commission, now requires, as of Dec. 19, that these providers block calls with numbers more than 15 digits long or that can't be dialed (such as those with a string of letters or zeros), or provide more advanced call-filtering services.

"Legislation would put the responsibility back on the organizations, and that will hit the cellphone carriers," says Matt Coveart, identity theft expert at DragonFly I.D., an identity restoration service provider. "They are going to have to do more."

Mitigate it

- Avoid answering any calls received from unknown numbers.
- If you do answer the call, immediately hang up and do not answer any questions.
- Never give out any personal information (such as social insurance numbers and banking information) without verifying the request is legitimate.
- Report any calls received to the Canadian Anti-Fraud Centre.
- Keep abreast of offerings by your mobile provider to help stop these calls

2. Porting for profit

Identities are now being compromised by phone porting, whereby the fraudster, with phone number in possession, links that phone to another SIM card, enabling access to its apps, cloud and email accounts and more.

From there, the fraudster may call the mobile service provider, impersonating the phone owner and make account changes or report the device lost or stolen. They may change passwords on accounts using the "forgot password" option, gaining access through verification codes now sent to them.

Meanwhile, victims may be locked out of their accounts, unable to call, text or use data. They may fall prey to extortion threats or have their bank accounts drained and **credit cards** racked up.

"It's very targeted. They find an old cellphone bill and try to leverage that information. The representatives believe the device is stolen or lost," says Coveart. "They [cyber criminals] say they would like to have the phone ported to another device. Once it's ported to that device … there are all sorts of impersonation scams from that point."

Mitigate it

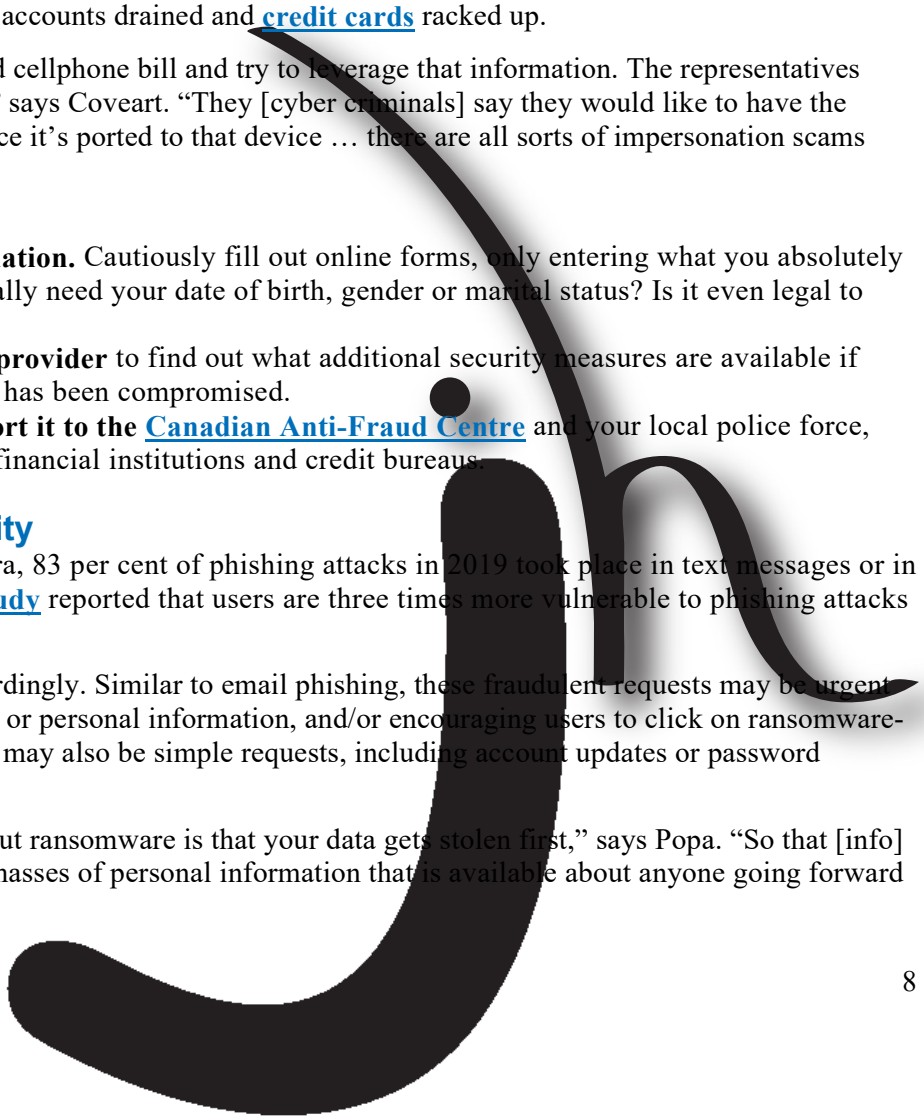
- **Protect your personal information.** Cautiously fill out online forms, only entering what you absolutely need to. Does this company really need your date of birth, gender or marital status? Is it even legal to request it?
- **Contact your mobile service provider** to find out what additional security measures are available if your phone is lost or stolen, or has been compromised.
- If your identity is hacked, **report it to the Canadian Anti-Fraud Centre** and your local police force, and immediately contact your financial institutions and credit bureaus.

