Association Loisirs et culture

Vous avez dit Phishing !

Toutes les astuces pour éviter de tomber dans le panneau.

Jean Marie Herbaux

Table des matières

Le phishing ou hameçonnage en français, est l'un des plus grands fléaux d'Internet. Des individus envoient des e-mails en tentant de se faire passer pour quelqu'un d'autre pour vous inciter à cliquer sur un lien. Ils parviennent ainsi à voler vos identifiants en vous faisant croire que vous vous connectez sur un site de confiance, mais ce n'est qu'une copie. Dès l'instant où vous entrez votre mot de passe, ils ont accès à votre compte.

Cette menace n'est pas nouvelle, mais elle prend de l'ampleur. En 2020, le nombre de personnes en télétravail ou effectuant des transactions sur Internet a largement augmenté, ce qui multiplie les opportunités pour les pirates informatiques. Des attaques plus sophistiquées reposent pour beaucoup sur l'ingénierie sociale, où les pirates tentent de duper leurs victimes.

Dans tous les cas la meilleure parade est d'abord de savoir repérer ce genre d'arnaque.

1. Qu'est-ce que le phishing ?

Le hameçonnage (phishing en anglais) désigne un type d'attaque où un pirate informatique part à la pèche aux informations. Le vocabulaire utilisé dans le domaine est généralement celui de la pèche, car les pirates essaient de leurrer leurs victimes avec un *appât*. Le terme phishing est un jeu de mot sur phishing en anglais, qui signifie « *pèche* ».

2. L'attaque est de deux sortes.

a. La première sorte :

La première est un message, le plus souvent un e-mail, envoyé eux victimes, Il contient généralement une alerte au sujet d'un problème avec le compte, qui demande de cliquer sur un lien pour passer en revue ou rectifier la situation. Ou bien il s'agit d'annoncer que vous avez gagné quelque chose. On estime que 135 millions d'e-mails de phishing seraient envoyés chaque jour.

b. La seconde sorte :

La seconde est une simple page web qui demande à l'utilisateur de se connecter.
Toutefois, il s'agit d'une *copie* d'un site légitime, par exemple une fausse page d'identification pour Facebook. Si l'utilisateur entre son mot de passe, celui-ci est immédiatement communiqué au pirate ayant lancé l'attaque.

c. Le cas le plus courant

Le cas le plus courant de phishing est *l'e-mail* de masse. Les pirates peuvent par exemple créer une fausse page d'identification pour PayPal puis envoyer un faux message mentionnant des transactions inhabituelles, aux contacts d'une base de données en contenant des milliers, voire des millions d'adresses e-mail. Tous n'utiliseront pas PayPal et une majorité ne cliquera pas sur le lien soit parce qu'ils ont identifié la supercherie, soit parce qu'ils passent par un marque-page (*Favoris*) de leur navigateur. Cependant en l'envoyant à un très grand nombre d'adresses cette attaque est très rentable. Il suffit qu'un très faible pourcentage de personnes tombe dans le panneau pour que les pirates accèdent à de nombreux comptes.

3. Comment se protéger ?

a. Méfiez-vous de tout message.

- La première protection passe par l'humain.

Il faut toujours se méfier de tout message reçu. Si un e-mail ou un SMS vous demande de cliquer pour accéder à votre compte, ne le faites pas à moins d'être absolument certain que le message est légitime.

- Passez toujours par les favoris du navigateur

Saisissez l'adresse du site directement dans la barre d'adresse.
S'il s'agit d'un problème avec votre compte. vous devriez pouvoir y accéder une fois identifié sans avoir à cliquer sur le lien.

- N'ouvrez jamais les pièces jointes

à moins de savoir exactement ce que c'est. Les pièces jointes sont souvent accompagnées d'un malware. Elles se font passer pour une facture, un dossier compressé ou tout autre fichier à priori inoffensif.

- Ne vous fiez pas à l'adresse de l'expéditeur, qui est très simple à falsifier !

Aucun agent de Microsoft ne vous appellera pour un problème sur votre ordinateur.
Le service client de la marque est incapable de savoir si votre machine présente un dysfonctionnement. Ces appels sont toujours une arnaque !
De la même manière, ne donnez jamais d'informations personnelles à un conseiller qui vous appelle, même s'il semble être en lien avec l'un de vos centres d'intérêt ou un achat envisagé ou effectué récemment.

b. Attention à l'orthographe :

Les auteurs des e-mails de phishing ne s'appliquent pas toujours à créer un message « crédible ». Dans certains cas le courriel est quasiment impossible à distinguer d'un vrai mais très souvent la qualité laisse à désirer. *L'orthographe* et la *grammaire* sont souvent médiocres. Les auteurs ne maîtrisent pas la langue française et ont notamment recours aux traducteurs automatiques.

c. Attention aux fausses adresses web :

Pensez également que les liens figurant dans les e-mails ne sont pas toujours ceux qui sont affichés. Tout comme il est possible de transformer les mots « *cliquez ici* » en un lien qui renvoie vers n'importe quelle adresse web. Il est également possible de mettre le texte d'une adresse ainsi qu'un lien qui renvoie vers un site complètement différent quand on clique dessus.
Pour savoir où renvoie un lien il suffit de passer sa souris dessus, sans cliquer, et de regarder dans la barre d'état de la fenêtre en bas à gauche.

d. Utilisez un gestionnaire de mots de passe

Les gestionnaires de mots de passe constituent l'une des rares solutions qui augmentent votre sécurité tout en vous simplifiant la vie. Notre préféré est LastPass. Il en existe d'autres, mais évitez celui intégré à votre navigateur qui est bien moins sûr. Chaque fois que vous vous inscrivez sur un site ou que vous vous identifiez pour la première fois, il vous propose de mémoriser votre *identifiant* et votre *mot de passe*. Ainsi à chaque nouvelle connexion sur le site, le gestionnaire remplira automatiquement les champs.
L'avantage est que ce programme ne sera pas trompé par un faux site visuellement identique au vrai. Si l'adresse ne correspond pas, il n'affichera pas le mot de passe. Si vous cliquez un lien dans un message de phishing, vous ne pourrez pas vous identifier automatiquement. Ceci bloque effectivement toute tentative de de phishing.

e. Prenez garde aux faux e-mails des banques !

Selon le dernier rapport de la société de sécurité informatique Bitdefender, la pandémie mondiale de coronavirus a provoqué un changement important dans le paysage des menaces. Les cybercriminels optent et perfectionnent leurs attaques. Au premier semestre 2020, Ils ont exploité les problèmes liés à la crise pour semer la peur et la désinformation. Résultat une augmentation des escroqueries, de la récupération d'identifiants et des logiciels malveillants sur les ordinateurs, les mobiles.
En mai et juin, environ 60 % de tous les e-mails reçus étaient frauduleux Qu'il S'agisse d'une escroquerie exploitant le *coronavirus*, d'une *collecte de fonds*, d'une *offre exceptionnelle à ne pas rater*. Les escrocs ont utilisé toutes les astuces du commerce pour tromper les victimes en leur soutirant des données sensibles ou en installant des logiciels malveillants. ***Parmi elles il y a les tentatives d'escroqueries via les faux e-mails bancaires.***