OUCH! Février 2024

SANS SECURITY AWARENESS

OUCH!

Votre bulletin mensuel sur la sensibilisation à la sécurité

# Le vol d'identité : prévenir, détecter et réagir

## Aperçu

À l'ère du numérique, vos informations personnelles sont plus précieuses que jamais. Malheureusement, cela en fait également une cible de choix pour les vols d'identité. Comprendre cette menace, la détecter et savoir comment se protéger sont des éléments essentiels pour préserver votre vie numérique en ligne.

## Qu'est-ce que l'usurpation d'identité ?

L'usurpation d'identité se produit lorsque quelqu'un obtient illégalement vos informations personnelles : votre nom, vos numéros d'identification tels que votre numéro de sécurité sociale ou de passeport, ou les détails de votre carte de crédit par exemple, dans le but de commettre une fraude ou d'autres délits. Une forme courante d'usurpation d'identité est l'usurpation d'identité financière, où quelqu'un utilise vos informations pour commettre une fraude financière. Par exemple, ils volent votre identité et obtiennent une carte de crédit, un prêt hypothécaire ou un prêt automobile à votre nom, et vous devez payer les factures. Il existe cependant d'autres types d'usurpation d'identité, par exemple l'usurpation d'identité médicale, où quelqu'un vole vos informations médicales et facture à votre nom une assurance médicale pour des actes médicaux que vous n'avez jamais reçus. Il y a aussi l'usurpation d'identité liée aux impôts, lorsqu'un criminel utilise votre numéro d'identification fiscale pour remplir une déclaration d'impôts en votre nom et demander un remboursement frauduleux. Ensuite, lorsque vous essayez de remplir une déclaration d'impôt, vous ne pouvez pas récupérer votre argent car il a déjà été remis à quelqu'un d'autre.

## Mesures préventives

Que pouvez-vous faire pour vous protéger ? Malheureusement, ce n'est pas aussi facile qu'il n'y paraît, car de nombreuses organisations possèdent déjà vos informations et c'est à elles de les protéger. Cependant, il existe quelques mesures clés que vous pouvez prendre.

- **Mots de passe forts** : L'un des moyens les plus efficaces de vous protéger est de sécuriser chacun de vos comptes avec un mot de passe unique et long et, si possible, d'activer l'authentification multifactorielle.
- **Mises à jour régulières des logiciels**: Veillez à ce que vos appareils soient mis à jour avec les derniers correctifs de sécurité et les dernières fonctionnalités en activant la mise à jour automatique sur tous vos appareils.
- **Cartes de crédit** : pour les achats en ligne, utilisez des cartes de crédit, jamais de cartes de débit, car les cartes de crédit vous protègent beaucoup mieux contre la fraude. Une autre idée consiste à utiliser une carte de crédit pour les achats en ligne et une autre pour les achats en personne. Certains services proposent des cartes de crédit virtuelles ou à usage unique pour chaque achat en ligne.
- **Gel de crédit :**Un gel de crédit bloque votre dossier de crédit, empêchant les fraudeurs d'ouvrir de nouveaux comptes à votre nom. Vous pouvez le faire gratuitement en contactant les principaux bureaux de crédit. Il se peut que cette option ne soit pas possible dans tous les pays.

## Détection de l'usurpation d'identité

La détection précoce est l'un des meilleurs moyens de se protéger. Plus tôt vous détecterez que votre identité est utilisée par quelqu'un d'autre, plus tôt vous pourrez agir. Voici quelques-uns des indices les plus courants d'une usurpation d'identité :

- **Des états financiers inhabituels :** Contrôlez régulièrement tous vos relevés bancaires et de cartes de crédit. Vous devez rechercher les frais ou les transferts d'argent que vous savez ne pas avoir effectués. Un bon moyen d'y parvenir est d'activer les notifications automatiques. Ainsi, chaque fois qu'un montant est débité de votre carte de crédit ou qu'une modification est apportée à votre compte d'épargne ou à votre compte courant, vous en êtes immédiatement informé.
- **Rapports de crédit irréguliers**: Examinez chaque année vos rapports de crédit pour y déceler toute activité suspecte. Cherchez des nouveaux prêts à votre nom que vous savez ne pas avoir contracté ou toute modification importante de votre cote de crédit.
- **Factures ou notifications suspectes**: Méfiez-vous si vous commencez à recevoir des factures pour des articles que vous savez n'avoir jamais achetés, ou si vous êtes contacté par des agences de paiement pour des factures impayées pour des articles ou des services que vous n'avez jamais achetés.
- **Dénégations inattendues**: Si l'on vous refuse inopinément votre remboursement d'impôt, un crédit ou une demande de prêt, cherchez à en connaître les raisons.

## Réagir et se remettre d'une usurpation d'identité

Si vous craignez que votre identité ait été compromise, agissez immédiatement.

- **Reportez immédiatement** : Signalez immédiatement tout incident que vous soupçonnez. Par exemple, si vous identifiez une activité frauduleuse sur votre compte bancaire ou votre carte de crédit, contactez votre banque. Déposez également une plainte auprès des forces de l'ordre locales. Cela peut s'avérer crucial pour prouver l'infraction et vous aider à recouvrer les coûts ou à déposer une demande d'indemnisation.
- **Alertes à la fraude et gels de crédit**: Placez une alerte à la fraude sur vos rapports de crédit et envisagez de geler votre crédit si vous ne l'avez pas encore fait. En outre, collaborez avec les agences d'évaluation du crédit pour supprimer les informations frauduleuses.
- **Documenter tout** : Lorsque vous appelez des organisations pour récupérer des fonds, veillez à conserver des enregistrements détaillés de vos communications et des mesures prises, en indiquant la personne à qui vous avez parlé, la date et l'heure, ainsi que le sujet de la discussion.
- **Changez de mots de passe** : Mettez à jour les mots de passe de tous vos comptes clés. Si vous n'avez pas de gestionnaire de mots de passe pour suivre tous vos nouveaux mots de passe, envisagez d'en acquérir un.

## Conclusion

En comprenant ce qu'est l'usurpation d'identité et en appliquant ces mesures, vous pouvez réduire considérablement le risque d'en être victime.

## Ressources

**Gestionnaires de mots de passe :** https://www.sans.org/newsletters/ouch/power-password-managers/
**Sécuriser vos comptes financiers :** https://www.sans.org/newsletters/ouch/securing-financial-accounts/
**Bloquer les crédits :** https://www.usa.gov/credit
**Signaler un vol d'identité :** https://www.identitytheft.org

**Traduit pour la communauté par : Juliette Busson**