MS/003-14/03

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la recherche scientifique

Université Abou Bakr BELKAID – TLEMCEN

Faculté De Science

Département de l'informatique

Mémoire de fin d'étude pour l'obtention du diplôme

De Master en informatique

THEME

UNE APPROCHE A BASE D'URL POUR LA DETECTION DES SITES PHISHING

Présenté par

Mr. BENAMMAR Safi

Encadré par

Mr.BELABED.

Devant le jury

Mr.BENAZZOUZ	President du Jury.
Mr. BENAMAR	membre du jury.
Mr.SMAHI	membre du jury.
Mr.MIDOUNI	membre du jury.
Mr.HADJILA	membre du jury.
Mme.HALFAOUI	membre du jury.

Année universitaire: 2010/2011.

SOMMAIRE

TABLE DES FIGURES

CHAPITRE I

CHAPITRE II

CHAPITRE III

Liste de tableaux

INTRODUCTION GENERALE

Le phishing (contraction des mots anglais « fishing », en français pêche, et « phreaking », désignant le piratage de lignes téléphoniques), traduit parfois en « hameçonnage », est une technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations.

Le phishing repose sur les techniques d'ingénierie sociale en usurpant des identités d'autres personnes (physiques ou entreprise) via l'envoi de mails qui incitent les utilisateurs à fournir des informations sensibles au pirate.

Le but de notre étude est de comprendre les concepts de phishing, ces techniques, et construire un système capable de traquer ce genre de fraude et protéger les utilisateurs.
Le présent mémoire est organisé comme suite :

Dans le premier chapitre qui constitue une introduction a notre travail nous exposons les différentes définitions de concepts, le jargon de ce monde.

Dans le deuxième chapitre nous exposons les différentes techniques du phishing, ainsi que les méthodes utilisées pour contrer ces attaques.

Dans le troisième et dernier chapitre nous adoptons une approche de lutte contre le phishing et nous essayons de la mettre en œuvre, avec la création d'un système capable de différencier des adresses légitimes et des adresses de phishing.

CHAPITRE I

INTRODUCTION

I INTRODUCTION

Ce premier chapitre a pour but de donner les différents concepts de base du monde du phishing ainsi que leurs définitions respectives. Nous commençons par les définitions.

Le phishing, ou l'hameçonnage par e-mail, est une action frauduleuse qui prend une ampleur importante sur Internet. Le phishing vise a détourner des fonds ou des identifiants de connexion à des services en ligne

Pour procéder les pirates créent des faux sites qui ressemblent esthétiquement aux sites légitimes visés par l'attaque. Ces sites sont visités par des utilisateurs redirigés par email. Et ils sont invités à remplir des formulaires pour récupérer des informations personnels ou d'organisations sensibles.

II LE PHISHING

Terme qui désigne une forme d'escroquerie en ligne qui a pour but d'obtenir de la part des utilisateurs des informations personnelles et sensibles, par des moyens détournés, en trompant leur vigilance.

Les données sensibles peuvent être :

- un code de carte bancaire,
- un numéro de sécurité sociale,
- des identifiants d'accès à différents services sur Internet.

Le pirate peut ensuite exploiter les informations recueillies pour usurper l'identité ou voler l'argent de la victime.

Le terme de phishing est issu de deux autres termes liés au piratage :

- phreaking, un terme utilisé pour définir le détournement des lignes téléphoniques, ce qui est un terme utilisé bien avant Internet.
- Fishing, un verbe anglais qui veut dire la pèche à la ligne.

Alors le phish est un e-mail malicieux provoquant le phishing, les phishers comme des pirates informatiques adeptes du phishing.

Dans le jargon français, le phishing prend le nom d'hameçonnage. Les premiers cas de phishing de grande ampleur sont apparus dès le début de l'année 2003. Le nombre de cas de phishing n'a cessé d'augmenter pour devenir aujourd'hui une des menaces les plus actives sur Internet. Le phishing est apparu grâce aux motivations des pirates informatiques se sont détournées du jeu ou de la performance vers les intérêts financiers et l'appât du gain.

Le phishing a popularisé des arnaques qui consistaient à mettre en ligne des sites Internet marchands fantômes sur lesquels la victime passait et réglait des commandes qui n'étaient jamais honorées mais pour lesquelles son compte bancaire était débité.

Le phishing associe les mécanismes d'envoi d'e-mails et de création d'un site Web frauduleux usurpant l'image et le design d'organisation ou d'entreprises.

Quand le phishing est apparu, la nouveauté était l'utilisation conjointe de plusieurs méthodes existantes dans le but de créer une nouvelle menace ayant ses mécanismes et ses buts propres.

On peut donc proposer une définition du phishing comme la conjonction des éléments suivants :

phishing = spam + mail spoofing + social engineering + URL spoofing + scam + URL cloaking + pratique mafieuse

La pratique du phishing consiste à attirer l'internaute à l'aide d'e-mails non sollicités(Spam) comme envoyés d'adresses officielles (mail_spoofing).

Le contenu de l'e-mail reçu incitant [social engineering] la victime, sous couvert d'une fausse raison, à cliquer sur un lien proposé dans le message.

Le lien est en réalité malicieux et conçu pour usurper une destination de confiance (URL Spoofing), ce qui a pour conséquence de conduire l'internaute sur un site Web visuellement identique au site officiel pour lequel il se fait passer (scam) mais dont la véritable adresse est dissimulée aux yeux de l'internaute victime (URL Cloaking)].

L'internaute étant conforté dans son idée d'être connecté au site officiel est à présent enclin à renseigner des informations personnelles qui seront exploitées par le phisher (pratique mafieuse).

Bonjour client de Visa Card ,

Votre Carte Bancaire est suspendue , Car nous avons remarquer un probleme sur votre Carte.
Nous avons determiner que quelqu'un a peut-etre utilisé Votre Carte sans votre autorisation. Pour votre protection, nous avons suspendue votre Carte de credit. Pour lever cette suspention, cliquez-ici et suivez la procédure indiquer pour mettre votre carte de crédit à jour.
Note: Si celà n'est pas achevé d'ici le 30 Février 2011, nous serons contraints de suspendre votre carte indéfiniment, car elle peut être utilise pour fraude.
Nous vous remercions de votre coopération dans le cadre de ce dossier.

Merci,
Support Clients Service.
Copyright 1999-2010 VerifedbyVisa . Tous droits reserves

Figure 1.1 : exemple d'email de phishing

III USURPATION D'IDENTITE

Nous pouvons définir l'usurpation d'identité comme le fait de prendre l'identité d'une autre personne, d'utiliser, sans son accord des informations permettant de l'identifier comme nom, prénom, numéro de carte bancaire. Ces information peuvent utilisées ensuite sans la connaissance de leur propriétaire pour avoir un crédit, un abonnement ou tout simplement a nuire a la réputation de la victime.

