Cybermenaces 2025

Vs Aînés au Canada

(Image créée par Dream Lab l'IA de Canva.com)

Contexte général

Hausse continue des cyberattaques visant les aînés :

Les criminels ciblent plus fréquemment les personnes de 65 ans et plus (phishing, fraude « grand-parent », usurpation d'identité, etc.).
Exploitation de la **confiance** et du **sentiment d'urgence** (p. ex. « Un proche est en danger »).

Évolution rapide des techniques d'arnaque
L'**IA** génère des faux courriels/textos ultra-réalistes (phishing automatisé).
Apparition de **deepfakes vocaux** ou vidéos permettant d'imiter la voix/la face d'un proche.

Suite…

Croissance du “smishing” (textos frauduleux)
Nombreuses campagnes d’hameçonnage bancaires ou « gouvernementales » (pension, santé).
Vol de données financières ou personnelles via des liens malveillants.

Transformation numérique accélérée:

Démarches administratives de plus en plus en ligne (gouvernements, banques).
Opportunités (gain de temps) mais aussi **vulnérabilités** (vol d’infos).

TENDANCES PRINCIPALES DES CYBERATTAQUES CONTRE LES AÎNÉS (2025)	DESCRIPTION / EXEMPLES	CONSEILS ET RESSOURCES	RÉFÉRENCES / LIENS
Phishing / Smishing soutenu par l'IA	Messages (courriels, textos) imitant parfaitement un organisme (banque, ARC, Revenu Québec). Orthographe impeccable, logos officiels.	Vérifier toujours l'identité de l'expéditeur (téléphone officiel, site web tapé manuellement Ne jamais cliquer sur un lien douteux.	Centre antifraude du Canada **Éducaloi** (capsule « Vos droits en ligne : comment signaler une arnaque? » – janv. 2025) **Sûreté du Québec** (YouTube, capsules 2025).
Fraude "grand-parent"	Appel ou texto prétendant être un petit-enfant (ou un proche) en détresse. Voix éventuellement modifiée (deepfake vocal).	Exiger de rappeler sur le numéro habituel du proche. Demander un détail que seul le vrai proche connaît (date de naissance, anecdote).	Témoignages médias (La Presse, Le Devoir, janv. 2025). **Ministère Sécurité publique Québec** (capsule « Arnaques téléphoniques » – 5 janv. 2025).

PRIORITÉS ET CONSEILS CLÉS POUR 2025 (D'APRÈS LES EXPERTS)	EXPLICATIONS / GESTES CONCRETS	RESSOURCES CLÉS
1. VÉRIFICATION EN DEUX ÉTAPES (2FA)	Activer 2FA sur les comptes bancaires, courriels, réseaux sociaux. Recevoir un code par SMS ou via une application (Google Authenticator, etc.).	Centre canadien pour la cybersécurité : tutoriels Guides bancaires (mise à jour janvier 2025).
2. MOTS DE PASSE ROBUSTES	Éviter les dates de naissance ou mots simples. Utiliser une phrase secrète ou un gestionnaire de mots de passe fiable. Changer périodiquement.	Capsules gouvernement du Québec (YouTube « Conseils de base pour une meilleure hygiène numérique », 3 janv. 2025).
3. VIGILANCE FACE AUX LIENS ET PIÈCES JOINTES	Toujours taper soi-même l'adresse du site officiel (banque, ARC, etc.). Ne pas ouvrir les pièces jointes inconnues, même si le courriel semble légitime.	Centre antifraude du Canada Ateliers locaux de sensibilisation (Centres communautaires).
4. SAUVEGARDE ET MISES À JOUR	Faire une copie régulière de ses documents (photos, papiers importants) sur un disque dur externe ou le nuage. Mettre à jour son système (Windows, iOS)	Site officiel Microsoft ou Apple (section Sécurité / Updates). Centre canadien pour la cybersécurité (webinaire fin déc. 2024).
5. COMMUNICATION ET SIGNALEMENT	Parler à un proche ou à un conseiller en cas de doute. Contacter le Centre antifraude du Canada et la police si on suspecte une fraude.	antifraudcentre-centreantifraude.ca Lignes d'assistance (Banques, Sûreté du Québec).

