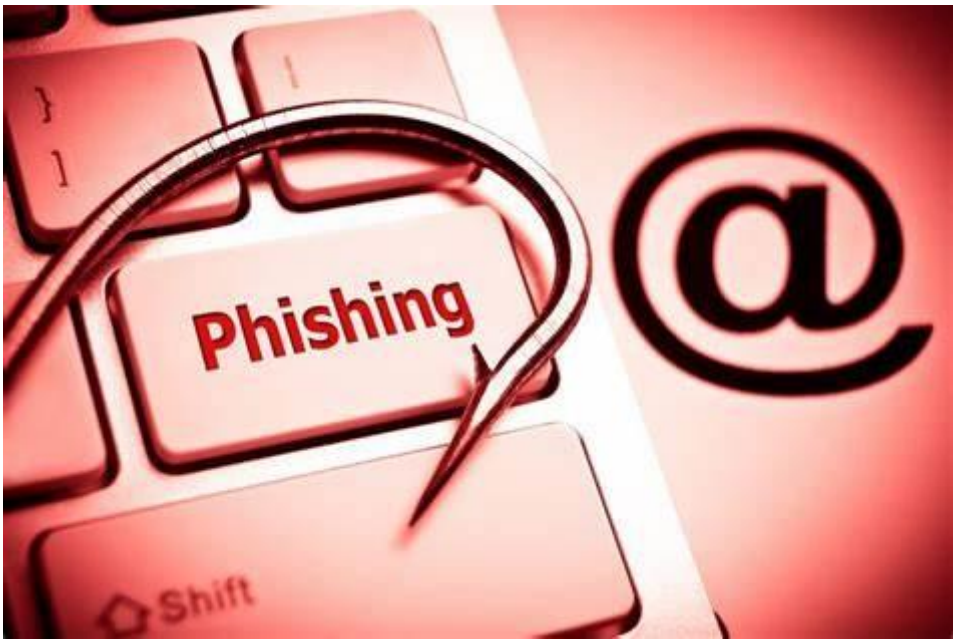


LE PHISHING

Veille technologique

PROBLEMATIQUE

Le phishing est un problème dont la gravité n'est pas mise en avant. Mais il peut s'avérer très dangereux entre de mauvaises mains. Qu'est-ce que le phishing et ses conséquences

David Koffi

BTS SIO SISR 2ème année

Table des matières

Veille technologique

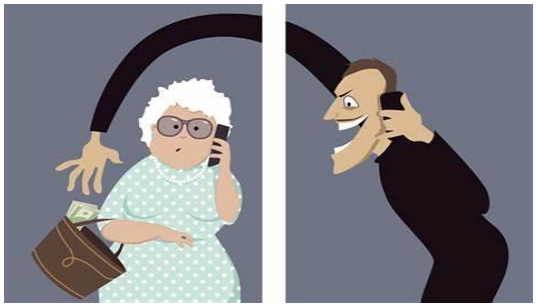
Le phishing est une technique utilisée par les cybercriminels pour tromper les utilisateurs et les inciter à divulguer des informations sensibles telles que des mots de passe, des informations financières ou des identifiants personnels. Cela se fait généralement en envoyant des e-mails, des messages texte, des appels téléphoniques ou en créant des sites web falsifiés qui imitent des entités légitimes, telles que des banques, des entreprises ou des services en ligne. Il existe différents types de phishing :

- Phishing téléphonique (vishing)
- Phishing par SMS (smishing)
- Phishing par e-mail
- Phishing sur les réseaux sociaux
- Spear phishing
- Whaling

I-) Les différents types de Phishing

A-) Vishing

Le vishing est une arnaque qui consiste à manipuler un utilisateur en appel téléphonique dans le but de lui soutirer des informations ou des données personnes. Les arnaqueurs ont accès à des informations sur leurs cibles et suscitent de l'intérêt pour eux tout en essayant de leur soutirer des données sensibles. Par exemple, des arnaqueurs qui se font passer pour des conseillers chez Free ou chez Bouygues et qui en profite pour avoir accès à des infos ou des données en posant des questions pour créer de l'intérêt chez leurs cibles.

