Définition du Phishing

Pourquoi faut-il s'en protéger ?

Personne n'est à l'abri du phishing. C'est une réelle menace qui ne cesse de prendre de l'ampleur et de se sophistiquer.
Le phishing ou hameçonnage, est un terme qui définit un ensemble de techniques qui ont pour but de faire croire à une victime qu'elle s'adresse à un tiers de confiance. Il existe de nombreuses façons d'être confronté aux attaques : arnaque CPF, fausse livraison de colis, mail « urgent », etc.

Le phishing peut prendre la forme d'une attaque standardisée pour toucher un maximum de monde, mais peut également être utilisé dans des attaques plus ciblées pour **essayer d'obtenir d'un employé ses identifiants d'accès par exemple.** Résultat :

Définition :

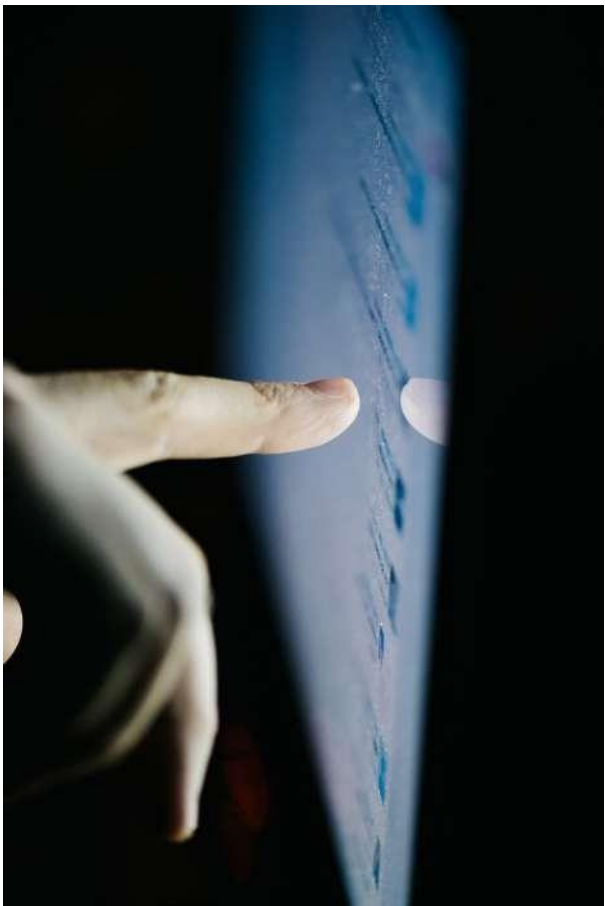
Le terme **SpearPhishing,** que vous rencontrerez désigne les attaques par mail spécifiquement ciblées.

En général, l'attaquant va usurper une identité et évoquer un sujet qui vous est familié.

80%
ne détectent pas un email malveillant.

97%
quand c'est un mail malveillant personnalisé

Malheureusement toutes les sécurités (Firewall, Antivirus…) **ne peuvent pas empêcher une erreur humaine si l'utilisateur n'est pas sensibilisé et clique sur un lien malveillant…**



Identifier l'expéditeur :

Reconnaître votre interlocuteur

Pour commencer, il est nécessaire d'analyser la provenance de votre email.
Selon votre boîte de réception vous pourrez être confrontés à un affichage différent.
Pensez à bien vérifier si l'adresse mail semble correcte et sans erreurs.

Cas n° 1 :

Vous pouvez faire confiance à cet expéditeur pour 2 raisons :
La photo de profil
Identité de Google reconnue

Ne pas faire confiance à cet email :
Photo de profil inconnue
adresse gmail notée g**rn**ail ! (nous y reviendrons par la suite)

Les conseils d'experts :
" L'identification d'un email malveillant repose sur l'accumulation de doutes et de preuves à vérifier ! Il s'agit toujours de bon sens et de reflexes à adopter !"

Cas n° 2 :

Attention aux expéditeurs inconnus !
Le point d'interrogation peut signifier que **l'expéditeur n'est pas reconnu.**

Les Liens : Attention Danger !

