la médiation
des communications
électroniques

Fiche pratique

Se protéger contre le phishing

Le phishing (ou hameçonnage) est une technique consistant pour le fraudeur à faire croire à la victime qu'elle s'adresse à un tiers de confiance, afin de lui dérober des informations confidentielles (mot de passe, numéro de carte de crédit…) pour détourner des fonds. L'escroquerie repose le plus fréquemment sur la contrefaçon d'un site internet. Par principe, les centres des impôts, les organismes sociaux (CAF, mutuelles, etc..), les banques ou les opérateurs ne demandent jamais, par courriel, de renseigner des données personnelles.

Cependant, les attaques par phishing font de plus en plus de victimes. Il convient d'ailleurs de souligner que les e-mails piégés adressés par des tiers se faisant passer pour votre banque ou votre opérateur afin de détourner des informations personnelles sont de plus en plus trompeurs (le message est souvent personnalisé et sans faute d'orthographe), ce qui nécessite d'être vigilant.

Comment identifier les tentatives de phishing ?

- Vous recevez un courriel alarmiste ou alléguant un prétendu remboursement en votre faveur qui semble provenir d'une source de confiance (banque, impôts, etc..). Vous êtes invité à vous rendre sur une page de formulaire afin de fournir des données personnelles.
- Vous recevez un courriel dans lequel il vous est demandé de « mettre à jour » ou de « confirmer suite à un incident technique » vos données, notamment bancaires.
- Vous recevez un mail de votre opérateur vous précisant que votre banque a refusé le dernier prélèvement en vous enjoignant de régler au plus vite votre facture.

Bon à savoir : Il peut être opportun d'essayer d'ouvrir d'autres liens hypertextes comme, par exemple, ceux situés en bas de page. Ces liens, étant le plus souvent inactifs, vous mèneront à un message d'erreur ce qui peut confirmer une tentative de phishing.

Le mode opératoire et les conséquences du phishing

Vous recevez un mail, un SMS d'une personne mal intentionnée qui se fait passer pour votre opérateur. En cliquant sur le lien présent dans le message frauduleux, vous êtes automatiquement renvoyé sur une page internet contrefaite, portant le logo de l'opérateur. Confiant, vous communiquez spontanément les informations qui vous sont réclamées, notamment l'identifiant, le mot de passe et/ou le numéro de carte bancaire.

Avec ces informations, le fraudeur peut agir de différentes façons :

- Retirer une nouvelle carte SIM dans une borne. En possession de la carte SIM, le fraudeur peut alors effectuer des communications depuis votre ligne ou contourner le principal dispositif de sécurité « 3D Secure ». Il récupère ainsi le code de sécurité envoyé par votre banque par SMS, pour effectuer une transaction financière depuis un site Internet. Il s'agit d'une « arnaque à la carte SIM »

- Récupérer le contrôle de votre adresse mail et envoyer à vos contacts un message de détresse pour l'achat de coupons PCS Mastercard ou Transcash.
- Commander un téléphone ou souscrire sur Internet un abonnement à votre nom avec vos identifiants.

Quels sont les bons réflexes pour se protéger du phishing ?

- Prendre en compte les conseils qui figurent sur le site de votre opérateur,
- Vérifier toujours l'identité de votre interlocuteur,
- S'assurer que l'adresse du site (son URL) est bien l'adresse habituelle de l'interlocuteur ou l'organisme concerné,
- Privilégier la saisie d'informations personnelles (coordonnées bancaires, identifiants, ..) sur des sites internet sécurisés. Attention, le cadenas qui apparaît dans le navigateur et l'adresse du site qui commence par Https au lieu de http, ne garantissent pas que le site n'est pas un faux,
- Adopter la règle d'or de ne jamais communiquer vos informations personnelles (code secret, coordonnées bancaires..) à qui que ce soit,
- Changer régulièrement de mots de passe qui doivent être suffisamment complexes,
- S'assurer que votre anti-virus est mis à jour régulièrement,
- Ne pas cliquer sur les liens contenus dans les courriers électroniques,
- Utiliser les fonctionnalités de protection contre le hameçonnage et les logiciels malveillants proposées par les navigateurs internet,
- Installer un logiciel de filtre anti-spam,
- Rester vigilant lorsqu'un courriel demande des actions urgentes,
- En cas de doute, prendre contact immédiatement avec votre agence bancaire ou votre opérateur.

Utiliser les plateformes de signalement

Les tentatives d'escroquerie par phishing peuvent être signalées sur la plateforme PHAROS (www.internet-signalement.gouv.fr), portail officiel de signalement des contenus illicites de l'Internet ou sur le site www.phishing-initiative.com
Il est possible aussi de s'inscrire gratuitement sur le site www.signal-spam.fr et de télécharger une extension pour le logiciel de messagerie ou le navigateur.

Pour en savoir plus

Site de la CNIL (Commission Nationale de l'Informatique et des Libertés) : https://www.cnil.fr
Site de la DGCCRF : fiche pratique sur le phishing https://www.economie.gouv.fr
Site d'information et d'assistance du gouvernement sur la cybermalveillance https://www.cybermalveillance.gouv.fr (vidéos pédagogiques disponibles pour alerter les particuliers, notamment sur les risques de phishing).