IV URL CLOAKING, SPOOFING ET LE URL SPOOFING

1 URL Cloaking

L'URL Cloaking est la dissimulation de la véritable adresse d'une page Web visitée dans la barre d'adresse du navigateur. Plusieurs méthodes peuvent être employées pour conduire de l'URL Cloaking :

- Profiter d'une vulnérabilité du navigateur Web permettant d'afficher le texte de son choix dans la barre d'adresse, et ce, quel que soit le site Internet visité,
- Placer astucieusement un pop-up pour faire croire à une autre adresse dans la barre d'adresse,
- Utiliser un jeu de frame (balise <frame> ou <iframe> en HTML).

L'URL Cloaking est utilisé pour dissimuler la vraie adresse pour ne pas attirer l'attention de l'utilisateur.

2 Spoofing

Spoofing signifie **usurpation.** Cette technique est utilisée dans le but de se faire passer pour une autre entité et profiter de ses privilèges d'accès ou de fonctionnement. Le plus souvent on parle d'IP Spoofing pour l'usurpation d'adresse IP (pour tenter de pénétrer dans un système d'information).

3 URL Spoofing

On effectue de l'URL Spoofing pour signifier **l'usurpation** d'une URL en lieu et place d'une autre.

V MOTIVATIONS DU PHISHING

Le phishing a pour but de voler des informations confidentielles aux internautes.
Le phishing nuit à l'image des grandes entreprises comme les banques car avec l'augmentation des attaques, les transactions en lignes avec les utilisateurs peuvent chuter a cause de la peur. Alors les organismes visés par les attaques de phishing voient leur réputation atteinte par la portée de ces attaques et par l'usurpation de leur identité.

Des organisations pour lutter contre le phishing permettent de suivre l'évolution de cette menace. Nous pouvons citer par exemple l'APWG (l'Anti-Phishing Working Group) créé en novembre 2003 afin de recenser et de centraliser les attaques de phishing et de mener des études et analyses sur la propagation du phénomène, afin de mieux le connaître et de tenter de le maîtriser par la sensibilisation des utilisateurs aux procédés et aux risques du phishing.
Cette organisation réunit des sociétés de services, des banques, des institutions financières, des cybermarchands et de nombreuses autres entreprises sur Internet.

* **Implication des victimes dans les attaques**

Pour toutes les entités connectées à Internet, internautes ou organisations, il subsiste un autre risque. Outre le fait d'être la victime d'une arnaque ou de voir son nom usurpé pour une campagne de phishing, le risque d'être un intermédiaire de cette attaque est présent.

Les phishers, afin de brouiller les pistes, se cachent souvent derrière d'autres ordinateurs pour lancer leurs attaques. Ainsi, toute entité connectée à Internet peut passer pour être à l'origine de l'attaque.

Des analyses ont montré que des ordinateurs d'internautes infectés par certains virus et transformés en machines zombies, sont utilisés à l'insu de leur propriétaire pour lancer des campagnes massives de spams, premier pas vers le phishing. De même, des serveurs Web d'organisations de confiance sur Internet peuvent être compromis pour héberger, sans que les administrateurs de ces serveurs ne le sachent, les sites Internet pirates, copies de sites officiels, utilisés dans les attaques de phishing.
Non seulement, les internautes et les organisations peuvent être abusés par le phishing mais, à leur tour, ils peuvent devenir un maillon essentiel pour piéger d'autres victimes potentielles. D'un point de vue légal, si un manquement avéré de moyen de protection est prouvé et si un préjudice est causé par ce manquement, les conséquences légales pour ces victimes, non pas de l'escroquerie de phishing mais plutôt d'être passé acteur dans les attaques, sont très importantes.

* **Les organismes internationaux [1]**

Les principaux organismes visés par le phishing appartiennent aux secteurs d'activité suivants:

1. Services financiers
2. Fournisseurs d'accès Internet
3. Gouvernements et divers
4. Vente de détail sur Internet

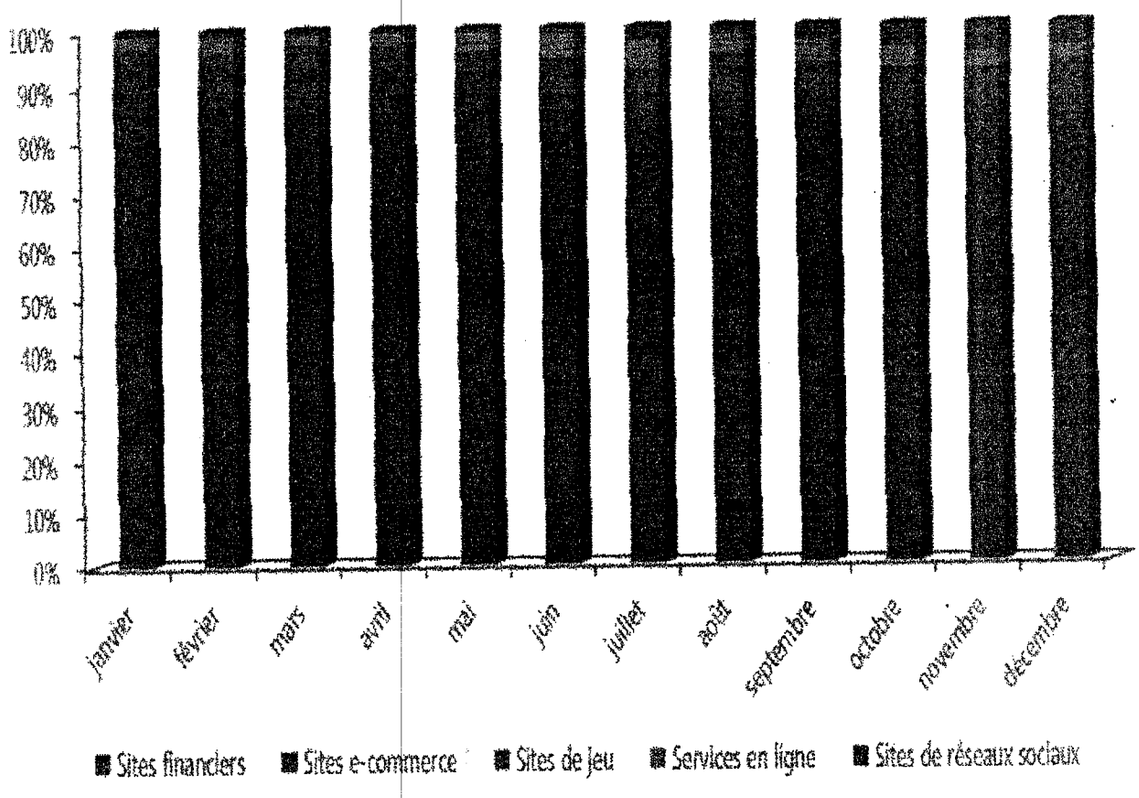


Figure 1.2 : Sites d'hameçonnage actifs observés chaque mois de 2010

C'est le secteur des services financiers, en particuliers les banques, le plus visé par l'usurpation dans les campagnes de phishing.
Ces chiffres illustrent bien la volonté des phishers et leur but premier que constitue l'appât du gain financier.