Ne pas cliquer n'importe où :

C'est le danger n° 1 : **les liens contenus dans les emails !**
Une URL permet aux attaquants de vous diriger vers une page malveillante ou bien de vous envoyer un fichier malveillant sur votre poste.
C'est la vérification concrète la plus efficace à mettre en place pour assurer votre sécurité face aux phishings ou même au spearphishing plus complexe à détecter.

Comment savoir si le lien est sécurisé ?

Parfois les liens sont cachés dans le texte, c'est à dire que l'url n'est pas affichée directement dans votre email. Souvent, vous pouvez être confrontés à ce type d'écriture qui signifie que le texte contient un lien hypertexte. **Dans ce cas, il faut afficher l'URL en survolant le lien sans cliquer dessus !**

Cas n° 3 :

Vérifier si l'URL est bien HTTPS et non pas HTTP ! Si vous ne connaissez pas le site vers lequel vous êtes dirigés : ne cliquez pas sur lien.
Par exemple faites plutôt confiance à : **https://si-cloud.fr**
mais méfiez vous d'un lien vers **http://si-cloud.fr.**

Rappel important :

Restez toujours méfiant !

Les acteurs malveillants peuvent eux aussi utiliser un lien https. En cas de doute, 2 sites certifiés et importants pour vous tenir informer :
https://www.cybermalveillance.gouv.fr: pour vous guider en cas de problèmes.
https://www.ssi.gouv.fr : pour vous renseigner des attaques en cours

Les pièges dans les pièces jointes !

Vous recevez un document word d'un prospect ? C'est peut-être trop beau pour être vrai...
Nous revenons en détail sur la gestion des risques des pièces jointes pendant notre sensibilisation au sein des entreprises ! N'hésitez pas à nous contacter pour en savoir plus !

Les rnail mal orth0graphlés :

Cornment les rec0nnaltres ?

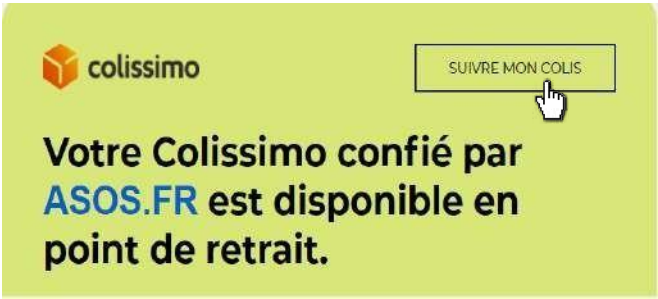
Cette fois-ci, nous allons voir comment l'orthographe peut être un piège et quelles sont les lettres à ne pas confondre. Si le message contient de très nombreuses fautes d'orthographes, il y a de grande chance qu'il s'agisse d'un mail de phishing.

Les pièges les plus fréquents :

Le m > rn par exemple si-cloud@grnail.com
Le l & le l > par exemple si-cloud (très dangereux)

Il existe de nombreuses autres combinaisons. Si vous êtes confronté à cette situation et que vous avez un doute, modifiez la police du texte !
Par exemple, passez les i et L en Times New Roman : Il.
Les lettres sont beaucoup plus simples à dissocier dans certaines polices !

Cas n° 4 :



À vous de jouer : trouvez le bon lien correspondant !

https://www.laposte.fr/outils/suivre-vos-envois

https://www.laposte.fr/outils/suivre-vos-envois

Ce n'est pas si simple ! Quand c'est bien réalisé c'est quasiment invisible à l'oeil nu !

Les actions urgentes

Pas de panique : pas de problèmes !

Mettez vos émotions de côté ! Les hackeurs le savent, les décisions prises dans l'urgence sont le meilleur moyen pour eux d'avoir une réponse à leur demande.