https://civbdl.org/wp-content/uploads/2025/01/evaluation-des-cybermenaces-nationales-2025-2026-1.pdf

- Publié par:
- https://www.cse-cst.gc.ca/fr

Gouvernement du Canada | Government of Canada

MENU

Canada.ca

Centre de la sécurité des télécommunications Canada

[Cyberattaques : voici ce que deviennent vos données lorsqu'elles sont piratées | TF1 INFO]

Cyberattaques : voici ce qu deviennent vos données lorsqu'elles sont piratées

Par V. F | Reportage : Roxane Sygula, Paul Bouffard et Erina Fourny

Publié le 7 janvier 2025 à 17h55

L’année 2024 aura été particulièrement agitée en matière de cybersécurité.
En France, plusieurs grandes entreprises ont notamment eu à déplorer des fuites de données qui ont impacté leurs clients.
Malheureusement, l’année 2025 ne nous donnera pas l’occasion de souffler.

Cybersécurité et 3 grandes menaces à surveiller en 2025

Hyperlien de ‘’Presse-Citron’’:
Cybersécurité : 3 grandes menaces à surveiller en 2025

Quand l’IA devient une arme

L’intelligence artificielle simplifie considérablement la tâche des cybercriminels. Certains logiciels malveillants boostés à l’IA peuvent par exemple changer de comportement en temps réel pour échapper aux systèmes de détection traditionnels.

Les pirates utilisent aussi ces outils pour mener des attaques à grande échelle dans l’espoir de tromper des utilisateurs inattentifs. Dans certains cas, il s’agit d’offensives bien plus élaborées où les technologies **deepfakes** laissent augurer de gains substantiels.

EN RÉSUMÉ

Contexte & Priorités 2025

Les attaques se multiplient et deviennent plus **sophistiquées** grâce à l'IA (phishing ultra-réaliste, deepfakes).

Les aînés sont particulièrement **ciblés** (fraude « grand-parent », faux textos, appels se faisant passer pour la banque ou le gouvernement).

Tendances Majeures

Phishing / Smishing :

- Courriels ou textos imitant parfaitement des organismes officiels.

Deepfakes & Fraude vocale :

- Voix simulées d'un proche.

Ransomware :

- Vol et chiffrement de données personnelles, demande de rançon.

Arnaques financières :

- Faux investissements, offres trop belles pour être vraies.

Principales Inquiétudes

Perte financière, stress, isolement.

Vol d'identité (fraude de crédit, utilisation de données personnelles).

Forte **augmentation** des campagnes ciblées par texto, courriel, réseau social.

Conseils Clés

- **Activer la double authentification (2FA)** et choisir des **mots de passe robustes**.
- **Vérifier** les liens, pièces jointes, et ne jamais cliquer sur un message suspect.
- **Sauvegarder** régulièrement ses données et **mettre à jour** ses appareils.
- **Discuter** avec un proche ou un organisme officiel en cas de doute (Centre antifraude, police, banque).

Ressources & Signalement

- **Centre antifraude du Canada** :
  - Site et ligne d'appel pour signaler toute fraude.
- **Sûreté du Québec / Éducaloi** :
  - Capsules vidéo pour reconnaître et signaler les arnaques.
- **Centre canadien pour la cybersécurité** :
  - Webinaires, guides pratiques.
- **Banques** :
  - Guides et assistance pour sécuriser comptes et cartes (Desjardins, RBC, etc.).

Aperçu des nouveautés depuis les Fêtes 2024

Augmentation des fraudes liées aux textos (smishing)
Plusieurs organismes gouvernementaux et bancaires rapportent une hausse notable de tentatives de fraude par textos.

Exemple : campagne d'hameçonnage se faisant passer pour la « Pension de vieillesse » ou les « Services de santé ».