Le phénomène du phishing touche principalement les organisations nord américaines pour les raisons suivantes :

- Les phishers exploitent l'image des géants des domaines bancaires et financiers (Citibank, US Bank ou Visa, mais aussi eBay ou Paypal),
- Sur un plan linguistique, les phishers utilisent la langue anglaise, une langue parlée et comprise dans le monde entier.

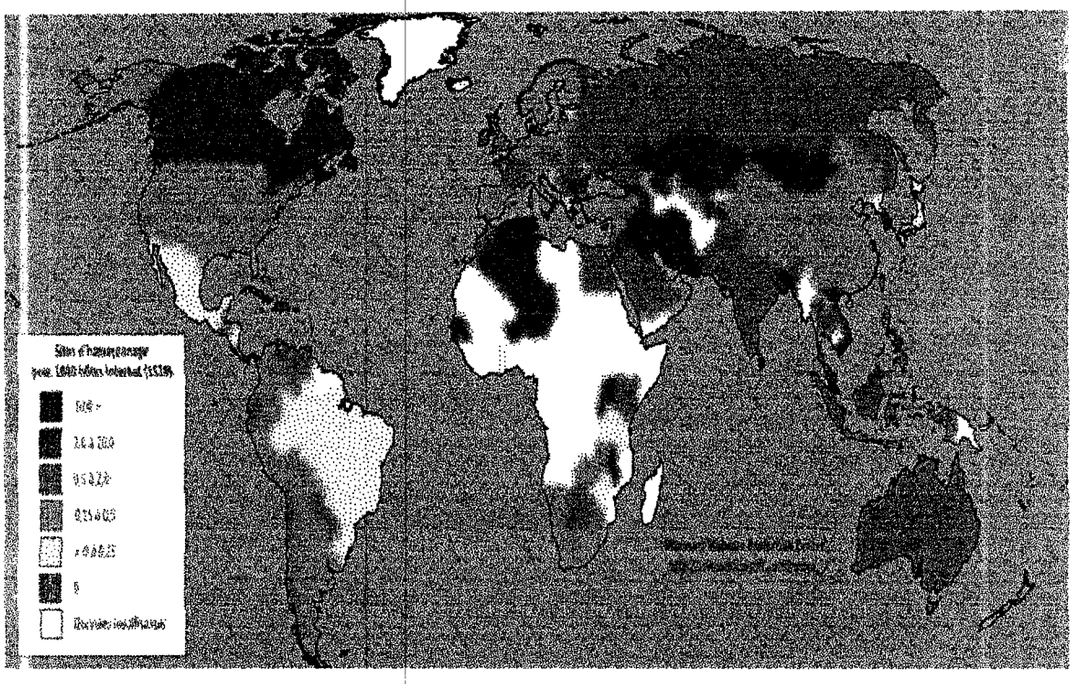


Figure 1.3 : Sites d'hameçonnage pour 1 000 hôtes Internet dans le monde

L'augmentation du nombre de cas et du nombre de sites de phishing est probablement lié à l'automatisation des outils et des techniques mais également à l'utilisation d'ordinateurs zombies qui lancent et hébergent des sites de phishing à l'insu de leur utilisateur suite à une infection par un virus informatique.

L'automatisation de la mise en œuvre des attaques de phishing et de la mise à disposition des sites de phishing est à lier à la croissance et l'utilisation des réseaux de machines zombies / botnets, en ce qui concerne l'envoi accru d'e-mails et l'hébergement d'un nombre croissant de sites de phishing.

VI FONCTIONNEMENT DU PHISHING

Le phishing profite du manque d'attention des utilisateurs et repose sur quatre principes :

1. Usurper l'identité d'une organisation de confiance pour collecter les données personnelles des clients de cette organisation,

2. Demander, sous un faux prétexte, de fournir des informations personnelles,
3. Rediriger la victime vers un site Internet pirate mais identique au site Internet officiel de l'organisation usurpée pour que la victime saisisse les informations demandées,
4. Exploiter les données collectées pour usurper une identité dans le but d'obtenir des avantages et services (argent, biens, papiers d'identité et documents administratifs).

4.2. Détail du déroulement d'une attaque de phishing

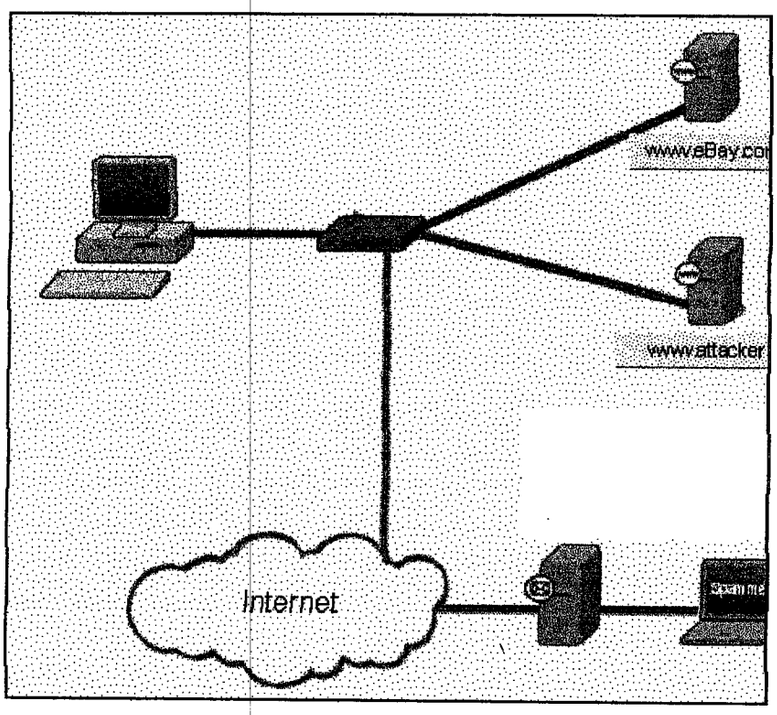


Figure1.4 : les étapes du phishing.

1 La première étape du phishing se fait par le social engineering et la manipulation. Un mail semble provenir d'une organisation digne de confiance et l'adresse expéditeur semble corroborer cela.

2 L'internaute est incité à donner des informations personnelles. Cette demande se fait au travers d'un e-mail à l'apparence officielle et demandant de fournir des informations sous un faux prétexte. L'e-mail demande bien souvent d'agir dans

l'urgence.

3 Pour accélérer la procédure, il suffit de cliquer sur le lien donné dans le message pour se connecter sur le site Internet sur lequel effectuer l'action demandée. La victime est à présent connectée sur un faux site Internet sous le contrôle du pirate. Une fois la redirection effectuée, l'utilisateur est sur un site Internet conçu de manière à être identique en tout point au site officiel. En réalité, ce site pirate est différent du site officiel mais sa véritable adresse est dissimulée à la future victime par divers moyens (exploitation de vulnérabilités du navigateur Web par exemple).