Ils peuvent utiliser l'urgence principalement dans deux cas de figure :

-Pour vous inciter à réaliser une action avec une durée limitée dans le temps :
"Il ne vous reste plus que 30 minutes pour participer à notre formation gratuite ! **Vite cliquez ici !"**

-Ou pour vous forcer à commettre un acte que vous n'auriez jamais réalisé sans urgence :
"Bonjour M.DUPONT, c'est Nicolas, de l'équipe commerciale, je t'envoie un mail depuis mon adresse perso car **il faut que tu fasses un virement tout de suite pour cette entreprise ! Vite c'est très urgent on a oublié de payer !!** Merci"

Il suffit que l'attaquant connaisse le nom d'un décisionnaire dans l'entreprise pour réaliser sa tentative, autrement dit, c'est très simple...

Nos conseils :

Nous avons régulièrement des clients impactés par ces tentatives !
Il est même parfois arrivé que ce soit la banque qui bloque le vire- ment au dernier moment.
Pour éviter d'en arriver là, nous conseillons toujours de faire une double vérification via deux canaux de communication différents et de contacter votre service informatique pour vérifier si le mail ne res- semble pas à du spearphishing.

Les outils et solutions efficaces :

Comment protéger votre boîte mail ?

Il existe de nombreuses solutions qui vous permettrons de rendre votre adresse de réception moins vulnérable. Voici les plus importantes à retenir :

DMARC & DKIM : des protocoles de vérification

DMARC(Domain-based Message Authentication Reporting and Conformance) est un **système de validation qui empêche l'usurpation d'identité.**
DKIM(DomaineKeys Identified) est un protocole d'authentification du courrier électronique qui **assure la protection au niveau du domaine.**
Votre adresse mail détectera une usurpation d'identité ! Par exemple, votre boite mail pourra détecter l'arnaque ci-dessous :

Cas n° 5 :

contact@si-cloud.fr.
Le **nom de domaine si-cloud.fr est vérifié**, vous recevez notre email.

contact@si.cloud.fr.
Le **nom de domaine si.cloud.fr n'est pas reconnu**, vous ne recevez pas notre email.

Messagerie chiffrée & EDR : les anti-spams

Quelle messagerie choisir ? Nous préconisons d'utiliser des organismes reconnus comme Microsoft Exchange ou Gmail.

Un EDR, à quoi ça sert ? Un EDR(Endpoint Detection and Response) est un logiciel à installer qui va détecter les menaces et les stopper ! Il utilise l'intelligence artificielle pour apprendre et s'adapter au fil du temps aux nouvelles attaques.

L’apprentissage & l’expérience

Vivez une expérience unique et amusante !

Évaluez votre niveau

Testez vos compétences en situation réelle grâce à une campagne de phishing organisée au sein de votre entreprise !

Analysez facilement vos risques

En réalisant une campagne de phishing, vous détecterez plus rapidement et plus facilement vos failles et comment les combler pour améliorer votre sécurité !

Amusez vous !

Mettre en place des mesures de sécurité, c’est important et ce n’est pas nécessairement ennuyant ! Il existe de nombreuses techniques pour rendre l’apprentissage ludique !

Tout en restant vigilant !

Gardez à l’esprit que ce que vous allez appliquer, suite à la lecture de ce book, vous permettra d’être plus vigilant et plus sûr dans votre utilisation de boîte mail !

Que faire si vous êtes victime de phishing ?

CONTACTEZ IMMÉDIATEMENT VOTRE **SERVICE INFORMATIQUE** !

Faites **opposition auprès de votre banque** si vous avez transmis vos coordonnées bancaires et conservez les preuves : le message d'hameçonnage et tout autre élément utile.

Changez vos mots de passe sur le site ou service concerné, ainsi que sur tous les autres sites ou services sur lesquels vous utilisiez ce mot de passe compromis.

Déposez plainte ! Cela permet de détecter plus facilement de nombreuses arnaques similaires.

Comment signaler un spam :

Signalez tout message douteux à **signal-spam.fr**, directement lié à la CNIL.

Signalez l'adresse du site d'hameçonnage à **phishing-initiative.fr** qui bloquera l'adresse du site.

Vous pouvez également signaler toute escroquerie ou tentative d'escroquerie sur la plateforme « PHAROS » (plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements) accessible sur le site : **internet-signalement.gouv.fr**