Le phishing

Le but d'une attaque de phishing (ou hameçonnage en français), est de dérober les identifiants de connexion à des utilisateurs de comptes d'e-banking par exemple ou de différents sites marchands. Les hackers exploitent alors la crédibilité de leurs victimes en se présentant à elles sous une fausse identité.

Pour vous protéger contre le phishing...

- ne cliquez jamais sur un lien reçu par email, SMS ou Messenger, ou que vous auriez obtenu après avoir scanné un code QR, pour vous connecter à un service de banque en ligne.
- ne remplissez jamais de formulaires envoyés par courriel et dans lesquels on vous demande d'indiquer vos identifiants de connexion.
- soyez méfiants à l'égard des pièces jointes de vos courriels et SMS.
- ne révélez au téléphone aucune information confidentielle comme vos mots de passe par exemple.
- tapez toujours manuellement l'adresse de la page d'accueil du site du fournisseur de services ou de la banque dans la barre d'adresse de votre navigateur.
- lorsque la page d'accueil s'affiche, vérifiez la connexion SSL (https:// et symbole du cadenas) et contrôlez l'adresse Internet dans la barre d'adresse du navigateur pour vous assurer que vous êtes bien sur le bon site.
- en cas de doute, contactez toujours directement votre institut financier.

(https://www.ebas.ch/fr/test-sur-le-hameconnage/)

Voici comment se déroule généralement une attaque par phishing

1. Prise de contact

Les hameçonneurs envoient une série de faux courriels en se faisant passer pour des collaborateurs de prestataires de services en ligne ou d'instituts financiers. Le contenu du message peut faire référence par exemple au fait que les informations concernant le compte ou les données d'accès (par ex. identifiant et mot de passe) sont obsolètes, invitant les destinataires à cliquer sur un lien pour leur permettre de les actualiser.

2. Interception des données personnelles

Or le lien en question ne conduit pas sur le site officiel du fournisseur de services mais sur un site piraté, ressemblant comme deux gouttes d'eau à l'original. Tous les identifiants et mots de passe tapés sur la page de connexion contrefaite finissent directement entre les mains des malfaiteurs.

3. Enrichissement
Grâce aux informations volées, les criminels peuvent par exemple effectuer des virements sur leurs propres comptes, faire des achats en ligne ou faire des offres sur les sites de ventes aux enchères, au nom et aux frais de la victime.

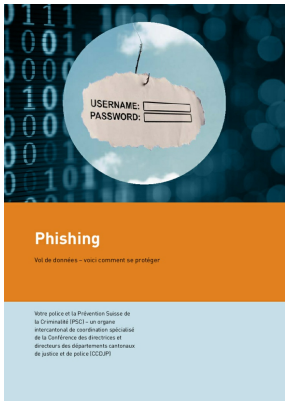
Si vous recevez des courriels d'hameçonnage, c'est que les escrocs connaissent votre adresse de messagerie électronique. Pour diminuer ce risque et plus généralement pour réduire la quantité de spam dans votre boîte de réception, il convient de suivre quelques règles simples que nous avons regroupées dans notre article consacré au spam (https://www.ebas.ch/fr/se-proteger-contre-le-spam/).

(https://www.antiphishing.ch/fr/)

Le phishing désigne le vol d'informations confidentielles comme p. ex. les identifiants de connexion des internautes.

Le terme anglais phishing est un mot-valise composé de « password » et de « fishing » et signifie donc littéralement « pêche aux mots de passe ».

Mémento :



(https://www.ebas.ch/wp-content/uploads/2019/10/phisingSKP_fr.pdf)

Pour aller plus loin

Le phishing ou hameçonnage classique

Lors d'une attaque de phishing classique, les assaillants tentent d'attirer leurs victimes sur des sites Internet piratés au moyen de faux courriels, dans le but de leur voler leurs identifiants (p. ex. numéro de contrat, mot de passe, etc.).

À la place ou en complément de cela, ils ajoutent souvent des pièces jointes contenant un cheval de Troie qui, à l'ouverture du fichier, va discrètement s'installer sur le dispositif de la victime et, à partir de là, enregistrer les identifiants de connexion aux comptes de l'internaute ou l'amener à se connecter sur des sites piratés.

Bon à savoir : les instituts financiers n'envoient jamais ce genre d'email.

Prévention : ne cliquez jamais sur les liens ou sur les pièces jointes contenus dans les courriels et tapez toujours manuellement l'adresse de l'institut financier dans la barre d'adresse. Vérifiez la connexion SSL et la validité du certificat (https://www.ebas.ch/fr/le-controle-du-certificat/).

Spear phishing (harponnage) et Dynamite phishing

Contrairement au phishing classique, qui consiste à envoyer au hasard de grandes quantités d'emails à un large public, les destinataires du spear phishing sont ciblés et reçoivent des courriels personnalisés et rédigés sur mesure.

