message you receive.**

Phishing is one of the most common types of fraud. In this case, emails or text messages are sent to individuals to trick them into divulging personal information, such as their bank details or social insurance number. Anyone who shops, pays or banks online can become the target of a phishing scam. It's important to be on your guard—especially since, most of the time, the content of these fake emails and text messages appears to come from a reliable, well-known source. In fact, the phishing websites that scammers use do a good job of masquerading as official websites.

Zoe, a publicist, experienced a phishing scam last fall. “A fraudster posed as my Internet service provider, and told me that they needed to refund an overpayment that I'd made to my account,” she recounts. “I was told to click on a link via text to retrieve my money. The next day, I saw that hundreds of dollars were missing from my account. That's when it sunk in that they'd stolen my banking information.”

To prevent the same thing from happening to you, refrain from answering text messages or emails of this sort or clicking on attached links, and never give out your personal information and banking details. When in doubt, contact the company that is requesting the information.

## **2. Go to the experts when you're just starting out.**

Although many people are buying into the cryptocurrency craze and eager to invest during the current bubble, very few actually know anything about it.

Jonathan, a 25-year-old entrepreneur, learned this the hard way. "Like a lot of people, I thought I could make a lot of money from cryptocurrencies," he recalls. "After doing a few searches here and there, I came across a website that appeared legitimate and decided to invest. It ended up being a scam and I lost several thousands of dollars. It didn't discourage me from investing, but it made me more prudent. Nowadays, as a cautionary measure, I turn my investments over to a financial advisor."

If you're intent on managing your own investments, another option is to do business with a reputable brokerage firm, which ensures safe and secure transactions. Always keep in mind that going to a specialist is a lot cheaper than getting scammed!

## **3. Don't share your bank details over social media.**

This may seem like common sense, but it's something that's increasingly prevalent on social media right now, especially on Facebook. Have you ever received a private message from someone pretending to be a friend in urgent need of money? This happened to Stephanie, a political science student, who wanted to help a friend out after she supposedly lost her wallet while on vacation in Australia. Unfortunately, the person on the other end turned out to be a scammer and had hacked her friend's Facebook account.

"To be honest, it was hard for me to detect, since the scammer mimicked my friend's writing style to a T," she recounts. "She said she lost her wallet and needed money for a rental car. The next thing I know, close to \$3,000 is charged to my credit card. It doesn't make me stingier about helping my friends in need, but it's certainly the last time I'll ever share my bank details through a conversation on social media. If it's really an emergency, I'll get on the phone with that person and handle it directly that way."

If you find yourself in this kind of situation, refrain from divulging your banking information, unless you are certain you are using a secure line of communication.

#### **4. Don't share personal identity information.**

Unlike other types of fraud, identity theft occurs when a criminal gets access to someone else's means of identification, with or without the victim's knowledge. An identity thief can obtain a victim's information by stealing his/her wallet, but also through using malware by hacking the victim's computer, smartphone or other device. Identity theft can damage your reputation or credit rating, as was the case with Daniel, whose identity was stolen when his social insurance number fell into the wrong hands.

"I've been freelancing for different companies for some time now, and I always included my social insurance number on invoices," says Daniel. "One day, I went to take out money on my credit card, but the transaction was declined, even though I'd always paid my bill on time. I called my bank to find out what was going on. The advisor told me they could no longer issue me cash advances because of my credit score. I requested a credit report from Equifax—having never requested one before—and saw that several loans had been taken out. And I've never taken out a loan in my life! That's when I knew my identity had been stolen."

To prevent Daniel's story from happening to you, make sure you only give out your social insurance number when absolutely necessary. Otherwise, ask if another piece of ID can be used. Before giving out personal information, ask how your details will be used and whether they'll be sent to a third party. Leave any documents containing your personal information at home in a safe place. To be on the safe side, you can also regularly request a copy of your credit report from credit reporting agencies like Equifax or TransUnion.

#### **5. Don't pounce too quickly on online deals.**

As the popularity of online shopping continues to grow each year, so too has the amount of money lost to online fraud—a figure that has reached over \$8 million in Canada. Julie, who works in the restaurant business, can attest to this.

"It happened during Black Friday. I was shopping for an online deal on shoes that I'd been eyeing for a while, when I came across an offer that was too good to pass up. I got so excited that I didn't bother to check whether the site was legit. In the end, I was swindled out of \$1,500 and never received the shoes. Now, even when it's not an impulsive buy, I'll take the time to check the website and its reputation, and go with trusted sites even if it means losing out on a deal."

It's important to exercise common sense when shopping online. If an offer appears too good to be true, it may very well be a trap.

## 6. Don't be blinded by love.

They say love is blind. For Eric, a young 40-something university professor who wanted to find his soul mate, the old adage is all too real. A wallflower by nature, Eric was drawn to the online dating scene. After chatting with a few potential partners, he thought he had finally found The One. Or so it seemed...

"There was definitely chemistry between us," he recalls. "We spent a month talking online every day and it felt like we were on the same wave length. But, strangely, we never got around to meeting. One day, she wrote me in a panic, telling me that her mother had major health problems and that she needed \$7,000 to pay for hospital bills. She said she didn't have the money, and pleaded with me to lend it to her. Under the spell of her sweet words, I cracked and transferred her the money. But, once that was done, I never heard from her again. But I can't blame the dating site. I've met some great women through it since then."

According to the latest numbers from the Canadian Anti-Fraud Centre (CAFC) and the Competition Bureau, over 17 million \$ in Canada have been lost to these "sweetheart scams." A tip for those looking for love online: be wary of anyone who's more interested in your financial situation than they are in you, especially before you've even had a chance to meet them.

## 7. Exercise caution when buying or selling stuff online.

Fraud is increasingly becoming an issue on peer-to-peer marketplace sites like eBay and Kijiji. Arthur experienced it firsthand a few months ago.

"I wanted to buy a cell phone for cheap on Kijiji," he recounts. "The seller asked me to pay through Canada Post, saying it was safer and faster. I shouldn't have trusted him, but I did. I never received my phone, and a lot of the money in my account went missing."

Although marketplace site users rate their experience as positive, many others like Arthur have fallen victim to fraud. When it comes time to pay, use secure payment services like Interac or PayPal, which allow you to send a payment to another person over the Internet from your checking account or using a credit or debit card. Never send a cheque and be careful when choosing an online payment processor. Scammers typically use these services and will even go as far as to produce fake documents. Of course, your best course of action is to stick to local and in-person transactions.

These seven tips should help to keep you protected from fraud, though to be fair, no one is safe from scams. When in doubt, read over these testimonials. They may steer you away from disaster and serious financial losses. You can also refer to our ABCs of security at any time.

*Edited on 14 February 2018 by National Bank*