4 La victime, en confiance, saisit les informations demandées et qui sont en réalité envoyées au pirate qui peut alors s'en servir quand bon lui semble.

Le succès des campagnes de phishing s'appuie sur la probabilité que de nombreux internautes se sentiront concernés par le message et agiront selon les souhaits du phishers. Afin d'augmenter cette probabilité, le premier mail est envoyé comme un spam : non sollicité et envoyé en masse, afin de toucher le plus grand nombre d'internautes et parier sur le fait que certains, en tant que clients de l'organisation dont le nom est usurpé, se sentiront concernés et seront donc plus enclins à tomber dans le piège du phishing.

* **Les tromperies à l'origine du phishing**

Il existe plusieurs objectifs visés par les attaques de phishing.

1. **attaques consternant l'émetteur de l'e-mail.**

Les mails semblent provenir de : Groupes financiers (Paypal, Citibank, Visa,).
Entreprises Internet (eBay, Yahoo!, MSN), Fournisseurs d'accès Internet.

2. **Attaques liée à l'e-mail reçu**

L'utilisation de social-engineering pour forcer la main des internautes à accomplir la volonté du phisher : cliquer sur le lien Internet et saisir les informations demandées (nom, prénom, mot de passe).

VII EXEMPLES DE PHISHING

1. PHISHING PAR PIECES JOINTES [2]

C'est une méthode très utilisée dans le domaine, le phisheur envoi un email contenant une pièce jointe contenant un formulaire à remplir par la victime, comme l'a subi la SNCF (Société Nationale de Chemins de Fer)(société française)

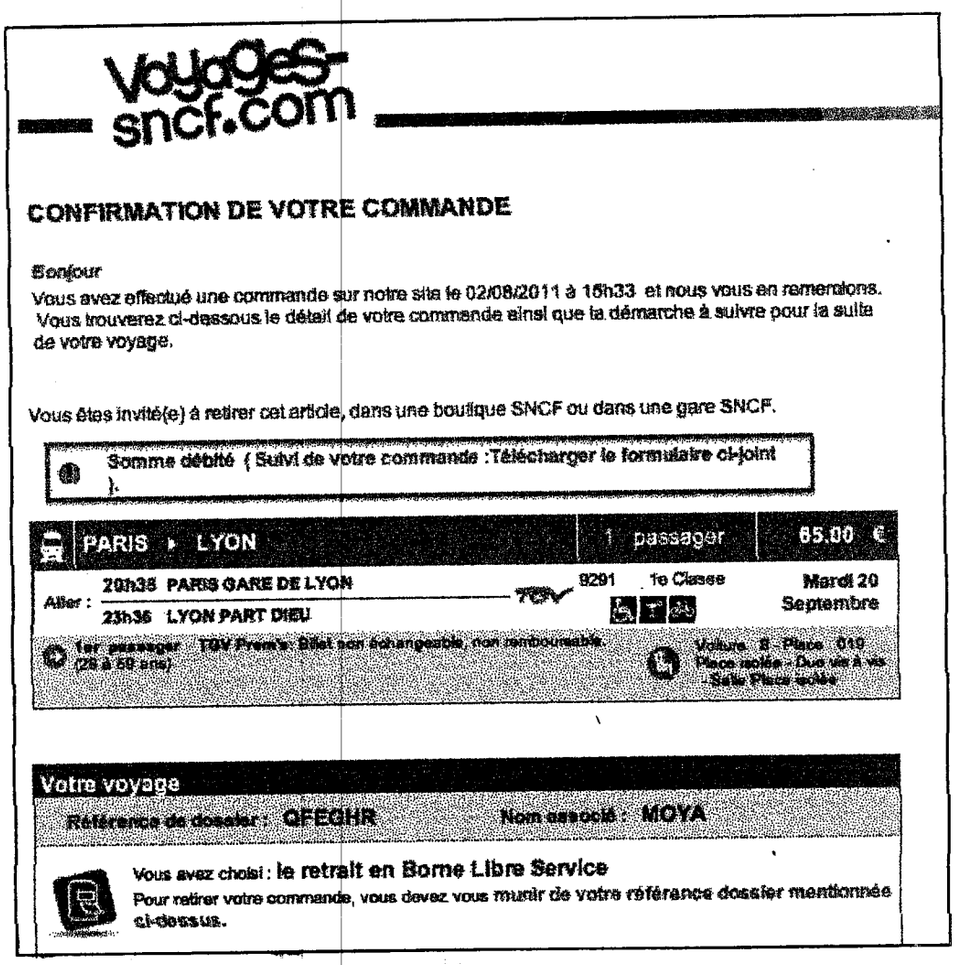
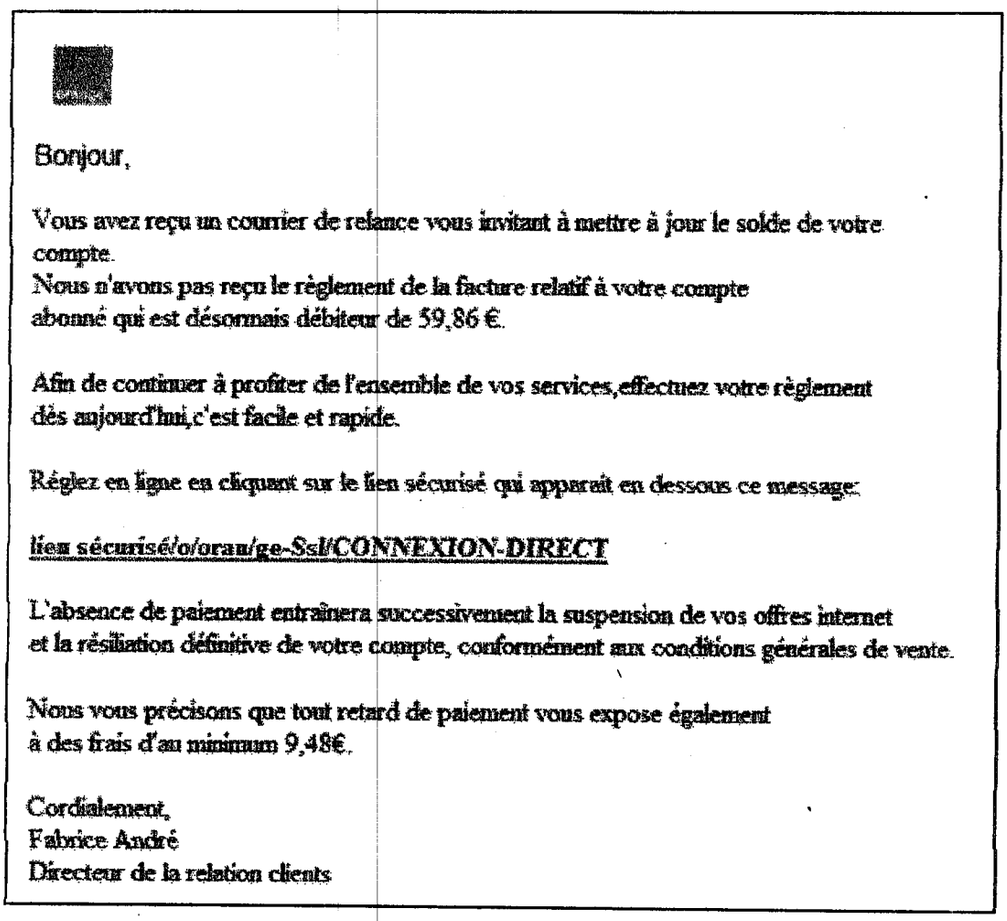


Figure1.5 : Phishing par pièce jointe.