Référence : Centre antifraude du Canada(Mises à jour en janvier 2025).

Initiatives gouvernementales récentes

Sécurité publique Canada a diffusé en décembre 2024 un nouveau guide simplifié destiné aux aînés pour repérer rapidement les signaux d'alarme dans les courriels frauduleux.

Le Gouvernement du Québec (Ministère de la Sécurité publique) a lancé en début janvier 2025 une capsule vidéo sur la chaîne YouTube officielle pour aider les personnes âgées à identifier les arnaques téléphoniques.

Vidéo : « Arnaques téléphoniques : comment s'en protéger? » publiée le 5 janvier 2025.

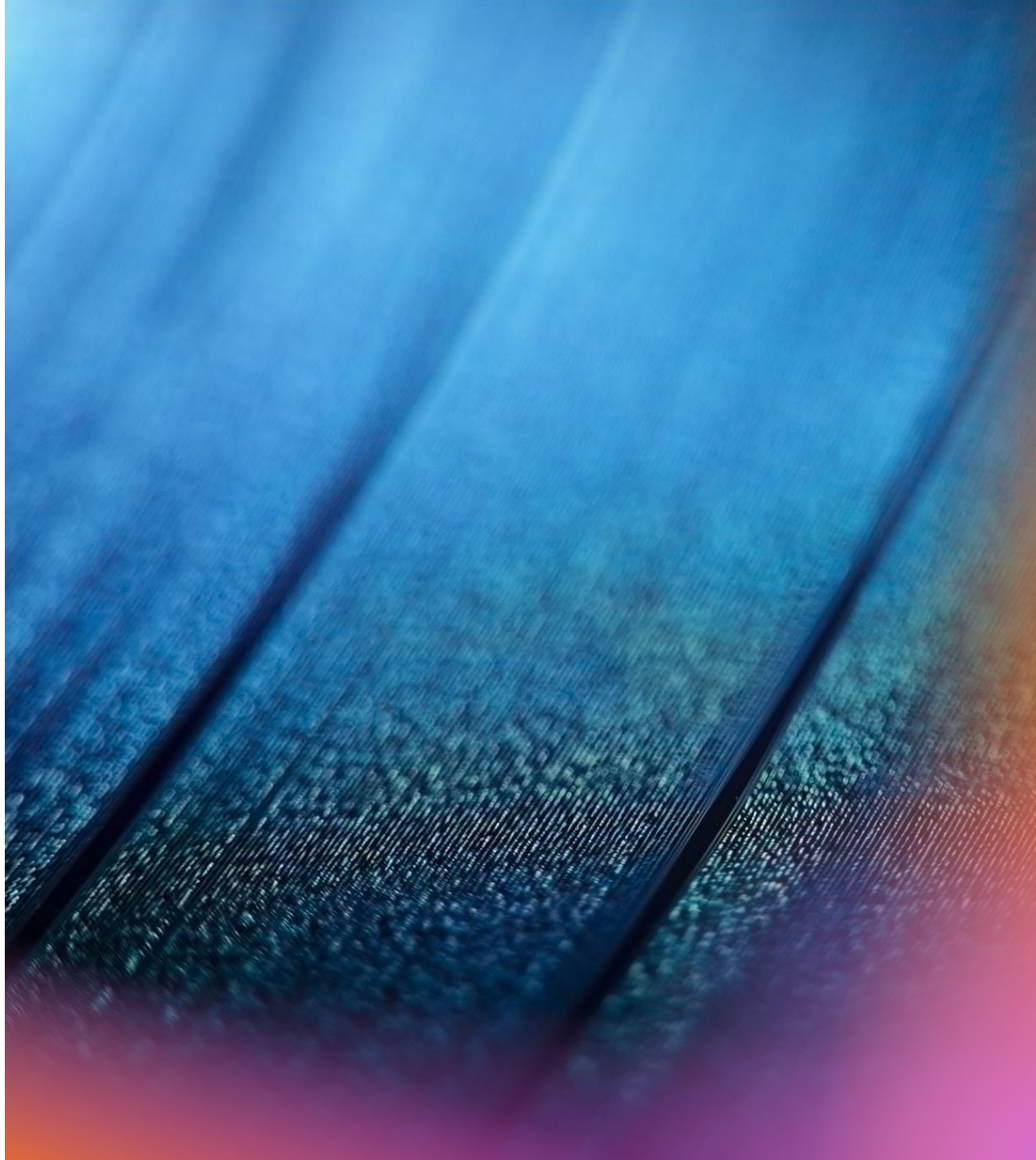
Suite…

Nouveaux signalements de fraudes “grand-parent”

- Des reportages dans les médias (La Presse, Le Devoir) soulignent un regain d’arnaques ciblant les aînés durant et après la période des Fêtes.
- Référence : Article du 7 janvier 2025 dans *Le Devoir* intitulé « Hausse des escroqueries visant les aînés : les faux appels en recrudescence ».

Contributions d’organismes privés et bancaires

- Plusieurs caisses et banques (ex. Desjardins, RBC) ont mis à jour leurs guides de cybersécurité pour aînés début janvier 2025, ajoutant des conseils sur la vérification à deux facteurs et les bonnes pratiques pour acheter en ligne.
  - Référence : Desjardins – Sécurité en ligne (Mise à jour de janvier 2025).



Ressources vidéo en français (publications récentes)

Chaîne YouTube de la Sûreté du Québec

- Nouvelle série de capsules début 2025 sur les fraudes en ligne visant les aînés.
- Titre recommandé : « Le phishing expliqué aux aînés » (publié le 6 janvier 2025).

Sécurité publique du Québec – Guide interactif

- Vidéo courte (moins de 5 minutes) : « Conseils de base pour une meilleure hygiène numérique ».
- Publiée le 3 janvier 2025, explique comment choisir des mots de passe sécurisés et reconnaître un lien suspect.

Éducaloi

