Cybersécurité
et les Aînés

"Protégeons la sécurité numérique de nos aînés… une vigilance perpétuelle en cybersécurité"

Synopsis :
Ce titre met l'accent sur la protection des aînés, la nécessité d'une sensibilisation continue et l'engagement à maintenir une vigilance constante en matière de cybersécurité.

Voici le tableau mis à jour des 12 pires cyberattaques ciblant les aînés au Canada en 2024 incluant les recommandations, pour s'en protéger :

Votre première réaction quand vous découvrez que vous êtes victimes d'une tentative ou d'une cyber-attaque avec pertes :

Réponse : Appeler la police de son quartier

Les fausses nouvelles (Fake News)

1. La propagation des fake news au Canada

La diffusion de fausses nouvelles est devenue une préoccupation majeure au Canada, affectant divers domaines tels que la santé publique, la politique, l'économie et la cohésion sociale.

- **Plateformes de diffusion** :

    - **Réseaux sociaux** : Facebook, Twitter, Instagram et TikTok sont les principaux vecteurs.
    - **Messageries privées** : WhatsApp, Telegram et autres applications de messagerie facilitent la propagation rapide d'informations non vérifiées.
    - **Sites web et blogs** : Certains sites diffusent intentionnellement de la désinformation pour influencer l'opinion publique ou générer du trafic.
- **Thèmes courants des fake news** :
    - **Santé** : Désinformation sur la COVID-19, les vaccins, les traitements alternatifs.
    - **Politique** : Fausses informations sur les élections, les politiques gouvernementales, les personnalités politiques.
    - **Économie** : Rumeurs sur les marchés financiers, les entreprises canadiennes, les opportunités d'investissement frauduleuses.
    - **Environnement** : Négation du changement climatique, fausses solutions écologiques.

2. Impacts et pertes associées

La diffusion des fake news a des conséquences significatives sur plusieurs plans :

2.1. Santé publique

- **Hésitation vaccinale** :
    - **Impact** : Réduction du taux de vaccination, mettant en danger la santé publique.
    - **Conséquence** : Recrudescence de maladies évitables, surcharge des systèmes de santé.
- **Adoption de traitements dangereux** :
    - **Impact** : Utilisation de remèdes non éprouvés ou dangereux.
    - **Conséquence** : Dommages à la santé, voire des décès.

2.2. Économie

- **Fraudes financières** :
    - **Impact** : Arnaques aux investissements basées sur de fausses informations.
    - **Conséquence** : Pertes financières pour les particuliers et les entreprises.
- **Atteinte à la réputation des entreprises** :
    - **Impact** : Diffusion de rumeurs néfastes.
    - **Conséquence** : Baisse de la confiance des investisseurs et des clients, chute des actions.

2.3. Cohésion sociale et politique

- **Polarisation de la société** :
  - **Impact** : Renforcement des divisions politiques et sociales.
  - **Conséquence** : Tensions accrues entre communautés, manifestations, violences.
- **Défiance envers les institutions** :
  - **Impact** : Perte de confiance dans le gouvernement, les médias traditionnels et les experts.
  - **Conséquence** : Difficulté à mettre en place des politiques publiques efficaces.

2.4. Sécurité nationale

- **Ingérence étrangère** :
  - **Impact** : Tentatives de pays étrangers pour influencer les élections et les opinions publiques.
  - **Conséquence** : Menace sur la souveraineté et l'intégrité démocratique du Canada.

3. Exemples concrets

- **Désinformation sur la COVID-19** :
  - Des fausses nouvelles affirmant que les vaccins contiennent des micropuces ont circulé, incitant certaines personnes à refuser la vaccination.
- **Scandales politiques fabriqués** :
  - Avant les élections, des informations non vérifiées sur des candidats ont été partagées massivement pour influencer le vote.
- **Arnaques aux subventions gouvernementales** :
  - Des escroqueries prétendant offrir des subventions en échange de renseignements personnels ont ciblé des milliers de Canadiens.

