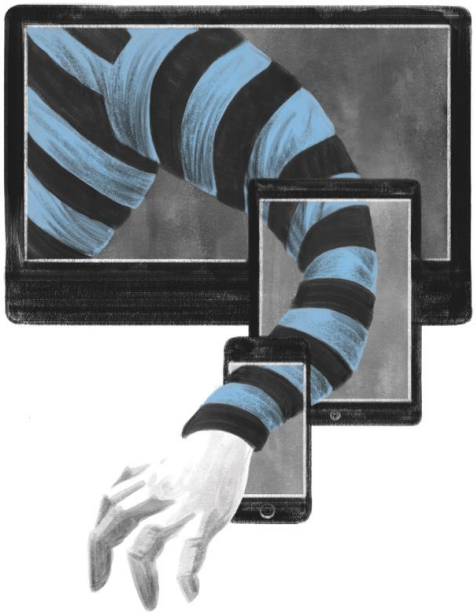
FINANCIAL POST

May 10, 2017

These five tech-based money scams are making millennials look like suckers

By Melissa Leong

All that sharing with less caring, and clicking with less checking, can lead to money lost, ruined credit and identity theft



The job posting was for a personal assistant. It paid $350 a week and would involve picking up mail, dropping packages off at the post office and some shopping.

Kaya was 31, had just returned to Toronto after working overseas and was desperate to make some money, so she replied to the Craigslist posting.

"I Googled the employer," the now 36-year-old business graduate said. "He was listed as a curator at an art gallery in Australia, but he said he lived part time in Canada."

He sent her a cheque for $2,950 and asked that she cash it, keep $350 as payment and wire the rest to a business to purchase some furniture. She brought the cheque into her bank to deposit into her account and the teller told her everything was fine - but, of course, it wasn't.

"A week later, the bank called and said that the cheque was fraudulent. The money was gone. That was almost everything that I had in savings," she said. She asked that her real name be withheld to avoid being recognized by the scammer. "You feel so helpless. I was super embarrassed. I didn't tell my parents."

Experts warn that millennials are increasingly prime targets for money scams, including the con that took Kaya's money. About half of the fraud victims in Canada are from Generation Y (followed by Generation X at 29 per cent, Baby Boomers at 17 per cent and the Silent Generation at 3 per cent), according to a study last year by ratings agency Equifax Inc.

"They're new at managing their money. They all need money and people who need money are usually good victims," cybersecurity expert Tom Keenan said.

Also, millennials suffer from optimism bias and are therefore less cautious. And while they're the most technologically savvy cohort, they're less savvy with privacy and with security.

Millennials are more likely than other generations to admit they share their PINs with family and friends, use their personal information such as their birthday as their PIN and share their credit card number over the phone or email, according to a survey for Capital One Canada.

"Millennials have grown up in the sharing economy so they're just so used to sharing information about their personal lives and their details with friends and people on social media," said Brent Reynolds, managing vice-president at Capital One Canada.

All of that sharing with less caring, and that clicking with less checking, can lead to money lost, ruined credit and identity theft.

Here are five financial scams that are particularly dangerous for millennials.

Fake job offers

Like Kaya, you may see a job posting online or on campus. It may even have the name and logo of a reputable company. But it could still be bogus. Or you may get a text to be a mystery shopper or a covert consumer where you receive a cheque to use for shopping and to evaluate products.

"For every real one, there are 10 scams," said Keenan who teaches at the University of Calgary and wrote a book called Technocreep. (Check mysteryshop.org for legitimate companies.)

If the job asks for money to sign up or for training, run the other way. Never pay money upfront for a job, Keenan said. Be cautious of jobs that tout "work from home," "start immediately" or "no experience required."

Online shoppers

"Millennials are so eager to shop online ... But there are plenty of sites out there that are not what they seem," Keenan said. "You can make up a totally fake store. There are enough rogue credit card company processors that will take people's credit cards and charge them money or they'll now have your credit card, expiry date and maybe the (three-digit number) on the back, and that can be sold."

To see if an online business is legitimate, Google the company for reviews, look for the lock icon in the status bar of your browser and, if available, use PayPal to checkout.

Check your account statements regularly for any errors or fraudulent activity; some credit cards have real-time notifications built into their apps to let you know when a purchase has been made. Also, request a free copy of your credit report from Equifax or Transunion once a year to monitor your activity.

Crowd-funding sources

"People have pulled off all kinds of scams," Keenan said. "They've put up sob stories, said they're dying of cancer when they're perfectly healthy; they've invented wonderful products that they're going to make."

Look into the person soliciting funds. Stalk their social media pages. Can they be contacted? Are they listed on more than one crowdfunding site (is it a copy of another real project)? As always, if the product sounds too good to be true, it probably is.

Bad behaviour scams

"It's awful to imagine, but blackmail is alive and well at our colleges," Keenan said. "It's very possible someone has a photo of you and even someone who appears to be a friend or a lover could use it against you. They may even ask for money in exchange for the photos ... Anything you post, you have to be happy if your grandmother sees it."

If you're a victim of "sextortion" (extortion involving sex-related digital images), contact police.

Being careless with technology

You download a fake app and infect your phone with malware that allows a criminal to look through your files. Or you click on a link from a co-worker and download ransomeware that locks your computer until you pay a ransom to release it.

Or you connect to a coffee shop's free Wi-Fi and now a crook who has set up the fake hotspot or hacked the service is watching your every move.

People often let their guard down when they use smartphones.

"You're on the train, you're running around and ... texting constantly," said Kelley Keehn, personal finance educator and author of Protecting You and Your Money: A Guide to Avoiding Identity Theft and Frauds.

"We don't have that spidey sense when we're holding our dear smartphone. We're vulnerable to these crime organizations around the world trying to defraud us every second of the day."

Consider buying a reputable anti-virus, anti-malware program for your computers and mobile devices, and keep your software up-to-date.

Financial Post
Twitter.com/lisleong
Illustration by Chloe Cushman / National Post

References

1. business.financialpost.com/personal-finance/young-money/buckle-down-and-stop-being-so-impulsive-three-millennials-get-the-money-makeover-treatment