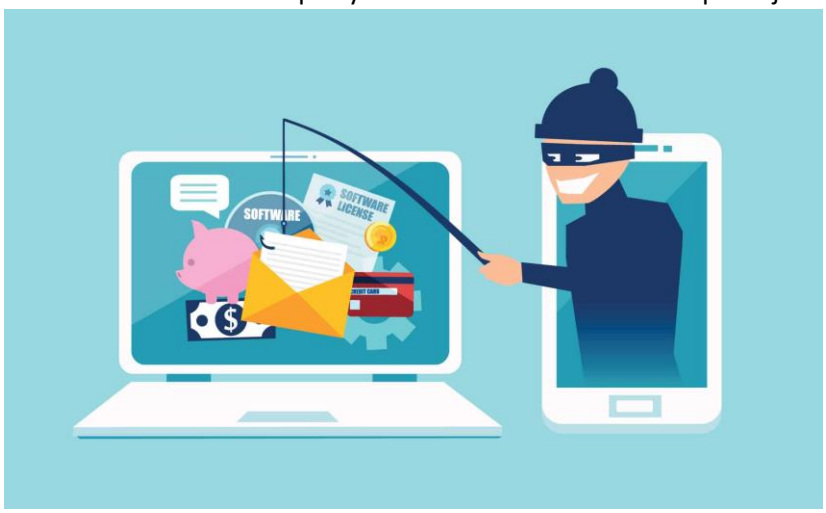


B-) Smishing

Le smishing est similaire au vishing, mais les arnaqueurs le font par sms. Ils utilisent un algorithme qui envoie un message automatique à des milliers de numéros de téléphones. Par exemples ils peuvent collecter tous les numéros de personnes qui ont de l'intérêt pour Netflix dans une base de données, et déployer l'algorithme. Il enverra un message du genre « ***Bonjour Emma, ayant consulter votre compte nous constatons un retard de paiement durant le mois de mars 2020 pour un abonnement à Netflix Japon, veuillez cliquer sur le lien suivant afin de procéder au paiement : lien.smishing.com*** ». Effectivement si l'algorithme a déployé le message à 10 000 personne, 50% des personne au moins qui ne sont pas souvent connectés ne verront pas que c'est un appât.

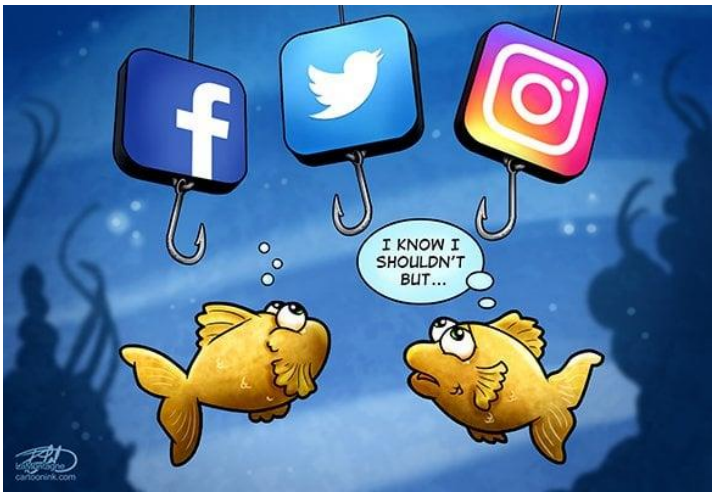
C-) Phishing par e-mail

C'est le même principe que le smishing mais par mail. En plus les arnaqueurs peuvent ajouter des pièces jointes téléchargeables malveillantes. Ex « ***Bonjour Emma, ayant consulter votre compte nous constatons un retard de paiement durant le mois de mars 2020 pour un abonnement à Netflix Japon, veuillez cliquer sur le lien suivant afin de procéder au paiement : lien.smishing.com Vous trouverez en pièce joint un document à télécharger pour voir la facture et les détails*** ». En effet il est évident qu'il y'a un cheval de Troie dans la pièce jointe ou une sorte de malware.



