techtip

15 Tips for preventing identity theft and online fraud

Cyber criminals and identity thieves want to steal your personal information to commit fraud. They may try to get a credit card in your name or to access funds in your bank account. On top of directly losing money, your credit status can be damaged and it can take a great deal of time and expense to restore your good name.

And this goes beyond being an issue of personal concern. LawPRO has seen situations where law firm bank accounts were hacked and where law firm bank account information was used on counterfeit cheques.

There are many different ways to steal personal information. Identity thieves will target you online and by "dumpster diving" in your garbage. You should also be familiar with the common ruses that criminals use to trick you into disclosing personal information.

Here are some simple steps you should take to protect yourself from identity theft and online fraud:

1 **Protect your Social Insurance Number:** It is a cornerstone of your identity and one of the best pieces of personal information an identity thief can have to create a new you. Don't carry your SIN card in your wallet or write your SIN number on your checks. Only give out your SIN when absolutely necessary for tax purposes, and never for identity purposes.

2 **Keep your PINs private:** Never write the PINs for your credit/debit cards on the cards themselves or on a slip of paper kept in your wallet. Watch for "shoulder surfers" and always use your free hand to shield the keypad when using an ATM or paying a cashier.

3 **Don't let your mail fall into the wrong hands:** Thieves can get a considerable amount of personal information from your mail. Empty your mailbox promptly, or better yet, install a mail slot that goes directly into your house. Ask the post office to hold your mail or get a neighbour to collect it when you are away. Pay attention to your billing cycles and if bills or statements are late, contact the sender.

4 **Keep your receipts:** Receipts are essential for cross-checking your billing statements (see the next tip.). Keep receipts for refunds and incorrect charges as well.

5 **Review bills and statements:** Carefully review your bills, credit card and banking statements for unauthourized charges or transactions. They are an indication that your credit card has been compromised or that someone has access to your account.

6 **Store personal information in a safe place at home and at work:** Never leave sensitive personal information lying around. This just makes it easier for a thief to steal your information.

7 **Tear up or shred unwanted or discarded receipts, credit offers, account statements, expired cards, etc.:** Destroying these documents will prevent dumpster divers from easily getting a wealth of personal information.

8 Never respond to "phishing" requests for personal information in the mail, over the phone or online: This includes cold-calls asking you to complete a survey or offering a prize. And most importantly – this is probably the most common way that personal information is stolen – never ever reply to unsolicited or suspicious emails, instant messages or web-pages asking for your personal information (e.g., usernames, passwords, SIN number, bank account numbers, PINs, credit card numbers, mother's maiden name or birthday), even if they appear to be from a known or trusted person or business. These "spoofed" messages or websites (see the next tip) will suggest your account has been compromised and will ask you to reset your password. By replying to them you are giving your personal information directly to the thieves.

9 When logging in always check for a secure connection to the correct website: First, look at the address bar in your browser or place your mouse over the link to see if the URL looks correct. It should start with the proper URL (e.g. cibc.com) and not a URL that appears unrelated (e.g., http://124.67.876.5/aed/banklogin). You should also check to see if the web address begins with https://, as opposed to http://. Look for the "s" which signals that your connection to the website is encrypted and more resistant to snooping or tampering. It's always better to go directly to a site by using a bookmark or typing in the site's address directly into the browser address bar.

10 Be careful with odd messages from people you know: If you get a message from someone you know that has odd information in it, their email account may have been compromised by a cyber-criminal who is trying to get money or information from you. These usually take the form of an urgent request for money because the person is stranded in another country and their passport or wallet has been stolen. Don't reply to or click on links in these messages. Contact the person by phone or use an alternate email address to tell them this has happened.

11 Install anti-malware software and firewalls on your computers: Computer viruses, spyware and other types of malware are a fact of life. Just clicking a link in an email or on a website can infect you. All your computers should have anti-malware software installed on them. And to keep up with current threats, make sure your anti-malware software is configured to automatically update itself. When you are connected to the internet, the internet is connected to you. Information can flow freely both ways across your internet connection. You also need a firewall to act as a gatekeeper to prevent unauthorized access to your computers and network.

12 Learn how to safely surf the web: Your internet browser is one of the more dangerous tools in your office. Even casual surfing on the web can expose you to malware and divulge personal data. Learn how to safely surf the web and how to configure your browser so that surfing is less dangerous. This involves disabling some browser features, controlling which cookies can be stored on your computer, and preventing pop-ups.

13 Use "strong" passwords: Don't use a common word or name – and especially one connected with you. Any new password should be significantly different from passwords you have used previously. Make your passwords at least eight characters long – the longer the better. Use a mix of uppercase and lowercase letters, plus numerals and symbols. Use different passwords for different programs, and especially for bank accounts and other sites with sensitive information.

14 Protect the confidentiality of your passwords: Never share your passwords (even with family or friends) and be careful that no one sees you type in a password. If you absolutely have to write down passwords, write them out so they have to be translated in some way. Don't save passwords on your hard drive unless you use a password manager (e.g., LastPass, RoboForm, 1Password). Change any compromised password immediately, even if you only suspect it has been compromised. Change important passwords every 60 to 90 days. Don't let your operating system, browser or other programs cache your passwords.

15 Check your credit report once a year: This can help you spot if someone is using your identity without your knowledge. Check it more frequently if you suspect someone has gotten access to your personal information. ■

Dan Pinnington is vice president, claims prevention and stakeholder relations at LawPRO.