2. PHISHING PAR REDIRECTION VERS DES SITE MALICIEUX

Dans ce type d'attaques les phishers, redirectent leurs victimes à de faux sites qui sont quasi identique aux légitimes. Ces sites utilisent souvent JavaScript pour récupérer les informations.



Bonjour,

Vous avez reçu un courrier de relance vous invitant à mettre à jour le solde de votre compte.
Nous n'avons pas reçu le règlement de la facture relatif à votre compte abonné qui est désormais débiteur de 59,86 €.

Afin de continuer à profiter de l'ensemble de vos services,effectuez votre règlement dès aujourd'hui,c'est facile et rapide.

Réglez en ligne en cliquant sur le lien sécurisé qui apparait en dessous ce message:

lien sécurisé/o/orau/ge-Ssl/CONNEXION-DIRECT

L'absence de paiement entraînera successivement la suspension de vos offres internet et la résiliation définitive de votre compte, conformément aux conditions générales de vente.

Nous vous précisons que tout retard de paiement vous expose également à des frais d'au minimum 9,48€.

Cordialement,
Fabrice André
Directeur de la relation clients

Figure 1.6 : Phishing par redirection vers un site frauduleux.

VIII CONCLUSION

Le phishing constitue un vrai danger sur internet, il crée un environnement de doute et de peur parmi les acheteurs en ligne, le nombre de sites de phishing est en augmentation continue, de nombreux personnes ont étaient victimes, et de nombreuses organisations ont vu leurs noms se détériorer.

Dans ce chapitre nous avons vu les concepts du phishing, les principales étapes utilisées pour tromper la vigilance des victimes depuis la réception de l'email jusqu'au piège.

CHAPITRE II

ATTAQUES ET SOLUTIONS

I INTRODUCTION

Dans ce nouveau chapitre nous exposons les différents types attaques utilisées en phishing, ainsi que les contre-mesures utilisées pour faire face à ces attaques qui ne cessent d'augmenter de jour en jour.

Ce qu'il faut retenir du chapitre précédent

« L'hameçonnage consiste en un envoi massif de courriels contrefaits, communément appelés courriels hameçon, utilisant l'identité d'une institution financière ou d'un site commercial connu de façon apparemment authentique.

Dans ces courriels contrefaits, on demande aux destinataires de mettre à jour leurs coordonnées bancaires ou personnelles en cliquant sur un lien menant vers un site Web illégitime qui est habituellement une copie conforme du site de l'institution ou de l'entreprise. Le pirate, ou criminel informatique qui a envoyé le courriel hameçon peut alors récupérer ces renseignements afin de les utiliser à son avantage.

Certaines techniques d'hameçonnage plus récentes, consistent en des logiciels malveillants, ou malicieux, qui sont développés dans le but de nuire à des systèmes informatiques.

Dans le cas d'une attaque d'hameçonnage, les logiciels malveillants peuvent varier d'un capteur de touches aux corrupteurs de données stockées.

Tandis qu'un capteur de touches est utilisé pour intercepter les touches frappées à l'aide du clavier et ainsi capter des mots de passe et autres informations personnelles, les corrupteurs de données de leur côté servent plutôt à corrompre les données des infrastructures de navigation afin de réorienter de façon automatique les utilisateurs vers des sites Web frauduleux à l'aide d'aiguilleurs (proxy) contrôlés par des pirates informatiques. »

II LES TYPES DES ATTAQUES [1]

1 EMPOISONNEMENT DU CACHE DNS (Cache poisoning)

Lorsqu'un serveur DNS est obligé d'interroger un autre serveur DNS pour obtenir l'adresse IP d'un nom de domaine faisant l'objet d'une requête, ce qui est le cas le plus général, il stocke temporairement (2 jours en moyenne) le résultat dans sa mémoire cache.

Ceci lui permet de pouvoir fournir immédiatement ce numéro en cas de nouvelle requête. Puisque ce cache est conçu pour recevoir des informations en provenance de l'extérieur, on conçoit que, s'il existe une faille de sécurité sur ce serveur, il soit possible à un pirate d'y

insérer un nom de domaine connu (par exemple www.google.fr) et lui faire correspondre le numéro *IP* d'un autre site (site piégé envoyant des programmes malveillants).
Un visiteur utilisant ce serveur DNS sera donc redirigé vers le site piégé au lieu d'atteindre le site demandé (Google dans l'exemple choisi).
C'est l'attaque par empoisonnement du cache.

2 INJECTION DE CODE

Les attaques de type **Cross-Site Scripting** (notée parfois *XSS* ou *CSS*) sont des attaques visant les sites web affichant dynamiquement du contenu utilisateur sans effectuer de contrôle et d'encodage des informations saisies par les utilisateurs. Les attaques Cross-Site Scripting consistent ainsi à forcer un site web à afficher du code HTML ou des scripts saisis par les utilisateurs. Le code ainsi inclus (le terme « injecté » est habituellement utilisé) dans un site web vulnérable est dit « malicieux ».
Il est courant que les sites affichent des messages d'information reprenant directement un paramètre entré par l'utilisateur. L'exemple le plus classique est celui des « pages d'erreur 404 ». Certains sites web modifient le comportement du site web, afin d'afficher un message d'erreur personnalisée lorsque la page demandée par le visiteur n'existe pas. Parfois la page générée dynamiquement affiche le nom de la page demandée. Appelons *http://site.vulnerable* un site possédant une telle faille. L'appel de l'URL *http://site.vulnerable/page-inexistante* correspondant à une page n'existant pas provoquera l'affichage d'un message d'erreur indiquant que la page « page-inexistante » n'existe pas. Il est ainsi possible de faire afficher ce que l'on souhaite au site web en remplaçant « page-inexistante » par toute autre chaîne de caractère.
Ainsi, si aucun contrôle n'est effectué sur le contenu fourni par l'utilisateur, il est possible d'afficher du code HTML arbitraire sur une page web, afin d'en changer l'aspect, le contenu ou bien le comportement.
De plus, la plupart des navigateurs sont dotés de la capacité d'interpréter des scripts contenus dans les pages web, écrits dans différents langages, tel que JavaScript, VB Script, Java, ActiveX ou Flash. Les balises HTML suivantes permettent ainsi d'incorporer des scripts exécutables dans une page web : <SCRIPT>, <OBJECT>, <APPLET>, and <EMBED>.
Il est ainsi possible à un pirate d'injecter du code arbitraire dans la page web, afin que celui-ci soit exécuté sur le poste de l'utilisateur dans le contexte de sécurité du site vulnérable. Pour ce

faire, il lui suffit de remplacer la valeur du texte destiné à être affiché par un script, afin que celui s'affiche dans la page web. Pour peu que le navigateur de l'utilisateur soit configuré pour exécuter de tels scripts, le code malicieux a accès à l'ensemble des données partagées par la page web de l'utilisateur et le serveur (cookies, champs de formulaires, etc.).

