Cybersécurité et les Aînés

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

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

Québec

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/

RBC Banque Royale

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 20240925
"C'est ensemble qu'on avance"