- Nouvelle vidéo mise en ligne le 8 janvier 2025 : « Vos droits en ligne : comment signaler une arnaque? »
- Ressort les étapes légales pour dénoncer une fraude et propose des conseils de prévention.

Centre canadien pour la cybersécurité (CCC)

- Sur cyber.gc.ca : webinaire en rediffusion (datant de fin décembre 2024) sur l'importance de la double authentification (2FA) et de la protection des renseignements personnels.

Références et liens utiles (en français)

Centre antifraude du Canada : antifraudcentre-centreantifraude.ca
(Mises à jour régulières, statistiques et conseils en janvier 2025)

Sécurité publique Canada : securitepublique.gc.ca
(Guide simplifié pour aînés, déc. 2024)

Ministère de la Sécurité publique du Québec :
Chaîne YouTube officielle : Sûreté du Québec (nouvelles capsules janvier 2025)

Éducaloi : educaloi.qc.ca
(Capsule « Vos droits en ligne : comment signaler une arnaque? » – publiée 8 janvier 2025)

Centre canadien pour la cybersécurité : cyber.gc.ca
(Webinaires et ressources ciblées pour les aînés)

Banques et caisses (ex. Desjardins) :
Mise à jour des ressources sur la sécurité en ligne en janvier 2025 :
Desjardins – Sécurité en ligne

Mot de Conclusion

- En **2025**, la cybersécurité pour les aînés canadiens demande plus de **vigilance** que jamais :
  - Les **technologies d'IA** rendent les arnaques plus convaincantes.
  - Les **textos frauduleux** (smishing) et les **appels téléphoniques** usurpant l'identité d'un proche se banalisent.
  - **L'information et la prévention** restent les meilleures protections :
    - Formation continue, vérification de l'authenticité des messages, sauvegardes régulières, et partage de toute tentative de fraude avec les organismes compétents.

Recherches et mise en page par :
*Michel Cloutier**
CIVBDL
Pour la rencontre du 20250115
C'est ensemble qu'on avance

** Et avec l'aide de l'IA*