3 Attaque man in the middle

L'attaque « **man in the middle** » (littéralement « attaque de l'homme au milieu » ou « attaques de l'intercepteur »), parfois notée MITM, est un scénario d'attaque dans lequel un pirate écoute une communication entre deux interlocuteurs et falsifie les échanges afin de se faire passer pour l'une des parties.
La plupart des attaques de type « man in the middle » consistent à écouter le réseau à l'aide d'un outil appelé sniffer.

4 phishing avec pièces jointes

Une tendance lourde est actuellement en cours chez les phisheurs. De plus en plus d'arnaques mettent en jeu un message frauduleux accompagné d'une pièce jointe comprenant le formulaire de vol d'informations.

La SNCF a été victime récemment d'une attaque de phishing de ce type, avec un message potentiellement à même de tromper un certain nombre internautes.

Evidemment, le piège demeure plus aisément identifiable si vous n'avez pas commandé récemment de billets de train en ligne !

Des indices peuvent également permettre à un individu vigilant de déceler la tentative d'arnaque. Quelques fautes se sont en effet glissées dans les légères modifications textuelles effectuées par le pirate.

5 Phishing par virus (malwares)

Les keyloggers sont assez rare, les phisheurs installent un programme sur l'ordinateur de la victime qui enregistre tous ce qui est tapé au clavier y compris les mots de passes.
Pour lutter contre ce type de piratafe il faut avoir un antivirus de qualité, et surtout un PC mis à jours!

6 Phishing par fenêtres pop-up

Durant l'utilisation d'un site de confiance sécurisé, une fenêtre pop-up s'affiche invitant l'internaute à réinscrire son identifiant et son mot de passe. Une fois les informations validées, l'instigateur de l'attaque peut les réutiliser.

Ce type d'attaque utilise, généralement, un script javascript. Il est techniquement possible pour un script Javascript de déclencher une action si le site prédéterminé est visité en même temps que le site contenant le script. Si c'est le cas, le script javascript se déclenche et ouvre la pop-up. Cette attaque est notamment basée sur la faille de Cross Site Scripting.

1.7 Utilisation de bar d'adresses

De nombreux sites web d'hameçonnage désactivent la "barre d'adresse" du navigateur, ce qui signifie que vous ne pouvez pas voir l'adresse du site web que vous visitez. Ceci est délibéré, afin que vous ne remarquiez pas que le site que vous consultez est contrefait et n'a pas la bonne adresse.

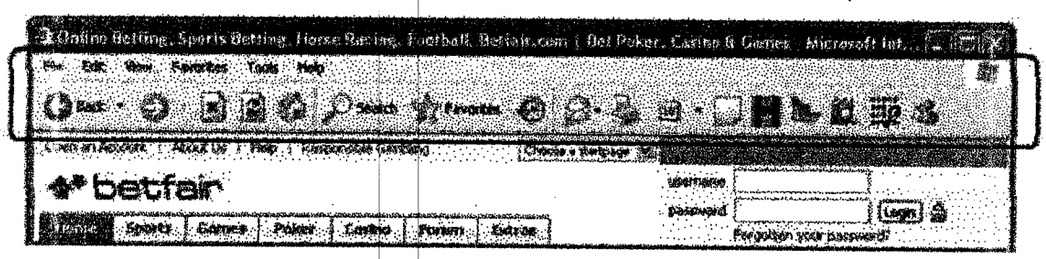


Figure2.1 :Désactivation de la barre d'adresses.

III LES SOLUTIONS

1 Contrôle d'intégrité

Lorsqu'un serveur a été compromis, le pirate masque généralement son passage en supprimant les traces dans les journaux d'activités. Par ailleurs, il installe un certain nombre d'outils lui permettant de créer une porte dérobée, afin d'être à même de pouvoir revenir ultérieurement.
Le pirate pense généralement à corriger la vulnérabilité lui ayant permis de s'introduire afin d'éviter que d'autres pirates s'infiltrent.
Sa présence sur un serveur peut néanmoins être trahie par un certains nombre de commandes d'administration permettant d'afficher la liste des processus en cours ou bien tout simplement les utilisateurs connectés à la machine. Il existe ainsi des logiciels, appelés rootkits, chargés d'écraser la plupart des outils du système et de les remplacer par des commandes équivalentes masquant la présence du pirate.
Il est donc aisé de comprendre qu'en l'absence de détérioration il peut être très difficile pour un administrateur de s'apercevoir qu'une machine a été compromise. Une des premières actions lors de la découverte d'une compromission consiste à dater la compromission afin d'évaluer l'étendue potentielle sur les autres serveurs.
En effet, d'une manière générale les serveurs stockent dans des fichiers une trace de leur activité et en particulier des erreurs rencontrées.
Or, lors d'une attaque informatique il est rare que le pirate parvienne à compromettre un système du premier coup. Il agit la plupart du temps par tâtonnement, en essayant différentes requêtes.
Ainsi la surveillance des journaux permet de détecter une activité suspecte. Il est en particulier important de surveiller les journaux d'activité des dispositifs de protection car tout aussi bien configuré qu'il soit, il se peut qu'ils soient un jour la cible d'une attaque.

2 Analyse de la présence de rootkits

Il existe certains logiciels (chkrootkit par exemple) permettant de vérifier la présence de rootkits sur le système. Néanmoins, afin de pouvoir utiliser ce type d'outils, il est essentiel d'être certain de l'intégrité de l'outil et de l'affichage qu'il délivre. Or, un système compromis ne peut pas être considéré comme fiable.

3 Analyse d'intégrité

Afin de s'assurer de l'intégrité d'un système, il est donc nécessaire de détecter les compromissions en amont. C'est ainsi l'objectif poursuivi par les contrôleurs d'intégrité tel que Tripwire.