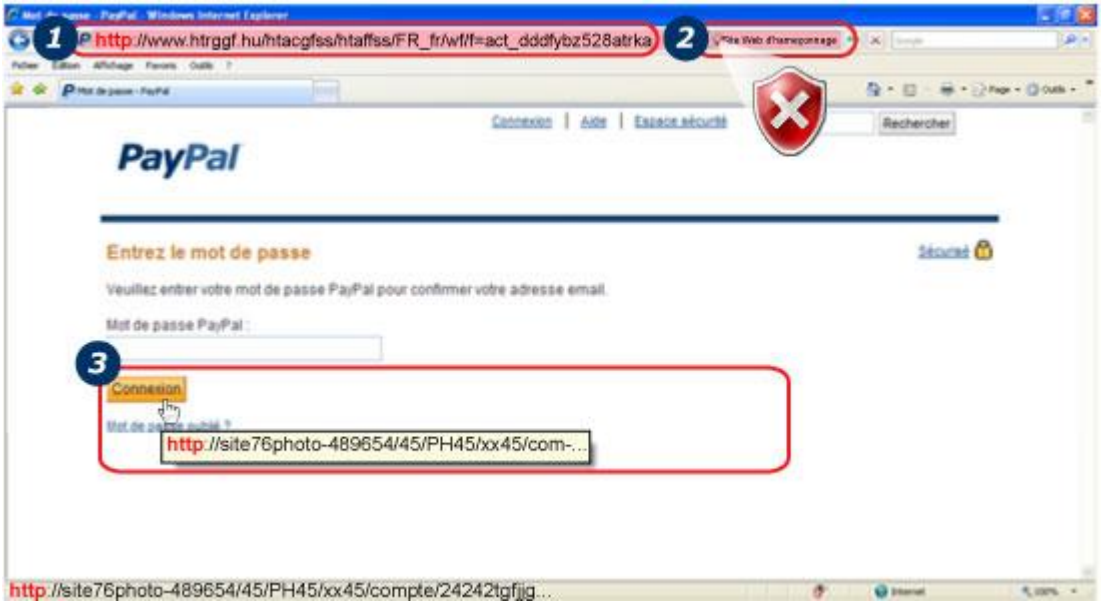
D-) Phishing sur les réseaux sociaux

C'est le même principe que le smishing et le phishing par e-mail, mais sur les réseaux sociaux. Les arnaqueurs vont sur les profils de leurs cibles et customisent leurs attaques en fonction du type de cible. Par exemple ils peuvent aller sur le profil d'un influenceur ou de quelqu'un qui est en recherche de vue et d'abonné et qui aime la mode. Ensuite ils envoient un message privé du genre « ***Bonjour John nous avons consulter votre profil et aimerions faire un partenariat avec vous pour promouvoir notre marque. Vous porterez des vêtements et prendriez des photos et les posteriez sur votre compte et vous serez rémunéré. Veuillez remplir ce formulaire et entrer votre RIB et signez ce contrat.*** » Si la cible est un jeune influenceur débutant qui n'a pas l'habitude ou qui n'a jamais reçu ce genre de message il peut tomber dans le piège.



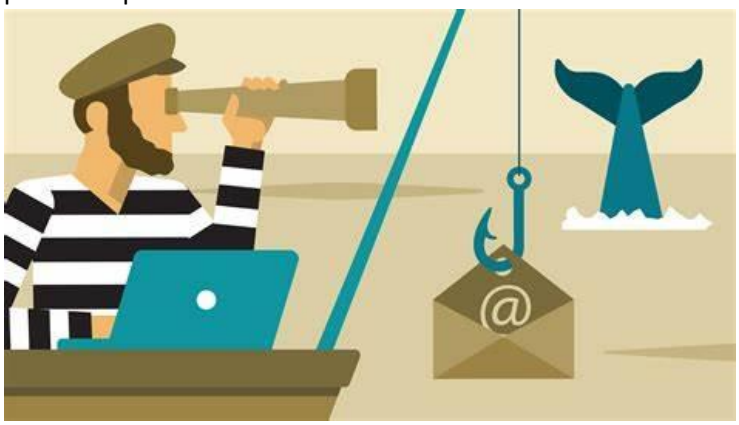
E-) Spear Phishing

Cette méthode est particulière car elle s'apparente à toutes les sortes de phishing. La seule différence est que les arnaqueurs créent des sites de société qui existent déjà et les reproduisent à la perfection. Par exemple, ils peuvent envoyer un message du genre : ***« Bonjour madame Dujardin, vous devez renouveler votre assurance santé car elle arrive à expiration. Rendez vous sur le site web de ameli ci-dessous : www.ameliee.com*** ». Il est difficile de distinguer le bon grain du mauvais.



F-) Whaling

Il est utilisé généralement entre les entreprises. Un membre d'une entreprise ou quelqu'un se faisant passer pour quelqu'un d'autre dans l'entreprise utilise toutes les techniques de phishing dans le but de cibler une autre entreprise ou quelqu'un dans une autre entreprise. Dans le but de voler de l'argent, des données confidentielles, des preuves, ou un secret spécifique de l'entreprise. C'est un type d'attaque ciblé (c'est-à-dire précis). Les autres types de phishing sont des attaques visant des cibles au hasard ou en masses. Tandis que le whaling lui cible une personne ou un groupe de personne précis.



II-) Comment éviter le Phishing ?

A-) Limiter l'erreur humaine :

Pour éviter le phishing, la première solution est d'organiser une campagne de sensibilisation. Comme le dit le dicton « l'erreur se situe souvent entre la chaise et l'ordinateur », l'appât c'est souvent la mentalité des cibles de phishing. Il faut sensibiliser les utilisateurs afin qu'ils fassent attention à ne pas cliquer sur, télécharger, partager n'importe quoi venant de n'importe qui même cela leur semble familier ou si cela suscite de l'intérêt chez eux.

