



Conseils pratiques

Escroqueries en ligne : l'hameçonnage

Le « hameçonnage » ou « *phishing* » est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels du grand public en envoyant des millions de mails au hasard. Ces mails ont tout pour faire croire qu'ils proviennent d'une société ou d'un organisme officiel : ils semblent parfaitement authentiques jusqu'au logo de la société ou de l'organisme officiel. Ces messages mettent en garde contre une erreur présumée d'un compte bancaire, d'une nouvelle législation ou trouvent un autre prétexte pour soutirer des renseignements personnels de la victime, comme son numéro de sécurité sociale ou son numéro de compte bancaire, sa date de naissance, même ses mots de passe sur les sites Internet ou encore ses numéros de code de carte bancaire. Souvent, le message mail contient des liens qui ressemblent étrangement à ceux des vrais sites, à tel point que même les experts ont du mal à faire la différence.

Parades :

Ne donnez jamais de renseignements personnels en réponse à un mail. Les vraies sociétés, banques et les vrais organismes officiels ne demandent jamais d'informations personnelles par mail.

Les citoyens ne doivent pas répondre à ces mails. Ne cliquez jamais sur les liens contenus dans ces mails, quelle que soit leur authenticité apparente. Si vous souhaitez vérifier la légitimité de la société ou de l'organisme officiel, saisissez la bonne adresse dans la barre d'URL plutôt que de cliquer sur le lien. Le cas échéant, utilisez un moteur de recherche reconnu pour trouver la bonne adresse.

Vos recours si vous pensez avoir été victime d'un hameçonnage :

- Les consommateurs devraient vérifier périodiquement leur relevé bancaire pour voir s'il n'y a pas eu d'opération suspecte. Si vous avez été victime d'une fraude, vous pouvez obtenir immédiatement et gratuitement un relevé de compte.

La législation fédérale impose à chacune des agences d'évaluation du crédit, Equifax, Experian et TransUnion, de vous remettre, une fois par an, un exemplaire gratuit de votre historique de crédit.

Vous pouvez obtenir des exemplaires gratuits auprès des trois grandes agences d'évaluation du crédit en écrivant à l'adresse suivante : Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281, États-Unis. Précisez le nom de l'agence auprès de laquelle vous souhaitez obtenir cet historique ou remplissez le formulaire disponible sur le site : <http://www.consumer.ftc.gov/articles/0155-free-credit-reports>. Vous pouvez aussi aller sur le site : www.annualcreditreport.com ou appeler le : 1-877-322-8228.

- Transférez les mails frauduleux à : spam@uce.gov et à la société, la banque ou l'organisation imitée dans le mail. Vous pouvez aussi signaler ce hameçonnage par mail à l'adresse reportphishing@antiphishing.org. Le groupe de travail anti-hameçonnage, groupe des ISP (fournisseurs de service Internet), les entreprises de sécurité informatique et les organismes de répression utilisent ces rapports pour lutter contre l'hameçonnage.
- Si vous pensez avoir été hameçonné par un mail, vous pouvez déposer plainte sur le site de la FTC : www.ftc.gov/complaint.

Ressources complémentaires :

- Pour de plus amples informations sur la protection contre l'usurpation d'identité, consultez la page de la FTC sur l'usurpation d'identité : [Federal Trade Commission's Identity Theft resource page](http://www.ftc.gov/identitytheft).
- Si vous avez des questions, appelez le service d'aide aux consommateurs du bureau du Procureur général au 860-808-5420 ou bien envoyez un mail à : attorney.general@ct.gov.