Le logiciel Tripwire, développé à l'origine par Eugène Spafford et Gene Kim en 1992, permet d'assurer l'intégrité des systèmes en surveillant de façon permanente les modifications apportées à certains fichiers ou répertoires. Tripwire effectue en effet un contrôle d'intégrité et maintient à jour une base de signature. A intervalles réguliers il inspecte notamment les caractéristiques suivantes des fichiers afin d'identifier les modifications et les éventuelles compromissions :

- permissions
- date de dernière modification
- date d'accès
- taille du fichier
- signature du fichier

Les alertes sont envoyées par courrier électronique, de préférence sur un serveur distant, afin d'éviter tout effacement de la part du pirate.

* Limites du contrôle d'intégrité

Afin de pouvoir s'appuyer sur les résultats d'un contrôleur d'intégrité il est essentiel d'être sûr de l'intégrité de la machine lors de l'installation. Il est également très difficile de configurer ce type de logiciel tant le nombre potentiel de fichiers à surveiller peut être important. De plus, lors de l'installation de nouvelles applications il est indispensable de mettre leurs fichiers de configuration sous contrôle.

Par ailleurs, ce type de solution est susceptible d'envoyer un grand nombre de fausses alertes, notamment lorsque le système modifie seul des fichiers de configuration ou lors de mises à jour du système.

Enfin, si la machine est effectivement compromise, il est possible que le pirate tentera de compromettre le contrôleur d'intégrité avant la prochaine mise à jour, d'où l'importance de stocker les alertes sur une machine distante ou bien un support externe non réinscriptible.

4 Listes noires

Jusqu'à aujourd'hui, la « liste noire » est sous-doute la technique de filtrage la plus commune (que la solution soit positionnée ou non sur le poste client). La logique de cette technique consiste à « marquer » certaines certains domaines dont il est risqué d'accéder.

Le problème posé par cette approche est que les utilisateurs doivent maintenir manuellement et/ou mettre régulièrement à jour leur liste noire auprès d'une base de données centralisée afin de toujours posséder la dernière version de la liste des « sites illégitimes ». De plus, cette technique peine en réalité à bloquer toutes les adresses, parce que les phisheurs peuvent trop facilement ouvrir d'autres sites, et rendent ainsi la liste noire inutile.

Il existe aussi des listes noires, mais basée sur le contenu des messages : l'exercice consiste à classifier certains mots-clés comme étant illicites et bloquer les emails qui contiennent ces mots.

En quelques mots, nous pouvons définir les listes "blanches" et "noires" de la manière suivante : les expéditeurs en liste noire sont bloqués et les expéditeurs en liste blanche sont les bienvenus.

Les listes noires sont les listes ayant identifié des spams collectifs et sont listés afin de ne pas les délivrer.

Sur le même principe que les listes blanches, il y a des listes noires "locales", et des listes noires générales, communément appelées les RBL(RBL ou Realtime Blackhole)

La RBL est une liste noire de machines ou de domaines bannis, mise à jour en temps réel.

III.1 LE FILTRAGE

3. LES TECHNIQUES TRADITIONNELLES DE FILTRAGE

Avant de parler technologie, voyons en premier lieu les différents types d'architecture pour un système utilisant une messagerie protégée par un antiphishing.

3.1 Le positionnement du filtre : deux types d'approche

Le phishing a une forte liaison avec le spam car le phishing est un spam qui a pour but de voler vos informations confidentielles même si le phishing est un peut plus specifique et cible des utilisateurs plus précis que le spam qui est un peut général. Nous observe classiquement deux types de scénarios :

1) Le filtrage antiphishing « à la demande ». Le filtre antiphishing est positionné sur un serveur proxy.

Le filtrage est alors automatique et transparent.

2) Le filtrage « vérificateur ». La solution antispam s'interpose entre l'utilisateur et le serveur POP, qu'elle scrute périodiquement.

Les deux types de scenarii et leurs points forts/faibles sont mis en valeur dans la figure ci-dessous :

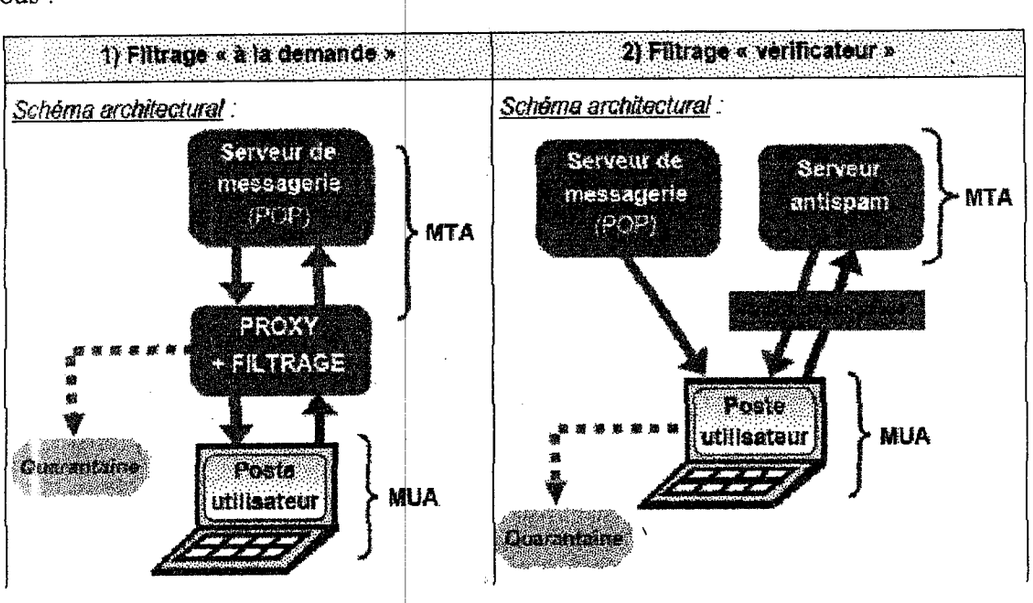


Figure 2.2 :Filtrage antiphishing/antispam.

