Phishing, à la pêche aux données !

Bastien Monnet | 21 janvier 2020 | www.bastien-monnet.fr

Préambule

Qui n'a jamais reçu un e-mail de sa **banque**, de son **assurance**, de son **fournisseur d'accès Internet** ou même des **impôts** l'invitant à, par le biais d'un **lien**, mettre à jour ses **informations personnelles** et/ou saisir ses **identifiants bancaires** ? Dit comme ça, ça peut paraître **anodin** et pourtant, un simple **lien** peut cacher une terrible menace, le **phishing** !

Sous ce terme équivoque, se trouve une **technique de piratage** vieille de plus de **20 ans**. En effet, d'après le site Internet Silicon.fr, le premier cas de **phishing** remonterait à **1996** ! Dont le but était d'obtenir des **données d'authentification** pour entrer, sans payer, sur le réseau **AOL** afin d'obtenir des quotas plus élevés de téléchargement (ô douce époque de l'abonnement limité à Internet et des modems 56k à la mélodie gracieuse).

Normalement, à ce stade, vous apercevez l'iceberg au loin sans vous doutez de la menace qui se profile. Approchons-nous et voyons ensemble sa face cachée.

Qu'est-ce que le phishing ?

Entre la phonétique du terme et l'illustration de cet article (sans parler du jeu de mot habile dans le titre), je pense que vous avez une petite idée sur l'origine du terme **phishing**.

C'est la contraction de "*fishing*" (qui signifie "*pêche*") et de "*phreaking*" (qui veut dire "*piratage téléphonique*"). En bref, cela consiste à "*pêcher*" des **informations** en "*piratant*" l'**identité** de quelqu'un afin d'obtenir aisément les dites informations.

En français, on utilise le terme **hameçonnage**. Ou aussi **filoutage** mais j'ai une nette préférence pour le premier qui fait bien plus sérieux.

Aujourd'hui, le **phishing** est principalement véhiculé par des **messages électroniques** mais à l'époque, où Internet en était encore à ses débuts, il était surtout pratiqué par **téléphone**. Le but était de **voler** des **numéros de carte de crédit** et/ou des **informations personnelles** (pour ensuite **usurper** l'identité des victimes). Le **phishing** se pratique aussi par **SMS** et **fax**. Et aujourd'hui, il se pratique également via les **réseaux sociaux** comme **Facebook**.

Les escrocs vont même jusqu'à faire de l'**ingénierie sociale** pour vous duper. C'est-à-dire qu'ils vont enquêter sur votre **vie privée** et **professionnelle** pour pouvoir vous approcher plus facilement. Et à l'ère de **Facebook** et Cie, où on publie dès qu'un événement survient (naissance, mariage, vacances, etc.), c'est un véritable jeu d'enfant !

D'après une étude menée par **Altospam**, un éditeur de solution anti-spam qui a conservé des statistiques depuis **2005**, près de deux e-mails sur trois étaient une tentative de **phishing** sur le **premier semestre 2019** (avec un taux moyen de **65,26%**). Pour comparaison, les **ransomwares** sur lesquels j'ai également rédigé un article, ne représentaient qu'une moyenne de **0,31%** sur le début de l'année 2019. Quant aux **e-mails légitimes** (non publicitaires), ils ne représentent que **19%** de la masse...

Phishing, à la pêche aux données !

Bastien Monnet | 21 janvier 2020 | www.bastien-monnet.fr

Comment ça fonctionne ?

Le procédé est simple et commence par une **usurpation d'identité**. Généralement, l'**escroc** se dissimule derrière une **administration publique** (impôts, sécurité sociale, etc.) ou une **société** où vous avez de fortes chances d'être **client** (banque, opérateur Internet, etc.).

Ensuite, l'**escroc** essaye d'instaurer un climat de **confiance**. En arborant le **logo** de l'**entité usurpée**, ses **mentions légales**, sa **charte graphique**, son **site Internet**, etc. Généralement, il est question d'**argent** (vous êtes éligible à un **remboursement**, par exemple) et/ou de **sécurité** (votre **compte** doit être **mis à jour**, par exemple).

