Se protéger contre le « phishing »

Qu’est ce que le phishing ?

Le phishing, également connu sous le nom d’ « hameçonnage » ou de « filoutage », est une forme d’escroquerie sur internet utilisée par des pirates informatiques. En pratique, ils vous envoient un mail :

- Soit vous demandant de « *mettre à jour votre dossier*», de « *communiquer vos informations suite à un incident technique* » ou même de « *consulter votre messagerie* ».
- Soit à connotation alarmiste ou prétendant que vous avez gagné une somme d’argent ou un objet.

Pour cela vous serez invités à cliquer sur un lien contenu dans le mail.

Leur objectif est de récupérer vos renseignements personnels, et notamment vos coordonnées bancaires (identifiants, mot de passe, numéros de votre carte bancaire), afin de les exploiter ou de les revendre à d’autres escrocs.

/ !\ Il faut faire très attention, car ils se « déguisent » en un organisme, une institution ou une société

que vous connaissez (la CAF, votre banque, les impôts, les opérateurs téléphoniques) en utilisant leur nom, leur logo, leur slogan. Ainsi, vous avez l’impression que c’est réellement votre banque qui vous écrit.

Un simple clic vous amène sur un « faux » site étant la réplique exacte des sites des organismes en cause. Une fois arrivés sur le faux site (bancaire par exemple), vous entrez vos identifiants et mot de passe en pensant être sur le véritable site de votre banque. De cette manière, les escrocs les récupèrent,

Comment savoir si le mail reçu est frauduleux ?

Si les premiers mails frauduleux étaient truffés de fautes d’orthographe ou de grammaire, désormais les pirates informatiques ont revu leurs copies. La plupart des messages sont désormais rédigés dans un français très correct, parfois sans aucune faute.

Pensez alors à regarder l'adresse mail de l'expéditeur. Celle-ci doit apparaître en entier.

Quels sont les risques ?

Le Phishing peut se révéler très dangereux. Les conséquences de ce piège ne sont pas anodines. En effet, cela va de l'usurpation d'identité au piratage des comptes bancaires.

Comment s'en prémunir ?

- Ne jamais répondre à ces messages, ni les transférer.
- Ne jamais cliquer sur les liens indiqués
- Ne jamais ouvrir les pièces jointes
- Si possible, activer la protection anti-phishing que chaque navigateur possède. Ou installer un logiciel de filtre contre le filoutage.

A savoir : aucun organisme officiel (banque, CAF, Trésor public,…) ne vous demandera jamais d'informations personnelles (exemple : mot de passe, copie de carte d'identité,…). Un tel mail devra donc vous alerter.

Les bons réflexes :

- Signalez les escroqueries auprès du site internet-signalement.gouv.fr ou sur signal-spam. Il est même possible d'installer un module de signalement sur votre navigateur (https://www.signal-spam.fr/).
- Vous y trouverez des conseils et serez guidés pour identifier la nature de l'attaque dont vous êtes victime : https://www.cybermalveillance.gouv.fr/blog

Dans la pratique comment faire ?

Exemple : vous recevez un mail de la CAF vous indiquant que vous avez reçu un message, consultable sur le site internet de la CAF. Ne cliquez pas sur le lien pour vous rendre sur le prétendu site de la Caf. Ouvrez une nouvelle page dans votre navigateur (Google, Yahoo !, Qwant, Duckduckgo…) et allez sur le site de la CAF. Vous serez alors assurés de ne pas avoir été aiguillés vers un mauvais site, etpourrez vérifier en toute sécurité si vous avez effectivement reçu un message sur ce site.