éclaire
le phare numérique

CyberPeace Institute

Sensibilisation à la fraude en ligne pour les particuliers

La fraude en ligne regroupe diverses pratiques trompeuses visant à voler de l'argent, des informations personnelles ou l'accès à des comptes sensibles. Les particuliers sont souvent ciblés par des e-mails de *phishing*, des arnaques sur les réseaux sociaux, de fausses transactions financières et des usurpations d'identité. Adopter de bonnes pratiques de cybersécurité permet de se protéger contre ces menaces.

Problèmes courants liés à la fraude en ligne:

- Usurpation d'identité: Il s'agit d'une utilisation injustifiée des données personnelles d'un individu sans son accord. Les cybercriminels peuvent se servir de ces données pour nuire à la réputation de la victime en créant de faux profils ou en commettant des actes répréhensibles en son nom. De nos jours, l'un des exemples les plus connus est le *deepfake*. Cela fait référence à des contenus faux (photo, vidéo ou audio) rendus profondément crédibles par l'intelligence artificielle (AI).

éclaire
le phare numérique

CyberPeace Institute

- **Arnaques en ligne:**
  - Le *phishing*, ou hameçonnage en français, est une technique d'escroquerie utilisée par les fraudeurs, par laquelle ceux-ci tentent d'amener la victime à leur divulguer ses mots de passe ou d'autres données personnelles, en lui envoyant par exemple de faux e-mails pour la tromper.
  - Le *ransomware*, ou rançongiciel en français, est un logiciel malveillant ou un virus qui bloque l'accès d'un ordinateur ou ses fichiers et réclame à la victime le paiement d'une rançon pour le déverrouiller.
- **Fraude bancaire:** Il s'agit de toute activité illégale menée par des cybercriminels dans le but de soustraire de l'argent sur le compte de leur victime, comme voler les informations de paiement d'une carte de crédit ou vendre des produits inexistants.

Bonnes pratiques:

Reconnaître une activité suspecte:

- En cas de réception d'un e-mail inattendu demandant des informations financières, vérifiez son authenticité en contactant directement l'expéditeur.
- Méfiez-vous des demandes urgentes d'argent ou d'informations personnelles provenant de contacts inconnus.
- Vérifiez régulièrement vos relevés bancaires pour détecter d'éventuelles transactions non autorisées.
- Méfiez-vous des redirections des réseaux sociaux, lesquelles sont susceptibles de mener sur des faux sites internet proposés, notamment en vérifiant qu'il n'y a pas d'erreur d'orthographe dans l'URL, que le prix du produit n'est pas excessivement avantageux et comparez l'offre promotionnelle au site internet officiel du fournisseur pour vous assurer de sa véracité.
- Ne cliquez jamais sur des liens, ni ne téléchargez des pièces jointes provenant de sources inconnues.
- Utilisez des filtres anti-spam pour détecter et bloquer les tentatives de *phishing*.

Gestion des mots de passe:

- Choisissez des mots de passe forts d'au moins 16 caractères, avec un mélange de lettres, chiffres et symboles.
- Ne réutilisez jamais le même mot de passe sur plusieurs comptes.
- Utilisez un gestionnaire de mots de passe pour générer et stocker des mots de passe forts et complexes en toute sécurité.
- Activez l'authentification multi-facteurs (MFA) pour les comptes sensibles, comme ceux relatifs aux banques, e-mails et réseaux sociaux.

éclaire
le phare numérique

CyberPeace Institute

Bonnes pratiques:

Sauvegarde régulière des données:

- Sauvegardez vos les fichiers importants sur un disque externe.

Sécurité des e-mails et des messages:

- Ne cliquez jamais sur des liens, ni ne téléchargez des pièces jointes provenant de sources inconnues.
- Méfiez-vous des messages créant un sentiment d'urgence, comme « Votre compte sera fermé si vous n'agissez pas immédiatement!».

Mises à jour logicielles et antivirus:

- Maintenez à jour votre système d'exploitation, votre navigateur et vos applications, afin de bénéficier des derniers correctifs de sécurité.
- Installez et utilisez un antivirus réputé.

Protection des informations personnelles:

- Ne partagez pas d'informations sensibles (adresse, numéro de téléphone, données bancaires) sur les réseaux sociaux.
- Ajustez les paramètres de confidentialité pour limiter la visibilité de vos informations personnelles.
- Soyez vigilant lorsque des applications demandent un accès aux données personnelles.

Sécurité financière et transactions en ligne:

- Vérifiez la légitimité des sites avant d'effectuer un achat.
- Privilégiez les options de paiement sécurisées (« https:// » et icône de cadenas dans la barre d'adresse du navigateur).
- Utilisez toujours des cartes bancaires virtuelles ou des services comme PayPal pour réduire les risques d'exposition.

Sécurité physique et des appareils:

- Protégez votre téléphone et votre ordinateur avec des mots de passe robustes ou l'authentification biométrique.
- Activez les fonctionnalités d'effacement à distance en cas de perte ou de vol de l'appareil.
- Ne laissez pas d'appareils ou de documents sensibles sans surveillance dans des lieux publics.
- N'utilisez jamais de câbles USB ou chargeurs mis en libre service sur des lieux publics (aéroport, cybercafé, etc).
- Évitez de se connecter à un wifi public, sans vous être au préalable connecté à un VPN (un réseau privé virtuel).

Formation à la prévention de la fraude:

- Tenez-vous informé des dernières tactiques de fraude en ligne.
- Suivez des formations ou ateliers sur la cybersécurité.
- Encouragez vos proches à adopter des habitudes sécurisées sur Internet.

éclaire
le phare numérique

CyberPeace Institute

Exercice de détection de fraude:

Évaluez les scénarios suivants pour déterminer les risques de fraude:

- Un SMS indiquant que vous avez gagné à une loterie à laquelle vous n'avez jamais participé.
- Un e-mail de votre « banque » vous demandant de réinitialiser votre mot de passe via un lien suspect.
- Un profil sur un réseau social proposant des investissements à haut rendement sans risque.
- Un message d'un ami mentionnant une urgence nécessitant un virement immédiat.

Le scénario le plus risqué est l'e-mail de la « banque », car les attaques de *phishing* sont une source majeure de fraude financière.

Conseils pour protéger sa vie privée et éviter les arnaques:

- Ne partagez jamais vos mots de passe ou informations bancaires par SMS, e-mail ou téléphone.
- Utilisez des outils comme HaveIBeenPwned pour vérifier si vos identifiants ont été compromis lors d'une fuite de données.
- Évitez d'enregistrer vos informations de paiement sur les sites e-commerce, sauf si nécessaire.
- Activez les alertes bancaires pour être informé en cas de transactions suspectes.
- En cas de suspicion de fraude, signalez immédiatement l'incident à votre banque et aux autorités locales.

En adoptant ces bonnes pratiques, chacun peut réduire considérablement les risques liés à la fraude en ligne et mieux protéger sa sécurité numérique. Et pour aller plus loin et tester vos connaissances en matière de cybersécurité, réalisez les exercices interactifs proposés par Take9.