How to prevent account takeover fraud

It can be distressing to learn that a criminal has taken over your bank account, but a few tips from the experts can help you avoid becoming a victim.

You log on to your online bank account and realize someone booked a trip to Mexico using one of your cards, but it wasn't you.

You receive your bank statement in the mail and notice a handful of wire transfers overseas, but you don't remember sending money to Thailand.

You pull a copy of your credit report and notice that you've applied for three credit cards over the last six months, but you haven't.

Scenarios like these are more common than you think: **34 percent of Canadians fell victim to fraud** in 2020.

Q: What is account takeover fraud?

Account takeover fraud occurs when a criminal gains access to your banking profile to either commit theft of your personal information or execute unauthorized transactions.

Criminals take advantage of online resources and social media to guess your basic information, accurately answer your security questions and then gain control of your accounts. They often use their short-term access to drain your savings or request a new credit card.

Multifactor authentication is the strongest way to prevent online account takeover.

Q: Is account takeover something that only happens online?

Account takeover can happen in person at a branch, over the phone through a call centre, through a written request via email, and through mobile and online banking platforms.

One of the more common schemes we've experienced in Fraud is when someone walks into a branch and requests an urgent wire transfer to another province. They typically claim to be travelling; they'll have a very elaborate explanation for why they don't have their bank card with them. In this scenario, what we're really seeing is a criminal impersonating an existing customer, using fake identification created based on information that likely found on social media or via other public sources, trying to transfer money from that customer into their own account.

These criminals are professionals; they know how to make a fake ID, build or imitate a persona, socially manipulate people they meet, and move money as quickly and discreetly as possible.

Q: What can I do to prevent an account takeover at a branch or call centre?

A little caution goes a long way. Never share your card or PIN with anyone, even family members. Grandparents, children and teenagers can be particularly vulnerable to social engineering and may share this type of sensitive information inadvertently. Even your bank will never ask you to share your PIN out loud, in an email, text or call.

When deciding on your PIN, avoid:

- Repeating patterns, such as couplets and straights e.g. 0202 and 3333
- Years, birthdays and anniversaries
- References to popular culture or historic events e.g. 1984 and 2001
- Keyboard patterns like 2580

Keep your bank card in sight and in hand. Don't loan it to a friend, don't add it to someone else's digital wallet, and don't let someone take it out of your hand to conduct a transaction on your behalf. Just as a magician can seemingly make playing cards appear out of thin air, so too can a fraudster disappear or switch out your bank card without you ever noticing.

Q: What about online account takeover fraud?

Multifactor authentication is currently one of the strongest ways to prevent online account takeover.

Multifactor authentication uses more than one piece of information to confirm a customer's identity.

Signing up for text alerts which let your bank tell you if something is different or unusual with your account, such as an email address change or a large transaction. Alerts are more than just keeping track of your spending and bills; they can empower you to own your security.

Text Alerts are available through Digital Banking (online or in the mobile app) and include options to be notified of suspicious account activity, as well as changes to your contact information, large transactions and account overdrafts.

Caution: When you are resetting your login credentials for mobile or online banking, your bank will send you a one-time password. Although a one-time password can help you get back into your account as quickly as possible, it can also be used by criminals to manipulate you into sharing your login information. Your bank will never send you a one-time password, and then later call and ask you to share that password back with us. If this happens to you, someone is trying to take over your account.

Q: How do I make sure that criminals don't guess my password or security questions?

A lot of security questions are easier to guess than you might think

'What was your first car?' a safe guess might be Chevrolet. 'What's your favorite pizza topping?' that Instagram picture of your pineapple pizza would easily give that away. 'What's your favorite childhood cartoon character?' Mickey Mouse might be a good starting point. Most answers are available in your social media posts.

If your password or the answers to your security questions are easy enough for a close friend to guess, they are probably obvious enough for a criminal to figure out. We emphasize the importance of building unique and complex passwords. Below are the top tips for creating strong passwords:

1. **Create passwords that are at least 8 characters long**, using numbers, upper- and lower-case letters and special characters. The more characters, the better!
2. **Use passphrases**. An example is: I love to ski downhill like a star, which becomes 1l0VEtsdhla*.
3. **Never use birthdays, anniversaries, pet's or children's names, seasons** or common phrases like *password*, *12345*6 1 2 3 4 5 6 or *qwerty*.
4. **Never reuse old passwords or share the same password** across multiple sensitive profiles.

5. **Every website & every app:** Use a different complex password.

Q: If I don't have online or mobile banking, will that help to protect me from account takeover?

"In fact, quite the opposite."

Not being signed up for online and mobile banking makes you more vulnerable to account takeover fraud. By signing up, you're making it much harder for someone else to create an online account on your behalf using your credentials.

"Even if you don't think you're likely to use them often, online and mobile banking make it easy to update your address and contact details, give you access to text alerts, and allow you to keep a closer eye on your recent transactions and bank statements."

Q: What should I do if I think I might be the victim of an account takeover?

If you notice unusual activity on your accounts that could indicate account takeover, don't panic. "There are lots of reasons you might not recognize a transaction or get locked out of your account. The first thing you should do is call your bank and validate your suspicions."

Sources:

- *Ontario Securities Commission*
- *Canadian Bankers Association*
- *Alberta Securities Commission*
- *Government of Canada Anti-Fraud Centre*
- *Government of Canada Finance Department: Protection from frauds and scams*