4. Mesures prises pour lutter contre les fake news

4.1. Initiatives gouvernementales

- **Lois et réglementations** :
  - **Projet de loi C-10** : Vise à réglementer les contenus en ligne et à responsabiliser les plateformes numériques.
  - **Groupe de travail sur la lutte contre la désinformation** : Coordonne les efforts pour identifier et contrer les fake news.
- **Campagnes de sensibilisation** :

    - **"Pensez avant de partager"** : Programme pour encourager les Canadiens à vérifier les sources avant de diffuser des informations.

4.2. Actions des plateformes en ligne

- **Modération de contenu** :
    - Suppression de contenus signalés comme faux ou trompeurs.
    - Signalement des informations douteuses avec des avertissements.
- **Collaboration avec des vérificateurs de faits** :
    - Partenariats avec des organisations indépendantes pour identifier les fake news.

4.3. Rôle des médias et de la société civile

- **Fact-checking** :
    - Médias traditionnels et organisations spécialisées publient des vérifications des faits pour corriger les fausses informations.
- **Éducation aux médias** :
    - Programmes éducatifs dans les écoles et les communautés pour développer la pensée critique.

5. Recommandations pour le public

- **Vérifier les sources** :
    - Consulter des médias reconnus et des sources officielles.
    - Être sceptique face aux informations sensationnelles ou non sourcées.
- **Ne pas partager sans vérifier** :
    - Éviter de propager des informations non confirmées.
    - Utiliser des outils de vérification en ligne.
- **Signaler les fausses nouvelles** :
    - Utiliser les fonctionnalités des plateformes pour signaler les contenus trompeurs.
    - Informer les autorités compétentes en cas de désinformation nuisible.

6. Conclusion

La lutte contre les fake news au Canada est cruciale pour préserver la santé publique, l'économie, la cohésion sociale et la démocratie. Les pertes associées, qu'elles soient financières, sanitaires ou sociales, sont significatives. Une approche collaborative impliquant le gouvernement, les plateformes numériques, les médias et les citoyens est essentielle pour contrer efficacement ce phénomène.

N°	Type de cyberattaque	Description	Conseils pour se protéger
1	**Fraude téléphonique « Oui, allô ? »**	Les fraudeurs appellent et incitent la victime à dire « Oui » pour enregistrer sa voix et l'utiliser à des fins frauduleuses, comme l'autorisation de transactions.	- Ne pas répondre directement par "Oui" à des questions d'inconnus au téléphone. - Demander l'identité de l'appelant avant de poursuivre la conversation. - Raccrocher si l'appel semble suspect.
2	**Fraude des grands-parents**	Les fraudeurs se font passer pour un petit-enfant en difficulté nécessitant de l'argent de toute urgence.	- Vérifier l'histoire en appelant un membre de la famille ou le petit-enfant directement. - Ne jamais envoyer d'argent sans confirmer la situation. - Être prudent avec les demandes urgentes d'argent.
3	**Hameçonnage (phishing)**	Envoi de courriels frauduleux pour obtenir des informations personnelles.	- Ne pas cliquer sur les liens ou pièces jointes d'expéditeurs inconnus. - Vérifier l'adresse courriel de l'expéditeur. - Utiliser des logiciels antivirus à jour. - Ne jamais fournir d'informations personnelles par courriel.
4	**Fraude par messages texte (smishing)**	Envoi de messages texte frauduleux incitant à cliquer sur un lien malveillant ou à partager des informations personnelles.	- Ne pas répondre aux messages texte d'inconnus. - Éviter de cliquer sur les liens dans les messages suspects. - Supprimer les messages douteux immédiatement.