Une fois que votre **confiance** est gagnée, l'escroc vous invite à cliquer sur un **lien**. Confiant, vous cliquez dessus. Vous arrivez alors sur un **site Internet** aux couleurs de l'**entité usurpée**, vous retrouvez vos marques, cela vous conforte d'autant plus. Sur la page, un banal **formulaire** à remplir (soit avec les **informations personnelles** nécessitant d'être mises à jour, soit avec les **informations bancaires** requises pour être remboursées).

Et là, la technique du **phishing** entre en action. En fait, vous n'êtes pas sur le **site Internet** de l'**entité usurpée** mais sur une **copie**, fidèle au possible (jusqu'à l'adresse URL). Les **informations personnelles/bancaires** que vous venez de saisir dans le **formulaire**, elles ne seront pas récupérées par l'entité usurpée mais par l'escroc. Vous avez été piégé !

Dans le cadre de **données bancaires**, il y a de fortes chances que vous constatiez des **prélèvements anormaux** dans les jours à venir. Dans le cadre de **données personnelles**, elles seront **revendues** au plus offrant qui les utilisera pour vous **spammer** ou, pire, pour **usurper votre identité**.

N'espérez pas résoudre le problème en **contactant** l'escroc, il y a de fortes chances qu'il ait utilisé une **adresse e-mail éphémère**. Qui plus est, il y a fort à parier qu'il ne soit pas dans le même pays que vous...

Cas concrets

À titre professionnel (**responsable informatique** d'une **PME**) ou à titre personnel (je baigne dans l'**informatique** depuis plus de 15 ans), j'ai eu l'occasion de croiser un bon nombre de tentatives de **phishing**. Des fois, l'**escroquerie** est aussi grosse que le nez de Cyrano de Bergerac. Des fois, c'est subtil au point de me faire douter (mais heureusement, il persiste des **signes révélateurs** difficiles à camoufler).

J'ai même eu l'occasion d'en faire une **formation vidéo**, disponible sur ma chaîne YouTube. Le format est un peu long (1h15) mais j'y explique **comment détecter un e-mail frauduleux**. Et pour cela, je m'appuie sur des **cas concrets**. Je clique même sur les **liens** (ce qu'il ne faut pas faire, on est bien d'accord) pour vous montrer l'envers du décor.

Parmi les grands classiques, il y a le **phishing à l'administration publique**. Par exemple, un e-mail d'**AMELI** (la branche Assurance Maladie de la Sécurité Sociale). L'**objet** est **légitime** et fait miroiter un **remboursement**. L'**adresse e-mail** pourrait confondre un néophyte car il contient le terme

"*AMELI*", genre "*remboursement-ameli@gmail.com*". Le message est plutôt bien **construit** et sans **faute d'orthographe**, comme un **e-mail officiel**. Bref, tous les signaux sont au vert. On nous invite donc à **cliquer sur un lien** pour renseigner nos **coordonnées bancaires** afin de recevoir le dit **remboursement**. Sauf que les **coordonnées bancaires** seront récupérées par l'**escroc**. Quant au **remboursement**, il va se transformer en **dépense anormale** sur votre **compte bancaire**...

Le but est toujours le même, gagner votre **confiance** pour "*pêcher*" vos **informations personnelles**.

Autre grand classique, le **phishing** sous couvert d'une **fraude au président**. Généralement, là on attaque un **service comptabilité** en se faisant passer pour le **dirigeant**. Cela nécessite de l'**ingénierie sociale** pour savoir qui contacter et sous quel nom (et quelle **adresse e-mail**). Mais le but reste le même, récupérer des **informations bancaires** comme un **RIB**.

On peut avoir la même chose à l'échelle d'un **particulier**. L'escroc se fera passer pour un **prestataire de service** connu et reconnu (Orange, EDF, etc.) et il prétextera une intervention chez vous (et ainsi obtenir votre **adresse postale** et/ou **e-mail**).