Pour cela nous pouvons les mettre à l'épreuve. Par exemple, étant Administrateur des systèmes et du réseaux d'une entreprise tu peux envoyer des mails « corrompus » inoffensif dans le but de tester les membres du personnel de l'entreprise. Si plus 10% des membres clique sur, télécharge ou partage des infos de l'entreprise, il faudra faire une sensibilisation interne car cela est grave.
De même avec des clefs USB disposé au hasard dans l'enceinte du bâtiment.

Une autre solution serai de faire une mini formation aux utilisateurs afin de les sensibiliser aux attaques comme le phishing ou autres ainsi que les conséquences qui en découle en entreprises et dans leur quotidien. Une présentation avec des slides ainsi qu'une démonstration serait idéale pour les sensibilisé et créer l'effet « machine à café » créant ainsi un engouement autour de la formation, tout en touchant le maximum de personne sans perdre pour autant l'aspect « dangerosité » que pourrait entrainer ce genre de situation pour l'entreprise et le personnel.

B-) Reduction des spams et des mails automatiques de bot :

Pour réduire au maximum les incidents liés au phishing au niveau du secteur de l'informatique, il faut :
-Faire des filtres dans les mails : par exemple sur Outlook il est possible dans les paramètres de filtrer les mails qui se ressemblent ou qui contiennent un mot ou une certaine phrase. On sait tous que les mails de phishing ou les spams son fait la plupart du temps par des bots. Donc ce sont souvent les mêmes mots ou les mêmes phrases. Dans le cas ou les mails sont travaillés faudrait faire une white liste de toute les adresses IP des mails des partenaires de l'entreprise. Et quand ont reçoi un mail douteux la boîte mail compare l'adresse IP de l'envoyeur pour la comparer avec celle de la white list.

-Faire une liste noire : faire une liste qui recensent des adresses de sites malveillants dans le but de les bloquer. Il existe plusieurs solutions pour faire cela :

- Serveur DNS : Mettre en place des serveurs DNS qui afin de filtrer les requêtes DNS et bloquer les adresses malveillantes.
- Les anti-virus : effectivement souvent ça ne sert à rien de se prendre la tête, on installe un anti-virus et il met tous en place pour bloquer les sites malveillants.
- Les extensions : utiliser des extensions tels qu'Ad block par exemple pour bloquer les pubs, créer un compte google pour l'entreprise et connecter ce compte sur les postes de l'entreprise, et ensuite se connecter en admin sur le compte et aller dans google store chercher des extensions à ajouter sur le compte google qui vont être ajouter sur tous les navigateurs chromes de l'entreprise.
- HOSTS : le fichiers HOSTS de Windows contient une liste d'adresses malveillants qui sont bloquée. Donc ne pas être timide et ajouter quelques-unes en passant.

C-) Anticipation du risque :

1-) Analyse comportementale

Analyser le comportement des utilisateurs, des appareils, des applications et logiciels afin de déceler tout comportement anormal dans le cas ou quelque chose n'est pas à ça place ou fonctionne différemment.

2-) Mettre en place des politiques de sécurité

Faire une liste de démarches et de règles à suivre concernant tous les systèmes et le réseau de l'entreprise. Ordonner aux membres du personnels de faire des mots de passe avec 8 caractères minimum inclus des majuscules et des minuscules et des caractères spéciaux et non de mettre 12345 ou le nom de leur animal de compagnie ou d'un membre de la famille (les arnaqueurs au phishing on souvent des infos sur la vie personnelle des utilisateurs). Ordonner de toujours mettre le poste en veille avant de quitter l'entreprise. Vérifier l'identité de toutes personne qui rentre dans l'entreprise, surtout si cette personne transport toute forme de matériels électroniques. Ne pas laisser les clés USB trainer. Veiller a ce qu'aucun visiteur laisse une clés USB ou un appareils à lui dans l'entreprise.

3-) Analyse forcé tous les mois de l'anti-virus

Faire chaque mois un checking complet de tous les post et faire une analyse anti-virus afin de vérifier si tous sont ok. Il existe de nombreux bons logiciels qui sont spécialisés dans l'analyse des fichiers, du disque dur, de la mémoire etc. Et aussi faire une analyse de sécurité du réseau dans le cas ou un anti-virus de type verre se déploie sur le réseau.

III-) Conclusion

Le risque zéro n'existe pas en sécurité, surtout avec le facteur humain. Car même si les ordinateurs et les algorithmes effectuent à la perfection leur rôle, l'homme commet des erreurs. Il faut donc miser sur la sensibilisation et des techniques de sécurité bien définies. Et également être à jour des dernières technologies pour avoir le maximum d'outils et de technique dans son camp.