5	**Arnaques téléphoniques classiques**	Appels prétendant être d'organismes officiels pour extorquer de l'argent.	- Ne pas fournir d'informations personnelles au téléphone. - Vérifier l'identité de l'appelant en rappelant l'organisme officiel. - S'inscrire sur la liste nationale de numéros exclus (LNNTE) pour réduire les appels de télémarketing.
6	**Logiciels malveillants (malware)**	Installation de programmes nuisibles pour voler des données ou endommager le système.	- Installer et mettre à jour régulièrement un logiciel antivirus. - Ne télécharger des logiciels que de sources fiables. - Éviter de cliquer sur des pop-ups ou des liens suspects.
7	**Fraudes de support technique**	Faux techniciens offrant de résoudre des problèmes inexistants contre rémunération.	- Ne pas accorder l'accès à distance à votre ordinateur à des inconnus. - Ne pas payer pour un service non sollicité. - Raccrocher si vous recevez un appel non demandé offrant du support technique.
8	**Usurpation d'identité**	Utilisation des informations personnelles pour commettre des fraudes.	- Protéger vos informations personnelles et documents sensibles. - Utiliser des mots de passe forts et uniques. - Surveiller régulièrement vos relevés bancaires et rapports de crédit.

9	**Escroqueries sentimentales**	Manipulation émotionnelle sur les réseaux sociaux pour obtenir de l'argent.	- Être prudent avec les personnes rencontrées en ligne. - Ne pas envoyer d'argent à quelqu'un que vous n'avez jamais rencontré en personne. - Parler à un ami ou un membre de la famille si vous avez des doutes.
10	**Arnaques de loterie ou de prix**	Annonces de gains fictifs exigeant des frais pour la réclamation.	- Se méfier des notifications de gains pour des concours auxquels vous n'avez pas participé. - Ne jamais payer pour recevoir un prix. - Ignorer et supprimer ces messages ou appels.
11	**Rançongiciels (ransomware)**	Blocage de l'accès aux fichiers personnels jusqu'au paiement d'une rançon.	- Sauvegarder régulièrement vos données sur un support externe. - Ne pas cliquer sur des liens ou pièces jointes suspectes. - Maintenir vos logiciels à jour avec les dernières mises à jour de sécurité.
12	**Fraudes aux investissements**	Offres d'investissements frauduleux promettant des rendements élevés.	- Consulter un conseiller financier de confiance avant d'investir. - Se méfier des offres trop belles pour être vraies. - Vérifier la légitimité de l'entreprise auprès des autorités financières.

1. Les fraudes en ligne ciblant les aînés

1. Les fraudes en ligne ciblant les aînés

Beaucoup d'aînés sont victimes de fraudes par courriel, SMS ou téléphone (comme les escroqueries liées aux fausses factures, aux remboursements d'impôts ou aux loteries). Expliquer comment repérer les signes d'une fraude et les précautions à prendre (ex. : ne jamais partager ses informations personnelles sans vérification).
Les aînés sont souvent des cibles privilégiées des fraudeurs en raison de leur confiance naturelle et de leur moindre familiarité avec les technologies numériques.
Voici quelques exemples de fraudes courantes :

- **Courriels de phishing** : Les escrocs envoient des courriels qui semblent provenir d'entreprises légitimes (banques, services publics, etc.) et demandent de cliquer sur un lien ou de fournir des informations personnelles.
- **Faux appels téléphoniques** : Certains fraudeurs se font passer pour des agents du gouvernement ou des compagnies de services pour demander des paiements immédiats ou des informations sensibles (comme le numéro d'assurance sociale).
- **Escroqueries liées à la santé ou aux impôts** : Avec l'augmentation des services en ligne, certains proposent de faux services de remboursement d'impôts ou de frais médicaux.

Conseils pour se protéger :

- Ne jamais cliquer sur un lien ou télécharger une pièce jointe provenant d'un courriel non sollicité.
- Toujours vérifier la légitimité d'un appel ou d'un message en contactant directement l'entreprise ou l'organisme via un numéro officiel.
- Ne jamais partager des informations personnelles ou bancaires par téléphone ou courriel.

