FORMATIO | RESSOURCE INFORMATIQUE BUREAUTIQUE

INITIER DES DISCUSSIONS SUR LES FRAUDES FINANCIÈRES

ROBERT ARSENEAULT

28 SEPTEMBRE, 2023

1. AUGMENTATION FRAUDES FINANCIÈRES

- Selon Statistiques Canada, une personne sur six (17 %, ou 5,45 millions de personnes de plus de 15 ans) a déclaré avoir été victime de fraude dans les cinq années précédentes. Ceci était plus élevé que le nombre de victimes de tous les crimes violents réunis au Canada.

- Existe bien plusieurs niveaux de fraudes et ses implications peuvent être catastrophiques pour certains. Lors de découverte, une panique majeure s'installe souvent.

- Quels sont les éléments qu'il faut faire immédiatement après, afin de limiter les dégâts et essayer d'identifier la faille pouvant offrir la possibilité de pénétration.

- Qu'est-ce qui aurait pu être fait avant, pour prévenir le désastre appréhendé. Identifier les questionnements d'après, en les ramenant avant pour assurer des protections améliorées.

2. ACTIONS RAPIDES SUGGÉRÉS APRÈS

- Après constat du piratage, selon des Pros entre autres il faut immédiatement aviser la banque et changer mots de passes, identifier les sites qui ont accès à votre carte de crédit, créer des alertes pour votre crédit, mise-en-place des niveaux d'authentification à 2 niveaux, faire le suivi en profondeur de vos comptes, isoler l'ordinateur, enlever le disque rigide, faire le back-up des documents importants, effacer l'ancien disque, réinstaller le système d'exploitation, réinstaller les logiciels de sécurité, accéder aux disques de back-up et refaire le back-up complet du système.

- Sources potentielles de grandes anxiétés et multiples efforts en période de panique à prévoir! Une connaissance qui a été récemment piraté, a attendu presque 8 semaines avant de ravoir accès aux montants complets du compte de banque.

3. NÉCESSITE GRANDE VIGILANCE AVANT

Les technologies ont évolué et les opportunités d'accès aussi, il faut aussi maintenant prévoir l'arrivée des outils d'Intelligence artificielle qui s'ajoutent aux outils existants. Malheureusement pas de solutions simplistes devant la multitude des méthodes essayées. Par contre l'on peut mettre en place des systèmes très solides.

- Vigilance: La fraude guette le citoyen dans toutes ses activités. Doit limiter au maximum la dissémination des renseignements personnels.

- Connaissance -- Rester informé des fraudes les plus courantes, apprendre nouvelles techniques de manipulation et scénarios inventés par les fraudeurs.

- Gros bon sens – Plusieurs bonnes techniques de préventions existent déjà, à continuer d'utiliser régulièrement.

4. QUELQUES OUTILS À UTILISER

Plusieurs outils sont discutés à votre Club et parmi ceux-ci:

- Utilisations mots de passes et méthodes de remplacements potentiels (Passkeys très intéressants). Suggère d'avoir un mot de passe différent, pour chaque application individuelle.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	Instantly	Instantly	Instantly
8	Instantly	Instantly	Instantly	Instantly	1 secs
9	Instantly	Instantly	4 secs	21 secs	1 mins
10	Instantly	Instantly	4 mins	22 mins	1 hours
11	Instantly	6 secs	3 hours	22 hours	4 days
12	Instantly	2 mins	7 days	2 months	8 months
13	Instantly	1 hours	12 months	10 years	47 years
14	Instantly	1 days	52 years	608 years	3k years
15	2 secs	4 weeks	2k years	37k years	232k years
16	15 secs	2 years	140k years	2m years	16m years
17	3 mins	56 years	7m years	144m years	1bn years
18	26 mins	1k years	378m years	8bn years	79bn years

Using ChatGPT Hardware To Brute Force your PassWord in 2023

5. QUELQUES OUTILS À UTILISER

- Utilisation de plusieurs adresses courriels d'identifications différentes, suggérant d'avoir une adresse spécifique pour les applications importantes (incluant financières), une autre possiblement pour social et une autre pour les courriels poubelles. Maximisant ainsi de planifier des distinctions et limitant grandement la possibilité d'accès partout. Pourquoi pas utiliser des chiffres au lieu des lettres dans les courriels poubelles, moins d'informations utiles en circulation.

