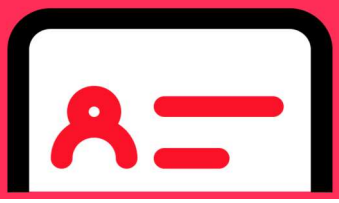
Je me suis fait usurper mon identité



Je renforce ma protection de renseignement personnel

Je protège ma vie privée

## 01
.
**Je signale**
le vol

**Contactez immédiatement le service de police** pour déposer une plainte.
Demandez et conservez soigneusement le **numéro de dossier** obtenu.

- *Déclarez l'incident au **Centre antifraude du Canada** (1-888-495-8501)*

## 02
.
**Je protège**
mes finances

Aviser sans délai vos **institutions financières et émetteurs de cartes** pour faire bloquer ou annuler les cartes compromises et comptes visés .

Contactez **Équifax et TransUnion** pour demander l'ajout d'une **alerte de fraude** sur votre dossier de crédit, et obtenir une copie de votre dossier pour détecter les fraudes.

## 03
.
**Informer**
les organismes concernés

Selon les documents volés, **prévenez** :

- RAMQ (carte d'assurance maladie)
- SAAQ (permis de conduire)
- Passeport Canada (passeport)
- Service Canada (NAS)
- Revenu Québec et ARC (déclaration d'impôt)
- Postes Canada (risque de redirection du courrier)
- Directeur de l'État civil (acte de naissance)

## 04
.
**Constituer**
un dossier solide

**Notez toutes vos démarches** : date, personne contactée, contenu de l'échange.

Recueillez les **preuves** : lettres des banques, avis de fraude, rapports de police.

## 05
.
**Mesures**
de sécurité
**renforcées**

**Changez tous vos mots de passe**, surtout pour courriel, banque, réseaux sociaux.

Mettez en place des **alertes ou verrous de sécurité** via Équifax/TransUnion.

Activez l'**authentification à deux facteurs** pour vos comptes essentiels.

## 06
.
**Recourir**
à des services d'aide et assurances

Certaines assurances-habitation (via Desjardins, CAA, Banque Nationale, Optimum...) offrent une **protection contre le vol d'identité**, couvrant frais juridiques, pertes de revenus et aide administrative.

## Exemple de scénario

Victime : Monsieur Tremblay, 45 ans, habitant à Québec
Fraudeur : Un inconnu ayant récupéré ses informations personnelles (nom, prénom, adresse, date de naissance, numéro de sécurité sociale).

**Déroulement de la fraude :**

- **Vol des données personnelles**
  Le fraudeur récupère les informations personnelles de M. Tremblay via :
  - Un phishing (mail frauduleux imitant une banque)
  - Ou un piratage de sa boîte mail / d'un compte en ligne
  - Ou même un vol de documents papier (relevé bancaire, facture…)
- **Demande de crédit à la consommation en ligne**
  Le fraudeur utilise ces données pour faire une **demande de crédit de 15 000 $** auprès d'un organisme de prêt en ligne. Il fournit :
  - Une fausse pièce d'identité avec la photo du fraudeur mais les vraies infos de M. Tremblay
  - Un faux justificatif de domicile
  - Une fausse fiche de paie
- **Versement du crédit sur un compte ouvert au nom de M. Tremblay**
  Le fraudeur a également ouvert un compte bancaire à son nom (encore avec de faux papiers) pour percevoir les fonds.
- **Découverte par la victime**
  Quelques semaines plus tard, M. Tremblay reçoit une **relance de remboursement** d'un crédit qu'il n'a jamais souscrit. En vérifiant son dossier auprès de la société de crédit, il découvre la fraude.

---

## Conseils de prévention

Ne jamais transmettre ses informations personnelles par mail ou téléphone sans vérification.

Surveiller régulièrement son dossier bancaire auprès de ses **institutions financières et émetteurs de cartes, Équifax et TransUnion**.

Utiliser des mots de passe sécurisés et la double authentification.

---

**Pour toutes questions ou suggestions d’amélioration.**

ubik-infosec.ca @michel-panouillot

**A propos de l’auteur**

Professionnel chevronné en sécurité de l'information, je cumule plus de dix ans d’expérience dans des environnements complexes et diversifiés, incluant les secteurs gouvernementaux, de la formation et militaire. Mon expertise est centrée sur l’analyse en cybersécurité, avec une spécialisation en gouvernance et conformité réglementaire.