2. Les mots de passe sécurisés et la gestion des comptes

1. Les mots de passe sécurisés et la gestion des comptes

Les mots de passe faibles ou réutilisés sont une porte d'entrée pour les cybercriminels.
Parler de l'importance d'avoir des mots de passe robustes et différents pour chaque compte, ainsi que de l'utilisation d'un gestionnaire de mots de passe, peut aider les aînés à se protéger efficacement en ligne.
La réutilisation des mots de passe sur plusieurs comptes est un des principaux vecteurs d'attaques.
Si un mot de passe est compromis, les cybercriminels peuvent accéder à plusieurs comptes, mettant en danger des informations sensibles comme les données bancaires ou de santé.

Quelques recommandations :

- **Utiliser des mots de passe forts** : Un mot de passe robuste doit comporter au moins 12 caractères, avec des lettres majuscules et minuscules, des chiffres et des symboles.
- **Changer régulièrement ses mots de passe** : Bien qu'il ne soit pas nécessaire de changer ses mots de passe trop fréquemment, il est important de le faire après avoir été informé d'une fuite de données.
- **Utiliser un gestionnaire de mots de passe** : Ces outils permettent de stocker en toute sécurité des mots de passe uniques pour chaque compte.
  Cela évite de devoir mémoriser plusieurs mots de passe complexes.

3. La protection de la vie privée sur les réseaux sociaux

1. La protection de la vie privée sur les réseaux sociaux

De nombreux aînés utilisent les réseaux sociaux pour rester en contact avec leurs proches.
Un sujet crucial pourrait être les risques liés à la sur-participation, comme le partage excessif d'informations personnelles, et comment configurer correctement les paramètres de confidentialité.
Avec l'usage accru des réseaux sociaux chez les aînés pour maintenir des liens avec la famille et les amis, il est essentiel de comprendre les risques liés à la sur-participation en ligne.
Le partage d'informations personnelles, de photos, ou d'autres détails peut être utilisé par des personnes malveillantes.

Risques courants :

- **Vol d'identité** : Les informations partagées publiquement peuvent être utilisées pour créer des faux profils ou pour d'autres activités frauduleuses.

- **Escroqueries** : Les arnaqueurs peuvent utiliser les informations personnelles pour établir des scénarios crédibles afin d'extorquer de l'argent ou des informations supplémentaires.

Mesures de protection :

- **Limiter les informations personnelles partagées** : Éviter de publier des détails comme son adresse, sa date de naissance complète ou des informations bancaires.
- **Configurer les paramètres de confidentialité** : Il est possible de restreindre la visibilité de ses publications à un cercle d'amis proches seulement.
- **Éviter les amis inconnus** : Accepter des demandes d'amis de personnes que l'on ne connaît pas personnellement peut augmenter les risques d'escroqueries ou d'intrusions.

Ces trois sujets offrent des solutions concrètes et immédiates que les participants peuvent appliquer à leur quotidien en ligne.
Ils sont à la fois actuels et spécifiques aux besoins des aînés.

Recherche de 6 sites effectuée

Pour créer un tutoriel sur la cybersécurité destiné aux participants, voici quelques ressources et outils que vous pouvez recommander :
(Documents trouvés au Canada et en français)

1. **Centre canadien pour la cybersécurité**

   https://www.cyber.gc.ca/fr

   Gouvernement du Canada | Government of Canada

   Synopsis : fait partie du Centre de la sécurité des télécommunications Canada.
   Il s'agit de la source unifiée de conseils, d'avis, de services et de soutien spécialisés en matière de cybersécurité pour les Canadiens.

2. **Ministère de la Cybersécurité et du Numérique**

   https://www.quebec.ca/gouvernement/ministere/cybersecurite-numerique

Synopsis : Le ministère de la Cybersécurité et du Numérique est chargé d'animer et de coordonner les actions de l'État dans les domaines de la cybersécurité et du numérique.