Avec de l'**ingénierie sociale**, il peut même se cacher derrière une **société** où vous êtes client (SFR, Free, Engie, votre banque, votre mutuelle, etc.) et vous demander des informations concernant votre contrat (jusqu'à votre **carte bancaire** ou votre **RIB**).

Dernièrement, j'ai même vu passer des cas concernant des **transporteurs** (UPS, DHL, Chronopost, etc.) sous couvert d'une commande à livrer. Avec soi-disant des **frais de livraison à régler**.

Bref, vous l'aurez compris, l'**escroc** pourra se faire passer pour une **société** mais aussi un **proche**, un **collègue**, un **policier**, un **huissier**, une **administration publique**, etc. Le but étant d'accrocher votre confiance par tous les moyens possibles.

Comment s'en prémunir ?

Il y a **deux axes de prévention** à mener. Les deux axes sont **complémentaires**, l'un ou l'autre ne suffisant pas. La particularité du **phishing** c'est qu'il ne se cache pas derrière un **vers informatique** (virus). Donc, on ne parlera pas d'**antivirus** ni de **pare-feu**.

Tout d'abord, il est primordial d'avoir un **anti-spam**. Il peut être déjà inclut, comme dans certaines solutions de messagerie style **Gmail**. Mais vous pouvez le compléter avec une solution payante comme **Altospam** ou **Vade Secure**.

Attention, à l'instar d'un **antivirus**, ce n'est pas une **protection ultime**. Un **anti-spam** repose sur des **listes noires** et des **algorithmes de détection** (basés sur des mots-clés, adresses e-mail, liens, etc.). En conséquence, un nouveau type de **phishing** peut passer entre les mailles du filet (je suis fier de ma blague, comprendra qui pourra).

Ensuite, c'est bête à dire mais il va falloir faire preuve de **vigilance**. Ne pas croire sur parole le premier message reçu, et ce même s'il vient de votre **famille/direction** ou d'une **administration**

publique. En règle générale, ne communiquez **JAMAIS** vos coordonnées personnelles **ET** bancaires sur Internet.

Par exemple, vous avez reçu un e-mail des **impôts** ? Appelez-les. C'était un **appel téléphonique/SMS** ? Rendez-vous sur place. Il faut savoir qu'une **administration publique** (et cela vaut également pour les **banques**) ne vous demandera jamais vos **coordonnées bancaires** et **personnelles** par **e-mail**.

En outre, évitez de vous rendre sur des **sites Internet** par le biais des **liens** contenus dans les e-mails, préférez l'**accès direct** (via vos **favoris** ou un **moteur de recherche**). La plupart de vos **correspondants professionnels** (banques, télécoms, administrations publiques, etc.) disposent d'un **espace client** et en vous y connectant, vous saurez si on vous réclame vraiment des **informations**.

Dans ce sens, je rappelle une astuce dont j'ai parlé dans mon article sur les ransomwares. En **survolant** un lien contenu dans un **e-mail**, vous verrez (en bas à gauche ou en bas à droite de la fenêtre) l'**adresse du site Internet** vers lequel pointe le **lien**. Si ce dernier n'a **aucun rapport** avec le correspondant mentionné au départ, passez votre chemin. Cela fonctionne aussi avec l'**adresse e-mail** (un e-mail de **Free** alors que l'adresse e-mail se termine par "*sfr.fr*" ? Passez votre chemin).

Vous pouvez également **vérifier le message** en lui-même, particulièrement les **fautes d'orthographe** (de grammaire, de syntaxe, etc.). Vérifiez également l'**expéditeur** et son **lien** avec vous (vous êtes client à la banque **LCL** et vous recevez un e-mail du **Crédit Agricole**, passez votre chemin).

En bref, il n'y a pas de **solution miracle** contre le **phishing**. Tout est question de **vigilance**. Prenez votre temps. Lisez, **analysez**, décortiquez l'**e-mail**. Posez-vous des **questions**. Rendez-vous sur l'**espace client**. **Appelez** l'expéditeur. Et dans le doute, même à 0.1%, **supprimez** l'e-mail. Si c'est important, l'**expéditeur** saura revenir vers vous.

N'hésitez pas à visionner ma **formation vidéo** sur les bonnes pratiques en sécurité informatique qui relate tout ce que je viens de dire, de façon plus **généraliste** (je n'y traite pas que du **phishing** mais de toutes les **menaces numériques**).

Comment réagir ?

C'est le drame, malgré mes **conseils**, vous avez **cliqué** sur un **lien** dans un **e-mail** et vous avez rempli le **formulaire** alors que c'était une **escroquerie** par **phishing**... L'erreur est humaine, au moins vous ne referez pas deux fois la même bêtise. Mais du coup, que faire ?

Si vous avez communiqué des **coordonnées bancaires**, contactez sans plus tarder votre **banque**. La majorité dispose d'un **numéro d'urgence** dans ce genre de situation, disponible **24h/24** et **7j/7**. Expliquez la **situation** et demandez le **blocage** de votre **compte**.

Si vous avez communiqué des **identifiants/mots de passe**, modifiez sans plus tarder le **mot de passe** du **compte** concerné (celui pour lequel vous avez communiqué le mot de passe). Modifiez également **tous les comptes** utilisant ce **même mot de passe** (en passant, ce n'est pas bien et on

aura l'occasion d'en reparler dans un prochain article). Si ce n'est pas possible (l'escroc a changé votre mot de passe, par exemple), alors **contactez la société** derrière le compte, **expliquez** la situation et demandez le **blocage immédiat**.

Si vous avez communiqué des **coordonnées** (téléphones, e-mails, postales, etc.), attendez-vous à recevoir du **SPAM**... À ce niveau-là, vous ne pouvez pas faire grand-chose à part **trier** et **faire attention**.

Dans tous les cas, **déposez une plainte** au **commissariat** ou à la **gendarmerie** la plus proche. Vous pouvez faire une pré-plainte en ligne, pour gagner du temps. Bien entendu, **conservez** les preuves (e-mail vérolé, échanges, etc.). Sachez qu'un numéro gratuit **INFO ESCROQUERIES** (0805 805 817) est à votre disposition pour être **conseillé** par des **policiers** et des **gendarmes spécialisés**. Et enfin, n'hésitez pas à **signaler les e-mails** via le site Internet de signalement du Gouvernement.

Le mot de la fin

On aura pu voir que le **phishing** est sournois. Très **difficile** à détecter, il peut s'avérer **fatal**. Il existe très peu de **solutions matérielles/logicielles** pour se protéger et il faudra redoubler de **vigilance** si vous ne voulez pas vous faire **piéger**.

Mais ce n'est pas une **mission impossible**. Comme nous avons pu voir, il existe des **signes révélateurs** qui ne trompent pas. Des fois, il suffit juste de **lire** (et de cogiter). Dans tous les cas, on ne clique pas sur n'importe quoi sans savoir ce qu'il en retourne. Et cela vaut pour tout, pas uniquement le **phishing**.

Pour conclure, n'hésitez pas à vous **abonner** à des **flux spécialisés** dans la **cybersécurité** (comme l'ANSSI et son site Internet d'alerte CERT-FR) ou même ceux des sociétés où vous êtes clients. Par exemple, certaines **banques** sont pointilleuses là-dessus et informent leurs clients dès qu'il y a une **vague de phishing** en leur nom. Jetez un œil à **Twitter** également (Damien Bancal, ZATAZ, CNIL, Cert-FR, Cybermalveillance, ANSSI, etc.).

Bref, **vigilance** et **information** seront vos meilleurs **alliés** contre le **phishing**.

Si vous avez aimé cet article, n'hésitez pas à le partager autour de vous.

Merci de votre précieuse attention.