ObserIQ Help Guide: Taking Control Back

Stop. Take a Breath. “You are safe right now.”

Listen. Please know one important thing: This is not your fault.

You were not "tricked" because you made a mistake. Professional criminals targeted you. They target doctors, lawyers, and grandparents every single day.

> **Do not feel ashamed.** Shame keeps you quiet, and silence helps the criminal.
>
> **Do not hide this.** Telling someone is the first step to fixing it.

We will fix this together. Follow these steps one by one.

Step One: Protect Your Money

Do not wait. You need to put a "lock" on your money immediately.

Your 3-Step Checklist:

1. **Call Your Bank:** Look at the back of your debit or credit card. Call that number. **Do not** use a phone number sent to you in a text message or email.
2. **Call Your Credit Card Company:** Tell them you want to stop any new charges.
3. **Call a Family Member:** Call a son, daughter, or friend you trust. Tell them what happened. You need a teammate right now to help you think clearly.

What to Say When Speaking With a Bank Representative

If you are nervous, read this exact note to the person on the phone:

> **"I believe I have been the victim of a scam. My personal information might be stolen. I need to speak to the Fraud Department right away to freeze my accounts. Please help me stop any money from leaving my account.”**

Step Two: Lock Your Accounts

Now that the money is safe, we need to change the locks on your computer and phone.

Change Your Passwords:

- Start with your Email and your Online Banking.
- Do not use the same password you used before.

***Tip*:** Make your new password a short, easy-to-remember sentence, like: Blue-Truck-Coffee-22!

Turn on "Safety Codes":

- Ask your bank to turn on "Two-Step Verification."
- This means that they will send you a code to your cell phone every time you log in. Even if a criminal guesses your password, they cannot get in without your phone.

Step Three: Report It

Reporting the crime helps the police protect your neighbours from the same criminals.

1. **Save the Evidence:**

   Do not delete the text messages or emails. Take a picture of them with your phone or write down the phone number that called you.

2. **Call the Anti-Fraud Centre:**
   - Phone: 1-888-495-8501 (Monday to Friday, 10:00 a.m. to 4:45 p.m. Eastern Time; closed on holidays)
   - Online (recommended and available 24/7): https://reportcyberandfraud.canada.ca/
   - You can report anonymously.

3. **Go to the Police:** If you lost money, go to your local police station with your evidence and the reference number the CAFC gives you.

4. **Important warning about recovery scams**

Criminals may contact you again, pretending to be from the police, CAFC, or a "recovery service," and promise to retrieve your lost money for a fee or in exchange for personal information. This is a secondary scam. Never send money, share details, or pay anyone who contacts you unsolicited about recovery. Report any such contact to CAFC immediately.

The “Rude Rule”

You have permission to be rude to a potential scammer.

If someone calls with **Urgency**….
If someone uses **Threats**…
If someone demands **Secrecy**…

Just Hang Up. No need to say goodbye.

Have a “Safe Word”

The Scenario: You get a call. It sounds exactly like your Grandson. He is saying he is in trouble and needs money.

The Defence: Establish a secret safe word.

How it Works:

Caller: “Grandma, I’m in jail, please help!”

You: “What is the safe word?”

Tip: If they don’t know the safe word, hang up. It is a scam.

Spotting the Fingerprints

Scams change, but the “fingerprints” stay the same. Watch for these three signs:

Urgency: “Act now or lose everything!” or “The police are on their way!”

Secrecy: “Do not tell your spouse.” or “Do not call the bank.”

High-Friction Payment: Pay via gift card. Transfer to a Bitcoin ATM.

A Weather Radar for Fraud

Analogy: You don’t walk into a storm without checking the weather. You shouldn’t walk into the digital world without a radar.

ObserIQ is building a tool that automatically scans for Scam Fingerprints.

A Final Note:

By taking these steps, you are taking control back. You are strong, and you are going to get through this.

Accessibility Statement (AODA compliant)

This guide conforms to the Accessibility for Ontarians with Disabilities Act (AODA) and WCAG 2.0 Level AA success criteria (excluding live captions and pre-recorded audio descriptions as permitted). It uses plain language, semantic headings, short sentences, and is designed for high-contrast viewing and screen-reader compatibility. If you require this content in an alternative format (e.g., large print, audio, Braille, or another language), please contact us.