06 novembre 2015
Arnaque en ligne

# Phishing : les nouvelles techniques des escrocs passent par les réseaux sociaux (et sont encore plus vicieuses)


Le phishing est une pratique qui a pour objectif de soutirer des renseignements personnels en passant par la falsification d'un mail ou d'un site.

| |
|---|
| Avec Alan Walter |
| Avec Jérôme Robert |

## Atlantico : La pratique du phishing sur internet est très fréquente. Comment un particulier peut-il concrètement se prémunir face à un tel risque ? Quelle est l'ampleur du phénomène ?

**Alan Walter** : A ce jour, il n'existe aucune méthode qui permette de se prémunir à coup sûr contre les procédés de phishing. En effet, la sophistication des méthodes employées va grandissante et les organisateurs de ces vastes tromperies en ligne rivalisent d'ingéniosité. Les meilleures réponses à apporter au phishing sont techniques et pratiques.

**Il semble judicieux en premier lieu de s'équiper d'une solution logicielle anti-virus qui intègre une protection anti-phishing.** Celle-ci aura pour effet d'alerter l'internaute lorsqu'un mail est d'une origine douteuse et lors de la visite d'un site potentiellement dangereux.

En parallèle, il est nécessaire de faire preuve de circonspection lors de l'ouverture des mails. Le phishing, technologie classique basée sur le social engineering, joue sur l'empathie et le sentiment d'urgence généré par le message. **Tout mail impliquant une action urgente à prendre par l'utilisateur, la désactivation imminente d'un compte ou l'annulation d'une commande devra être considéré comme suspicieux.** Dans ce cas, l'internaute évitera de cliquer sur l'un quelconque des liens présents dans l'e-mail mais se connectera directement au site de l'émetteur présumé ou prendra attache avec celui-ci par téléphone afin de confirmer l'authenticité de la demande.

**Jérôme Robert** : Pour se protéger **il n'y a rien de très technique en réalité, il s'agit surtout d'avoir une certaine "hygiène" ou bonne pratique**. Concrètement lorsque l'on reçoit un email qui demande d'accéder quelque part ou de cliquer sur un lien, il convient toujours de vérifier si l'adresse du site correspond véritablement à l'organisme falsifié. En cas de demande de coordonnées bancaires par exemple il ne faut pas cliquer sur le lien mais rentrer soi-même l'adresse tout simplement. Par définition le phishing c'est induire l'utilisateur en erreur pour lui extorquer de l'argent, il faut donc se montrer vigilant.

## Des cibles sont-elles privilégiées pour ces pratiques ? Les entreprises sont-elles particulièrement

**exposées ?**

**Alan Walter** : Le taux d'ouverture d'un mail de phishing étant très faible (estimé entre 1 % et 10 %), les pirates qui usent de cette méthode ont recours aux mêmes procédés qu'en matière de spam et procèdent à des envois de messages en masse, par milliers, voire dizaines de milliers.

Les entreprises ne sont donc pas des destinataires plus exposés que les particuliers.

En revanche, les messages copiés par les faussaires seront de manière générale des sites d'établissements bancaires et/ou des sites très fréquentés et regroupant de grandes quantités d'informations sur ses utilisateurs (e.g., eBay, Facebook).

**Jérôme Robert** : Il y a deux types de phishing : le spear phishing personnalisé et le phishing qui est une attaque aveugle visant à voler les données de particuliers. Les emails sont envoyés à l'aveugle à un nombre maximum d'utilisateurs comme le spam. Ni les entreprises ni des personnes en particulier ne sont visées. Il y a des entreprises qui subissent le phishing parce que l'on utilise leur image. Imaginons qu'un faussaire utilise l'image de la SNCF pour tromper un utilisateur, la victime demandera des comptes directement à la SCNF. Si le nombre de cas s'accumule, l'image de l'entreprise sera dégradée.

## Quels sont les derniers "progrès" en la matière ? Quelles sont les techniques les plus efficaces et novatrices qui permettent d'extorquer des informations ?

**Alan Walter** : Les dernières technologies virales sont désormais mises au service des pirates à l'origine des mails de phishing. De nombreux messages renvoient désormais vers un site internet contenant du code malicieux (souvent un rootkit) qui infectera le poste de l'internaute du simple fait de la visite du site, sans action de sa part, et collectera ses informations sans même qu'il ne les saisisse sur le site.