- Utiliser les niveaux d'authentification à 2 niveaux.

- Il est souvent trop facile de récupérer les mots de passes, ré-évaluer le processus et prévoir courriel de récupération différent de celui habituellement en circulation.

- Et ne pas s'aventurer dans l'engouement des cryptos, les plateformes de placements ou des transferts d'argent, avec seulement une compréhension partielle du domaine. Des mises en garde de l'Autorité Des Marchés Financiers: https://lautorite.qc.ca/grand-public/salle-de-presse/mises-en-garde

6. FAIRE LE SUIVI EN CONTINU

- Malintentionnés et voleurs profitent de toutes les opportunités qui se présentent à eux. Trouvent même des nouvelles manières et visant toute faille pour accéder à leurs fins. Et l'hameçonnage et le harponnage semblent beaucoup plus habiles qu'avant, utilisant des logos et language crédible, etc.

- Subir une fraude financière, c'est inquiétant et pénible. Prendre aussi connaissance du site : **Fraude-alerte.ca**

- D'excellentes documentations et formations existent déjà au Club Informatique et chez Formatio. Des exemples très utiles incluent: **Atelier – Cours Sécurité des courriels**

- Faut régulièrement être vigilant, se garder à jour s'informant régulièrement sur leurs méthodes et vos expériences partageant mutuellement les informations entre membres. Pourquoi pas amener des exemples de méthodes de fraudes et discuter des outils pour mieux se protéger.

7. FAIRE ATTENTION EN CONTINU

- Différents concours, concours d'habilités, jeux gratuits, etc.
- Attention à tous courriels réclamant venir des organisations financières, aussi du genre courant tels Netflix, Amazon, etc .
- Demandes léger montant, avance relâcher grands montants.
- Demandes d'un prince voulant transférer une grande somme.
- Certains magasins en ligne avec des prix intéressants sur des produits non existants assurer d'avoir le « https:// ».
- Fausses offres de support techniques, accès à votre ordi, faux A/V
- Prudent de donner infos personnelles, même sites de confiance.
- Intérêts amoureux, personnes non rencontrées en personne.
- Sites d'investissements, faire recherches et consulter experts.
- Sites d'enchères frauduleux, aussi sites ventes pyramidales.
- Faux chèques, faux sites d'aides des sinistres, fausses loteries.
- Offres d'emplois, voyages, locations, héritage, chantages,
- Photos et diffusions diverses incluant jalons succès des enfants
- Maintenir les applications incluant A/V, VPN, etc. toujours à date.

DISCUSSIONS SUR FRAUDES FINANCÈRES

RÉFÉRENCES:

- https://www.lapresse.ca/affaires/2023-07-24/un-canadien-sur-six-a-ete-victime-de-fraude.php
- https://www.zdnet.com/article/how-to-keep-your-bank-details-and-finances-more-secure-online/?ftag=TRE-03-10aaa6b&bhid=%7B%24external_id%7D&mid=%7B%24MESSAGE_ID%7D&cid=%7B%24contact_id%7D&eh=%7B%24CF_emailHash%7D
- https://www.gobankingrates.com/money/finance/best-strategies-to-safeguard-against-online-fraud/
- https://www.msn.com/en-ca/money/technology/12-everyday-things-that-pose-huge-security-risks/ss-BB1bhGxh?ocid=windirect#image=1
- https://www.msn.com/en-ca/lifestyle/smart-living/how-to-avoid-the-no-1-text-message-scam-putting-your-money-at-risk/ar-AA1fZ2nG?ocid=hpmsn&cvid=5f9a9beb7286409fb05cfca394c951fa&ei=54
- https://www.lapresse.ca/contexte/2022-11-20/identite-numerique/une-solution-mille-interrogations.php
- https://www.msn.com/en-ca/money/other/what-are-the-pros-and-cons-of-passwordless-authentication/ar-AA1fut4U?ocid=hpmsn&cvid=0133ab8dbcec4866b6c0bc908101f6cf&ei=56
- https://www.zdnet.com/article/better-than-the-best-password-how-to-use-2fa-to-improve-your-security/?ftag=TRE-03-10aaa6b&bhid=23068586413125987424037827013043&mid=13138611&cid=716503125

DISCUSSIONS SUR FRAUDES FINANCÈRES

ATELIERS: