Octobre 2024 et la Cybersécurité

Le mois de la sensibilisation

Ressources - Mois de la sensibilisation à la cybersécurité

De : Pensez cybersécurité

Suivre:

Hyperlien : https://www.pensezcybersecurite.gc.ca/fr/ressources/ressources-mois-sensibilisation-cybersecurite

Sujet	Description	Exemple
1. Introduction à la cybersécurité	Présentation des bases de la cybersécurité et de son importance dans la vie quotidienne.	Expliquer pourquoi la cybersécurité est essentielle pour protéger les informations personnelles et éviter les fraudes en ligne.
2. Types de menaces en ligne	Description des différentes menaces telles que les virus, les logiciels malveillants, le phishing, etc.	Montrer des exemples de courriels de phishing et expliquer comment les identifier.
3. Sécurité des mots de passe	Importance de créer des mots de passe forts et uniques pour chaque compte en ligne.	Illustrer comment créer un mot de passe sécurisé en combinant lettres, chiffres et caractères spéciaux
4. Reconnaître les arnaques en ligne	Identifier les signes des arnaques courantes et savoir comment réagir.	Présenter des scénarios d'arnaques téléphoniques ou par courriel et discuter des actions à entreprendre.

5. Sécurité des appareils	Conseils pour sécuriser les ordinateurs, smartphones et tablettes contre les menaces.	Expliquer l'importance des mises à jour régulières et de l'installation d'un logiciel antivirus fiable.
6. Protection des données personnelles	Méthodes pour protéger les informations personnelles en ligne et éviter le vol de données.	Démontrer comment configurer les paramètres de confidentialité sur les réseaux sociaux
7. Utilisation sécurisée d'Internet et des réseaux sociaux	Meilleures pratiques pour naviguer en toute sécurité et utiliser les réseaux sociaux de manière protégée.	Conseiller de ne pas partager d'informations sensibles et de vérifier les paramètres de confidentialité sur Facebook ou Instagram.
8. Bonnes pratiques de navigation	Techniques pour naviguer sur Internet de manière sûre, incluant la reconnaissance des sites sécurisés et l'évitement des téléchargements risqués.	Montrer comment identifier un site web sécurisé (https://) et éviter de cliquer sur des liens suspects.
9. Que faire en cas d'incident de cybersécurité	Étapes à suivre en cas de suspicion ou de confirmation d'une violation de sécurité.	Expliquer comment signaler un compte piraté, contacter les institutions financières et changer les mots de passe immédiatement.
10. Ressources et support	Fournir des ressources supplémentaires et des moyens d'obtenir de l'aide en cas de besoin.	Partager des liens vers des sites gouvernementaux canadiens sur la cybersécurité, comme le Centre antifraude du Canada, et mentionner les lignes d'assistance téléphonique.

Hyperlien : https://antifraudcentre-centreantifraude.ca/index-fra.htm

Répercussions de la fraude depuis le début de l'année

En date du 30 june 2024

rapports traités :

21 604

(63 519 en 2023)

Victimes de fraude :

15 941

(41 988 en 2023)

En pertes financières liées aux fraudes :

284 M$

(569 M$ en 2023)

Fraudes récentes :

Octobre est le Mois de la sensibilisation à la cybersécurité - Apprenez-en davantage sur la fraude d'identité

Signalements d'extorsion par courriel

Synopsis : Il y a extorsion lorsqu'une personne obtient illégalement de l'argent, des biens ou des services d'une personne, d'une entité ou d'une institution par la coercition

Extorsion

Remarque

Si vous êtes en danger immédiat, veuillez appeler le 911. Si vous craignez pour votre sécurité ou celle d'autrui, contactez la police locale.

Alerte à la fraude!

2 octobre 2024 : Le Centre antifraude du Canada (CAFC) a reçu des signalements de lettres d'extorsion envoyées par courriel. Ces lettres contiennent votre nom complet, votre numéro de téléphone personnel, l'adresse de votre domicile et une saisie d'écran de votre adresse tirée d'un service de cartographie en ligne. Les auteurs de la lettre affirment que vous avez visité des sites Web explicites et vous menacent d'envoyer une vidéo à votre liste de contacts, à moins que vous ne les payiez en cryptomonnaies. Certaines lettres comportent aussi un code QR. C'est une fraude! N'envoyez pas d'argent sous pression et ne répondez pas aux messages de menace. Signalez cette lettre à votre service de police local et au CAFC.

Moyens utilisés :

Courriel et texto | Internet | Téléphone et télécopieur | Poste

Fraude ciblant :

Les entreprises | Les particuliers

Synopsis : Le Centre antifraude du Canada (CAFC) et l'Organisme canadien de réglementation des investissements (OCRI) mettent en garde les investisseurs contre la hausse des stratagèmes de récupération d'argent. La plupart de ces stratagèmes viennent s'ajouter à d'autres fraudes.

Dans ce type de stratagèmes, les fraudeurs affirment pouvoir rendre aux victimes les fonds qu'elles ont perdus. Ils tiennent une liste de victimes d'offres de placement

frauduleuses et communiquent avec elles par téléphone, courriel ou médias sociaux, ou encore utilisent le référencement naturel. Ils disent qu'il y a des frais pour leurs services et, dans certains cas, demandent aux victimes d'avoir accès à distance à leur ordinateur ou appareil. À la fin, celles-ci ne reçoivent pas de fonds et d'autres sommes pourraient leur être volées.

Certains fraudeurs mentionnent l'OCRI ou ses prédécesseurs, l'Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM) ou l'Association canadienne des courtiers de fonds mutuels (MFDA) pour se donner une apparence de légitimité.

Dernièrement, des fraudeurs se sont fait passer pour des employés d'organismes de réglementation des investissements. Sachez qu'un employé de l'OCRI ne demandera jamais de paiement à un investisseur. N'envoyez jamais d'argent et, en cas de doute, communiquez avec le Service des plaintes et des demandes de renseignements de l'OCRI pour vérifier la légitimité de la personne.

Les investisseurs doivent toujours vérifier de façon indépendante l'information qu'ils trouvent sur Internet. Ne vous fiez pas à des renseignements non sollicités et vérifiez toujours les antécédents, les compétences et les renseignements d'ordre disciplinaire des conseillers en investissements en consultant les rapports Info-conseiller de l'OCRI (rapports gratuits portant sur les conseillers actuellement autorisés auprès d'un courtier en placement) ou en faisant une recherche de renseignements sur leur inscription sur le site de l'ACVM.

Synopsis :

Enquêteur bancaire

Alerte à la fraude!

10 septembre 2024 : Méfiez-vous de fraudeurs qui prétendent travailler pour votre institution financière et qui vous demandent de leur fournir l'adresse URL (lien) d'unvirement électronique ou le code d'authentification multifacteur qui protège votrecompte. Il s'agit d'une fraude. Les institutions financières ne demandent jamais cetteinformation.

Moyens utilisés :

Téléphone et télécopieur

Fraude ciblant :

Les particuliers

Hyperlien : https://antifraudcentre-centreantifraude.ca/scams-fraudes/b-investigator-enqueteur-fra.htm

Bulletins spéciaux

- Mois de la sensibilisation à la cybersécurité 2024
  - Fraude d'identité
  - Protégez-vous en ligne

Fraude d'identité :
Synopsis : Les fraudeurs utilisent de plus en plus souvent des renseignements personnels volés pour présenter des demandes de prestations gouvernementales, ouvrir des comptes bancaires et des comptes de cartes de crédit, s'approprier des comptes de médias sociaux et de courriel, et même créer des comptes de téléphone cellulaire non autorisés. Il est essentiel pour les Canadiens de prendre les devants pour protéger leurs renseignements personnels et financiers et savoir comment réagir en cas de fraude d'identité.
Hyperlien : https://antifraudcentre-centreantifraude.ca/features-vedette/2024/10/identity-fraud-fraude-identite-fra.htm
Protégez-vous en ligne :
Synopsis : Le Mois de la sensibilisation à la cybersécurité vise à aider les Canadiens et les Canadiennes à assurer leur sécurité en ligne en leur donnant des moyens simples et efficaces de se protéger et de protéger leurs appareils. La cybercriminalité étant encore en hausse cette année, nous vous proposons une liste aide-mémoire pour vous aider à vous protéger en ligne.
Hyperlien : https://antifraudcentre-centreantifraude.ca/features-vedette/2024/10/protecting-yourself-protegez-vous-fra.htm

Références :
Si vous croyez avoir été la cible d'un acte de cybercriminalité ou de fraude, vous devez le signaler à votre service de police local et au Centre antifraude du Canada (CAFC) au moyen de son système de signalement en ligne

ou par téléphone au 1-888-495-8501. Il est recommandé de signaler une fraude, que vous en ayez été victime ou non, au CAFC.

Pour plus d'information sur les moyens de vous protéger contre les stratagèmes d'hameçonnage, visitez notre page sur le l'hameçonnage.

En ce Mois de sensibilisation à la cybersécurité, passez à l'action :

- **Suivez @cyber_securite et visitez son site Web : @GetCyberSafe**
- **Suivez-nous à @antifraudecan sur Twitter et Facebook et visitez notre site Web : @Canantifraud**
- **Utilisez les mots-clics #MoisCyber2024, #PensezCybersécurité, #Cybersécurité et #Cyber.**

- **Apprenez-en plus sur le nouveau système de signalement des incidents de cybercriminalité et de fraude développé par le CAFC en partenariat avec le Centre national de coordination en cybercriminalité**

Attention! Communiqué de presse!
Sujet : Des fraudeurs se font passer pour des employés du Centre antifraude du Canada

Synopsis : Le Centre antifraude du Canada (CAFC), la Police provinciale de l'Ontario (OPP) et la Gendarmerie royale du Canada (GRC) mettent en garde les Canadiens à propos de la menace croissante de fraudeurs qui se font passer pour des employés du CAFC et des membres de services de police. Parfois, les fraudeurs prétendent participer à une enquête menée par le CAFC en utilisant l'en-tête et le logo du CAFC. Il arrive également qu'ils falsifient les numéros de téléphone de services de police.
Hyperlien : https://antifraudcentre-centreantifraude.ca/news-nouvelles/2024/2024-07-02-fra.htm
Détails :

Les trois arnaques liées à l'usurpation d'identité les plus courantes sont les suivantes :

1. **Inspecteur de banque**

Le fraudeur prétend être un employé d'une institution bancaire, d'un fournisseur d'une carte de crédit reconnue ou, dans certains cas, d'entreprises comme Amazon. Il affirme que des transactions non autorisées ont été effectuées dans votre compte ou que votre compte a été compromis. Il arrive que le fraudeur exige que vous lui fournissiez les renseignements liés à votre carte de crédit et qu'il vous demande d'envoyer de l'argent qui servira à rembourser des frais ou qui sera utilisé comme appât pour aider à pincer le soi-disant employé fautif.

Afin de convaincre la victime de la légitimité de l'enquête, les escrocs envoient par courriel une lettre frauduleuse qui peut présenter le logo du CAFC, selon laquelle vous, la victime, devez coopérer avec le CAFC, qui fait enquête, pour l'aider à « attraper » le suspect. De fausses coordonnées (numéro de téléphone

et adresse courriel) sont fournies pour que vous communiquiez avec les fraudeurs.

2. **Soutien technique**

Le fraudeur prétend qu'un virus a infecté votre ordinateur. Il vous informe que votre appareil envoie des virus ou a été piraté et doit être réparé. Il demande l'accès à votre ordinateur et peut exécuter des programmes ou modifier des paramètres. Il affirme avoir détecté des activités frauduleuses dans votre ordinateur et qu'une enquête doit être effectuée. Les fraudeurs entrent en contact avec les victimes :

- **au moyen de fenêtres publicitaires sur des sites Web dans lesquels on vous demande d'appeler au numéro à l'écran sans tarder;**
- **au moyen d'appels non sollicités (le fraudeur peut prétendre travailler pour Microsoft ou une autre entreprise d'informatique connue).**

Les escrocs envoient par courriel une lettre frauduleuse qui peut présenter le logo du CAFC, selon laquelle vous, la victime, devez coopérer avec le CAFC, qui fait enquête, pour l'aider à « attraper » le suspect. De fausses coordonnées (numéro de téléphone et adresse courriel) sont fournies pour que vous communiquiez avec eux.

3. **Récupération d'argent**

Si vous avez déjà été victime d'une fraude, des fraudeurs pourraient vous cibler de nouveau en vous promettant de récupérer votre argent. La personne prétend travailler pour un organisme gouvernemental ou d'application de la loi et vous demande de l'aider dans une « opération d'infiltration » afin d'arrêter les fraudeurs qui ont volé votre argent.

Afin de vous convaincre de la légitimité de l'enquête ou du fait qu'ils ont détecté des activités frauduleuses dans votre ordinateur, les escrocs vous envoient par courriel une lettre frauduleuse qui peut présenter le logo du CAFC, selon laquelle vous devez coopérer avec le CAFC pour l'aider à « attraper » le suspect. De fausses coordonnées (numéro de téléphone et adresse courriel) sont fournies pour que vous communiquiez avec eux. Ils vous demanderont

ensuite de leur verser de l'argent pour les aider à mener leur enquête et vous promettront de vous rendre les fonds, ce qu'ils ne feront jamais.