**Jérôme Robert** : Le phishing traditionnel par email envoyé massivement est le plus efficace. Il s'est beaucoup amélioré. Il y a de moins en moins de fautes d'orthographes et des liens sont plus proches de la réalité. Tout cela s'améliore avec des campagnes utilisant de véritables rédacteurs qui écrivent des textes sans faute d'orthographe ! Les achats de noms de domaines sont très proches de ceux qui sont usurpés. "goagle" au lieu de "google" par exemple. Le smishing, qui utilise les sms, existe également mais ne se développe pas de la même façon. Il n'est pas aussi efficace.

Ce que l'on risque de voir en revanche dans le phishing traditionnel c'est le développement d'outils de personnalisation automatique qui découle du spear phishing qui est ciblé. Un email très contextualisé sera envoyé par exemple celui de l'AFP pour un journaliste. Cependant tout cela demande beaucoup de travail et ne pourra atteindre autant de monde. Or de nouvelles technologies permettent d'utiliser les réseaux sociaux pour identifier une personne. Elles se développent déjà en marketing où l'activité des personnes sur les réseaux sociaux est utilisée pour mettre en place la meilleure campagne de pub. Nous devrions donc avoir demain l'équivalent du spear fishing c'est-à-dire une attaque relativement bien personnalisée mais à grande échelle. Cela permettra à ces spams d'atterrir plus facilement dans une boite mail même si elle est protégée.

## Que fait l'Etat en matière de prévention et de protection des utilisateurs contre ces pratiques ? A quoi servent les plateformes mises en place telles que PHAROS et Phishing Initiative France qui travaillent ensemble ? Les auteurs de ces infractions sont-ils poursuivis ?

**Alan Walter** : La plate-forme Pharos constituer le point central national de recueil de signalements des contenus illicites. Via le site internet-signalement.gouv.fr, l'Etat a donc mis en place un système qui lui permet notamment de mutualiser les données recueillies sur l'origine des mails de phishing, permettant ainsi d'identifier et localiser leurs auteurs avec une efficacité accrue.

Ces informations, transmises directement au service de lutte contre la cybercriminalité de la police judiciaire, servent ainsi de fondement à la mise en œuvre de procédures d'enquête.

Phishing Initiative France poursuit les mêmes objectifs, en étant opérée par une structure associative.

Le nouveau partenariat entre Pharos et Phishing Initiative permettra une transmission réciproque des signalements et d'en assurer un traitement plus rapide et plus efficace. La mutualisation de ces informations devrait faciliter l'identification et la localisation des émetteurs des messages frauduleux.

**Toutefois, la principale difficulté réside dans l'efficacité des poursuites.** En effet, les auteurs de ces e-mails sont fréquemment des utilisateurs isolés, qui résident le plus souvent dans des pays étrangers, en dehors de l'Union Européenne ou de la zone Schengen. **Ainsi, la mise en œuvre de procédure internationale est des plus ardues en raison de l'absence de coopération entre les autorités de police et les organes judiciaires des pays concernés avec les autorités françaises.**

Cette coopération nouvelle, même si elle est parfaitement louable, a de fortes chances de subir le même sort que la « boite à spam » mise en œuvre par la Cnil il y a quelque années, laquelle s'était soldée par une base importante d'émetteurs d'e-mails non sollicités, sans réellement déboucher sur des poursuites et, a fortiori, des condamnations.

**Jérôme Robert** : Le phishing étant de plus en plus difficilement détectable par les moyens automatisés, le signalement sera de plus en plus important. L'Etat a mis en place la plateforme PHAROS qui a pris un coup de fouet après les tristes événements de janvier dernier puisque la plateforme sert également à signaler les sites terroristes. La capacité a été augmentée mais il faut surtout communiquer au maximum, la fusion avec Phishing Initiative va d'ailleurs dans le bon sens. Nous publions par ailleurs de nombreux

rapport sur la cybercriminalité pour informer au maximum. Le partenariat sert aussi et surtout au niveau de l'efficacité de la réponse. PHAROS était une plateforme de signalement pour mener des enquêtes ce qui prend beaucoup de temps et d'argent. Phishing Initiative de son côté permet de faire fermer les sites. Les deux ont maintenant fusionné ce qui permettra logiquement plus de fermeté. Un lien qui ne fonctionne plus dans une boite mail sera bien évidemment devenu totalement inutile et le signalement par un seul utilisateur peut permettre d'en sauver de nombreux autres.