L'expéditeur se fait alors passer pour une personne de confiance, un membre de l'entourage, un collaborateur ou un interlocuteur connu de la victime. Conçu sur mesure, le contenu du courriel apparaît plausible et authentique, si bien qu'il n'est souvent pas reconnu par les filtres anti-spam.

Lorsque ces emails personnalisés sont rédigés de manière automatique et envoyés en masse, on parle alors de « Dynamite phishing ».

Prévention : méfiez-vous des emails non sollicités ou dont le contenu vous semble inhabituel, même si vous avez l'impression de connaître l'émetteur du message. En cas de doute, contactez ce dernier en utilisant un autre moyen de communication, par téléphone par exemple.

Smishing ou phishing par SMS

Les SMS sont de plus en plus utilisés pour les attaques de phishing. Le problème du « smishing », c'est que la plupart des critères servant à reconnaître les mails de hameçonnage ne s'appliquent pas dans le cas des SMS où le nom du destinataire n'est pratiquement jamais mentionné. La langue et l'organisation de ces messages courts sont par ailleurs trop simples et trop succinctes pour permettre de tirer des conclusions sur l'authenticité du message. Enfin, la plupart des dispositifs mobiles ne permettent pas de vérifier facilement le lien contenu dans le message ou l'identité du véritable émetteur. N'oublions pas non plus que beaucoup d'utilisateurs ont l'habitude de recevoir des SMS de vérification lorsqu'ils ouvrent une session d'e-banking ou effectuent des transactions financières.

Prévention : ne cliquez jamais sur les liens contenus dans les SMS. Au contraire, tapez vous-même l'adresse de votre institut bancaire dans la barre d'adresse et assurez-vous qu'il s'agit d'une connexion sécurisée (symbole du cadenas, adresse cible). Si vous recevez un SMS non sollicité de votre banque,

alertez-la en utilisant les informations de contact officielles (ex. numéro de téléphone) et demandez à ce que l'on vous confirme l'envoi du SMS en question.

Vishing ou phishing par téléphone
Le vishing est une variante du phishing basée sur la communication vocale par téléphone. Comme dans le hameçonnage classique, l'utilisateur est incité, après s'être entendu raconter une histoire bien ficelée, à révéler des informations confidentielles comme par exemple ses identifiants de connexion à son espace e-banking.

Prévention : ne communiquez jamais de données confidentielles (p. ex. un mot de passe) à une autre personne. Raccrochez immédiatement, lorsque l'on vous le demande au téléphone. Utilisez uniquement les numéros de téléphone officiels pour contacter votre institut financier.

Phishing par QR Code
Le principe de cette variante consiste à recouvrir des QR Codes (Quick Response Codes) authentiques présents dans des lieux particulièrement fréquentés par des mosaïques du même type, conçues par des cybercriminels pour diriger les utilisateurs vers de fausses adresses URL. Ce système permet ensuite aux hackers de démarrer immédiatement des téléchargements, en particulier sur les dispositifs mobiles, mais aussi d'exécuter des scripts ou d'afficher une fausse page d'ouverture de session d'e-banking.

Prévention : n'utilisez jamais un code QR pour vous identifier auprès d'un institut financier. Avant de scanner un code QR, assurez-vous que celui-ci n'a pas été recouvert par un autre piraté. Vérifiez si possible que le lien conduit effectivement à l'adresse souhaitée.

Phishing avec page web en pièce jointe
Dans ce genre de hameçonnage, le courriel reçu par la victime ne contient pas de lien ni de document, mais une page web frauduleuse au format HTM- ou HTML- en pièce jointe. En l'absence de lien à cliquer, la victime se sent plutôt en confiance au premier abord, d'autant plus que le fichier joint n'est pas un document (Word, Excel, etc.) pouvant contenir par exemple des macros malveillantes.

Mais le danger est bien là, car les fichiers HTM- et HTML- peuvent renvoyer directement au serveur d'un hameçonneur qui n'aura plus qu'à récolter les identifiants éventuellement saisis par la victime. Mais de tels fichiers peuvent également contenir des scripts susceptibles de provoquer d'autres dégâts.

De fait, les programmes de messagerie électronique modernes bloquent systématiquement ces renvois et scripts pour des raisons de sécurité. Mais si vous décidez d'ouvrir une pièce jointe HTM- ou HTML-, celle-ci échappe aux paramètres de sécurité de votre programme de messagerie. Cette méthode est particulièrement perfide dans la mesure où elle peut tromper même les utilisateurs déjà sensibilisés, car la barre d'adresse du navigateur contient « uniquement » un chemin d'accès local et non une URL douteuse comme dans le cas du phishing classique.

Prévention : méfiez-vous des pièces jointes au format HTM- et HTML. Ne cliquez pas sur les pièces jointes contenues dans les courriels et tapez toujours manuellement l'adresse de l'institut financier dans la barre d'adresse du navigateur.