Indices – Comment vous protéger

- **Le CAFC ou un service de police ne vous demandera jamais :**
  - **de transférer de l'argent ou de faire un paiement;**
  - **d'accéder à votre ordinateur à distance;**
  - **de lui fournir des renseignements personnels ou de lui faire un paiement, peu importe le mode.**
- **Les fraudeurs vous fourniront souvent les quatre à six premiers chiffres de votre carte de débit ou de crédit.**
  - **N'oubliez pas que la plupart des numéros de carte de débit ou de crédit d'une même institution financière commencent par les mêmes quatre à six chiffres.**
- **Ne présumez jamais que les numéros de téléphone qui apparaissent sur votre afficheur sont authentiques. Les fraudeurs utilisent la technique de « falsification des données de l'appelant » pour induire les victimes en erreur.**
- **Si vous recevez un appel d'un supposé employé de votre institution financière, dites-lui que vous le rappellerez.**
  - **Mettez fin à l'appel et composez le numéro inscrit au dos de votre carte de débit ou de crédit à partir d'un autre téléphone ou attendez une dizaine de minutes avant de faire l'appel.**
- **N'hésitez jamais à raccrocher le téléphone.**
- **Ne donnez jamais accès à votre ordinateur ou appareil à une personne que vous ne connaissez pas.**
- **Adressez-vous toujours à une entreprise locale de bonne réputation pour faire réparer votre ordinateur ou appareil.**
- **Ne payez jamais à l'avance pour obtenir un remboursement.**

Si vous croyez avoir été victime d'une de ces arnaques ou d'une fraude similaire, communiquez immédiatement avec votre institution bancaire, le service de police local et CAFC.

Faits en bref

- **Le CAFC est un service national qui fait la collecte de renseignements sur la fraude à l'échelle du pays et qui soutient les corps policiers dans leurs activités de prévention et de répression.**
- **Le CAFC est géré conjointement par la Gendarmerie royale du Canada, le Bureau de la concurrence et la Police provinciale de l'Ontario.**
- **Toute personne qui croit avoir été victime de fraude doit le signaler au service de police local ainsi qu'au CAFC au moyen de son système de signalement en ligne ou par téléphone au 1-888-495-8501. Si un incident s'est produit sans que vous tombiez dans le piège, signalez-le tout de même au CAFC.**

Liens utiles

- **Protégez-vous contre les fraudes**
- **Centre antifraude du Canada**
- **Gendarmerie royale du Canada**
- **Police provinciale de l'Ontario**

Coordonnées

Centre antifraude du Canada
705-499-4572
media@antifraudcentre.ca

Vidéos YouTube en français :
Titre : Sensibilisation à la cybersécurité : Introduction à la sécurité de l'information
Résumé : Chaque employé a une responsabilité en matière de cybersécurité ; la vigilance quotidienne est essentielle pour protéger l'organisation contre les menaces en constante évolution.

- **La sécurité de l'information concerne tous les employés, pas seulement le personnel technique.**
- **Les risques liés à la sécurité évoluent constamment.**
- **Chaque employé doit être conscient des risques.**
- **Tous les employés partagent une responsabilité en matière de sécurité.**
- **La vigilance quotidienne est cruciale.**
- **Tous les employés doivent être des maillons forts pour protéger l'organisation.**
- **La sensibilisation à la sécurité de l'information est essentielle.**

Hyperlien YouTube : https://youtu.be/4kJdnlcn9Y8?si=N53zP3hnKb2Xni9w
Titre: CANADA CA- QUEBEC MQ cybersécurité et informatique
Résumé :
Cette vidéo explore les ressources et la législation en cybersécurité au Québec et au Canada, mettant en lumière le programme québécois de primes aux bogues (jusqu'à 3000$) et les ressources du Centre canadien pour la cybersécurité, notamment les alertes de vulnérabilité et les bulletins de sécurité en français.
Le Québec possède une législation plus stricte que la France, exigeant des services en français.
Un centre gouvernemental de cyberdéfense (CGCD) offre des services au Québec
Le Québec a mis en place un programme de primes aux bogues allant jusqu'à 3000$ pour les vulnérabilités critiques.
Le Centre canadien pour la cybersécurité fournit des conseils, des alertes de vulnérabilité et des bulletins de sécurité en français.
Le Canada offre des ressources pour signaler les cyber incidents et fournit des bulletins de sécurité, notamment de Cisco, en français.

L'importance d'une approche systémique de la sécurité informatique est soulignée.
Des exemples de programmes de primes aux bogues dans d'autres pays (Suisse) sont mentionnés.

Hyperlien YouTube :
https://youtu.be/YiwtPMF0blY?si=ogHSsoLz4s8_E0dM

Recherche et mise en page par:
Michel Cloutier
CIVBDL
Rencontre du 20241009
"C'est ensemble qu'on avance"