3. Phishing for vulnerability

According to security firm Wandera, 83 per cent of phishing attacks in 2019 took place in text messages or in apps. Meanwhile, a recent **IBM study** reported that users are three times more vulnerable to phishing attacks on a mobile device than a desktop.

Hackers know this, and target accordingly. Similar to email phishing, these fraudulent requests may be urgent or threatening, demanding payment or personal information, and/or encouraging users to click on ransomware-infected links or attachments. They may also be simple requests, including account updates or password confirmations.

"What people don't understand about ransomware is that your data gets stolen first," says Popa. "So that [info] goes out there and it just joins the masses of personal information that is available about anyone going forward and forever."



Mitigate it

- **Never respond** to (or click on) suspicious messages, links or attachments sent via text or apps.
- **Report suspicious messages** to your mobile service provider, and anti-fraud centre.
- If the message sent looks legitimate, **contact the alleged sender** (i.e., your bank) before responding or entering any information to confirm receipt.
- **Update any passwords/log-in credentials** associated with targeted accounts.

4. Mining for identities

With access to one piece of personal information, fraudsters can mine for more data to piece together an identity, Popa says. With the amount we share online – from birthdates, to family members, to marital statuses, to employers – we make it easy for them, he adds.

A quick search of a phone number, he says, can lead to its mobile service provider. One phone call to that provider can reveal account details when the right questions are asked. One account detail can direct to a social media account. Furthermore, Popa adds, fraudsters can use data they collect from multiple individuals and combine the information to create virtual people.

"It could be a phone number. It could be a picture. It could be a home address, social media profile. Any one of these identity elements can give rise to an opportunity to gather more data about an individual," he says.

"You can mix someone's social insurance number with someone's home address and suddenly you don't have someone who really exists. That's called a synthetic identity … and you can multiply your opportunities for making money."

In an internal report completed last August, and **obtained by the Canadian Press** through an Access to Information request, Privacy Commissioner Daniel Therrien called out federal political parties for not adequately protecting Canadians personal information and misusing voter data without proper consent. The report states that Canadian privacy policies fall short on setting limits on how data is used, how long it is kept, whether it is accurate, and how it is safeguarded through security systems.

Mitigate it

- When possible, **create distinct digital identities** across platforms and accounts using pseudonyms or nicknames, different email addresses, fake birthdates, and so on, advises Popa. Keep track of this information for customer service. "People need to understand one thing. The person that they are in real life is different than the digital identity that they have online. Divorce these two concepts," he says. "The way they do that, is to be as pseudonymous as possible online."
- **Use an offline password manager** and database to keep track, creating new and distinct passphrases, rather than passwords (minimum of 12 characters, including spaces and punctuation), advises Popa. "Type in a sentence. It's much easier to remember and it's less likely to guess it."

These stories first appeared on CPA Canada's online news site.

BUSINESS MATTERS is prepared bimonthly by Chartered Professional Accountants of Canada for the clients of its members.

Authors:

Ask the right questions when hiring virtually, pros say	Sophie Nicholls Jones
Four common questions about the CRA's principal residence exemption	Sophie Nicholls Jones
The tax consequences of leaving Canada permanently	Mathieu De Lajartre
Four threats to watch out for when a hacker gets your phone number	Sophie Nicholls Jones