Fiches pratiques

Le phishing (hameçonnage ou filoutage)

Le *phishing* (hameçonnage ou filoutage) est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but d'usurper l'identité d'une entreprise, d'un organisme financier ou d'une administration. Soyez vigilants sur les informations que vous communiquez !

Quel est le principe du *phishing* ?

Le principe du *phishing* consiste à récupérer des données personnelles sur internet. Le moyen utilisé est l'usurpation d'identité, adaptée au support numérique. L'escroquerie repose le plus fréquemment sur la contrefaçon d'un site internet (celui d'une banque ou d'un marchand en ligne). L'adresse URL du lien comprise dans le mèl est également « masquée ou maquillée » afin de paraître authentique.

Des mèls à connotation alarmiste (« Votre compte va expirer », « Vous venez d'effectuer un achat », etc.) ou d'autres alléguant d'un prétendu remboursement en faveur de l'internaute sont ensuite massivement adressés.
Ils semblent provenir d'une source de confiance (banque, CAF, opérateurs de téléphonie, impôts, sites de VAD, etc.) et invitent à se rendre sur une page de formulaire à celle de l'organisme évoqué sur laquelle seront demandées et récupérées des données personnelles, souvent à caractère financier (coordonnées bancaires).

Pendant toute la procédure, la victime croit avoir à faire à un site officiel d'un opérateur qu'elle connaît. Toutefois, les liens figurant sur la page internet du formulaire sont souvent inactifs.

Ces mèls peuvent également être accompagnés d'une pièce jointe généralement présentée comme une facture. Le message est rédigé de sorte à inciter l'internaute à l'ouvrir ce qui aura pour effet d'infecter la machine.

Comment s'en protéger ? (https://www.ssi.gouv.fr/)

- **Les mèls constituant des tentatives de *phishing* sont très généralement anonymes** (« Cher client », « Madame, Monsieur », etc.).

- **Les centres des impôts n'envoient jamais ce genre de courriel ni les banques et organismes sociaux (CAF, mutuelles, etc.)**. Ils ne passent jamais par un courrier électronique pour demander à leurs assujettis ou clients de saisir leurs informations personnelles.
- **Ne pas cliquer sur les liens contenus dans les courriers électroniques** : les liens affichés dans les courriers électroniques peuvent en réalité diriger les internautes vers des sites frauduleux.
- **Préférer se rendre directement sur le site de l'organisme en question en tapant soi-même l'adresse de celui-ci dans le navigateur.**
- **Être vigilant lorsqu'un courriel demande des actions urgentes.**
- **Utiliser le filtre contre le filoutage du navigateur internet** : la plupart des navigateurs (Google Chrome, Microsoft Internet Explorer, Mozilla Firefox, Safari) proposent une fonctionnalité d'avertissement contre le filoutage. Leurs principes peuvent être différents (liste noire, liste blanche, mot clé, etc.) et sans être parfaites, ces fonctions aident à maintenir la vigilance de l'utilisateur.
- **Utiliser un logiciel de filtre « anti-pourriel »** : la plupart du temps ces tentatives d'escroquerie se diffusent par le biais de courriers électroniques. Même si les logiciels de filtrage ne sont pas parfaits, ils permettent de réduire leur nombre.
- **Ne jamais répondre ou transférer ces courriels.**
- **En cas de doute ou de problème, prendre contact rapidement avec son agence bancaire ou l'organisme qui aurait envoyé ce courriel.**
- **D'une manière générale, être vigilant et faire preuve de bon sens** : ne pas croire que ce qui vient d'internet est forcément vrai.

Signalez l'abus d'utilisation d'informations personnelles aux autorités compétentes

Si vous pensez avoir été victime d'une escroquerie par *phishing*, signalez le immédiatement sur la plateforme «PHAROS» (plateforme d'harmonisation, d'analyse de recoupement et d'orientation des signalements).
Cette plateforme permet de signaler les sites internet dont le contenu est illicite, mais aussi transférer les messages reçus.

Votre signalement sera traité par un service de police judiciaire spécialisé dans ces questions : l'office central de lutte contre la criminalité et de la communication (OCLCTIC).

Si vous avez subi un préjudice pécuniaire, vous pouvez déposer une plainte sur ce site.

Rapprochez-vous également de votre organisme bancaire pour lui signaler un usage frauduleux de votre moyen de paiement.

Enfin, vous pouvez signaler les tentatives de *phishing* sur le site phishing, édité par l'association *phishing* Initiative. Il permet d'alimenter les principaux navigateurs afin de bloquer l'accès à ces sites.

CONSEILS

- Méfiez-vous des formulaires demandant des informations bancaires, il est en effet rare qu'une banque vous demande des renseignements aussi importants par un simple courrier électronique. Dans le doute contactez directement votre agence par téléphone.
- Assurez-vous, lorsque vous saisissez des informations sensibles, que le navigateur est en mode sécurisé, que l'adresse dans la barre du navigateur commence par https et qu'un cadenas est bien affiché.

Textes de référence

Code pénal - article 313.3 (tentative d'escroquerie) et article 226-4-1 (usurpation d'identité)

Liens utiles

- Association *Phishing* Initiative
- La Commission nationale de l'informatique et des libertés (CNIL)
- Portail officiel de signalement des contenus illicites de l'internet - PHAROS
- La sécurité informatique

Les éléments ci-dessus sont donnés à titre d'information. Ils ne sont pas forcément exhaustifs et ne sauraient se substituer aux textes officiels.

Pour tout renseignement complémentaire, reportez-vous aux textes applicables ou rapprochez-vous d'une direction départementale de la protection des populations (DDPP) ou direction départementale de la cohésion sociale et de la protection des populations (DDCSPP).

Crédit photo : ©Fotolia