3. **Liste de vérification sur la cybersécurité à l'intention des aînés**

   https://www.rbcroyalbank.com/fr-ca/mes-finances-dabord/academie-financiere/cybersecurite/comprendre-la-cybersecurite/liste-de-verification-sur-la-cybersecurite-a-lintention-des-aines/

Synopsis : Avec la montée du cybercrime partout dans le monde, il importe plus que jamais de s'informer et d'informer ses proches sur les façons d'assurer sa cybersécurité.
La présente liste de vérification vise à vous renseigner sur les façons de vous protéger, vous et votre famille, et de protéger vos actifs numériques.

4.

   https://cyberseniors.org/fr/cyber-seniors-francais/

   Synopsis : Cyber-Seniors fournit le support et la formation technologique GRATUITS aux personnes âgées.

5. Octobre est le Mois de la sensibilisation à la cybersécurité au Canada

   https://www.pensezcybersecurite.gc.ca/fr/mois-de-la-sensibilisation-la-cybersecurite

Gouvernement du Canada | Government of Canada

Synopsis : La meilleure façon de sensibiliser le grand public à la cybersécurité est d'impliquer davantage d'organisations championnes dans la campagne – y compris la vôtre!
Chaque année, Pensez cybersécurité choisit un sujet ou un thème en lien avec la cybersécurité à promouvoir durant le Mois de la cybersécurité.
Vous pouvez choisir d'utiliser les ressources en lien direct avec le thème annuel ou les ressources non spécifiques disponibles.
Dans tous les cas, ces ressources peuvent faciliter votre participation à la campagne.
Montrez à votre public que vous vous souciez de leur cybersécurité en utilisant nos ressources du Mois de la cybersécurité

Ces ressources te permettront de créer un tutoriel structuré et accessible pour ton public. Elles fournissent des informations concrètes et adaptables à ton sujet sur la cybersécurité.

Voici quelques exemples de cyberattaques cet été au Canada qui ont affecté des aînés, certains ayant perdu de l'argent ou leur identité.

1. **Escroqueries et pertes d'identité chez les aînés**
   En 2022, les Canadiens ont signalé des pertes de **530 millions de dollars** dues à des fraudes et cybercrimes, avec un grand nombre de victimes âgées.
   Les arnaques les plus fréquentes incluaient des tentatives d'hameçonnage (phishing), des fraudes par extorsion et des arnaques utilisant des informations personnelles.
   Ces attaques ont visé des personnes âgées, souvent parce qu'elles sont perçues comme plus vulnérables et susceptibles de faire confiance plus facilement.
   Ces tendances se sont poursuivies en 2023(RCMP-GRC)(NCOA).

2. **Vols de données chez des entreprises canadiennes**
   Plusieurs incidents récents, comme les attaques contre **Beneva** et **Ernest & Young**, ont compromis les données de milliers de clients, y compris des aînés.
   Par exemple, chez Beneva, environ 30 000 personnes ont vu leurs informations personnelles exposées.
   Bien que des mesures aient été prises pour atténuer les impacts (comme offrir des services de protection contre le vol d'identité), les conséquences de ces cyberattaques

peuvent être graves pour les victimes
(Packetlabs) : Votre guide des plus grandes cyberattaques au Canada en 2023

3. **Perte d'argent due à des cyberattaques**
   Le rapport de l'**IBM** de 2023 indique que des entreprises canadiennes ont perdu des millions de dollars en raison des cyberattaques, et les particuliers, y compris les aînés, sont souvent victimes d'escroqueries sophistiquées visant à leur soutirer des fonds (Global News)(Global News).

Ces articles montrent que les aînés sont fréquemment pris pour cible par des cybercriminels en raison de leur vulnérabilité perçue, et que la protection contre ces menaces nécessite une vigilance accrue et des solutions de cybersécurité adaptées.

Recherche et mise en page par :
Michel Cloutier
CIVBDL
Rencontre du 20241204
"C'est ensemble qu'on avance"