1 Installation d'un logiciel antiphishing

Qui veut offrir une solution antiphishing à son serveur de messagerie peut l'installer en tant que logiciel en local se comportant comme une « passerelle de messagerie ». Pour ce faire, il faut s'assurer que ce dernier est le premier à recevoir le courrier destiné au serveur de messagerie (courrier entrant), ainsi que le dernier pour le courrier en partance (courrier

sortant). Cette installation est aussi connue sous le nom de « Smart host » (Hôte Actif). Le schéma architectural suivant montre qu'une telle solution antiphishing s'apparente généralement à un serveur-relais de courrier :

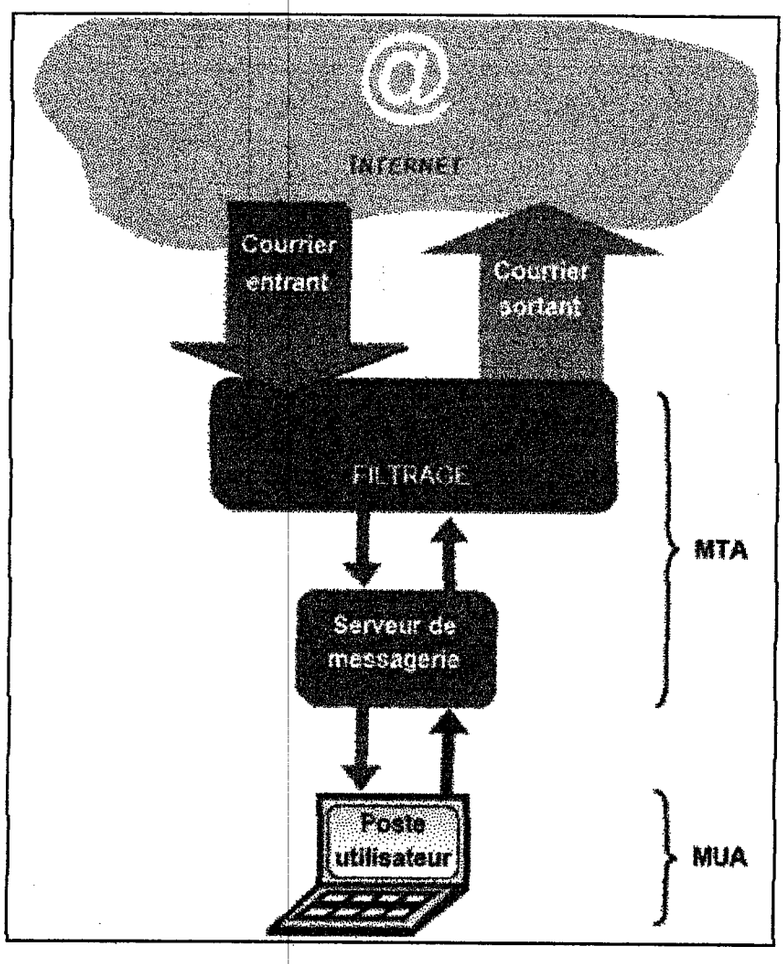


Figure2.3 :

Au passage, il faut noter qu'un bon nombre de logiciels antivirus s'interposent d'une façon équivalente entre le courrier entrant/sortant et le serveur de messagerie. On trouve même de nombreuses solutions intégrant à la fois la fonction d'antispam et d'antiphishing. On peut citer en exemple l'outil ProtecMail

ProtecMail. Ce dernier, situé sur Internet, sait auprès de quel serveur de messagerie (niveau MTA) récolter les mails susceptibles de contenir des spams ou des virus.

L'avantage de ce type de service est double. D'une part, il permet à ses bénéficiaires d'éliminer une majorité de spam avant leur téléchargement, ce qui diminue leur temps de connexion (ce qui n'est pas négligeable pour les utilisateurs d'un modem téléphonique 56Kb/s). D'autre part, il n'y a ni logiciel à installer, ni de mises à jour régulières à planifier : il

suffit juste de paramétrer ce service une fois pour toutes. En revanche, un inconvénient des services de filtrage en ligne est de rendre difficile, voire impossible, la maîtrise du filtrage des courriels.

3.2 Les listes blanches/noires, base des procédés de filtrage traditionnels

La politique de liste blanche et de liste noire n'est pas propre au domaine de la lutte antiphishing : les serveurs proxy des entreprises en sont souvent pourvus afin de restreindre l'accès vers les sites web n'étant pas jugés en relation avec l'activité professionnelle exercée. Dans ce cas, l'expression « liste noire » désigne une liste contenant les URLs interdites. Au contraire, l'expression « liste blanche » contient les URLs autorisées. Ce concept impose souvent un compromis entre le coût d'entretien de la liste blanche par les administrateurs de l'entreprise et la perte engendrée18 par le fait que certains sites ne sont pas couverts par la liste noire. Il faut évaluer la taille d'une liste blanche, ainsi que son évolution dans le temps. Quant aux listes noires, elles sont mises à jour régulièrement, et, le plus souvent, par des sociétés spécialisées fournissant ce service.

1 Les listes blanches

Le filtrage de phishing par liste blanche, comme par listes noires, nécessite l'usage d'un outil spécifique qui permet à la fois des mises à jour fréquentes et une personnalisation possible du contenu de ces listes.

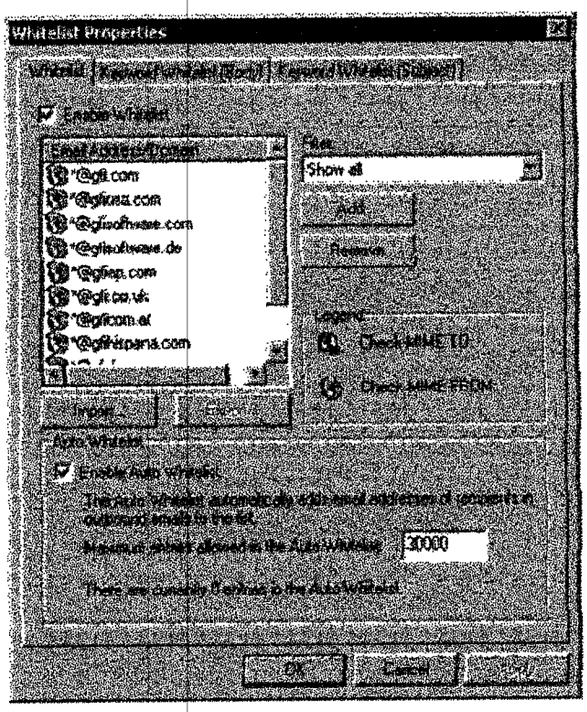


Figure2.4 : Gestion de la liste blanche.

L'inconvénient des listes blanches est que le destinataire doit traiter manuellement les messages provenant d'expéditeurs inconnus.

Il n'est jamais conseillé de compter uniquement sur les listes noires ou listes blanches. En effet, ces méthodes ne se sont pas gérables pour ceux qui reçoivent une grande quantité de messages provenant de personnes inconnues. Cependant, la technologie en elle-même n'est pas complètement inutile.

Elle peut être utilisée en complément à d'autres technologies pour améliorer les taux de détection et rendre les produits anti-phishing plus simples d'utilisation et plus personnalisables.

3.3 L'analyse par mots-clés

La correspondance par mots-clés est une très ancienne méthode. Elle marque le site en tant que dangereux si certains « mots suspects » sont détectés, et les marque plus favorablement en légitime si certains « bon mots » sont trouvés.

Cette approche implique d'analyser le corps de la page pour des mots-clés spécifiques et des expressions. Ces mots sont en effet peu susceptibles d'apparaître dans une correspondance

professionnelle classique. Mais l'analyse de mot-clé en tant que solution antiphishing autonome est une technique très primitive, car :

- Elle produit un taux élevé de faux-positifs.
- Il est possible pour les spammeurs d'abandonner certains mots-clés et d'en utiliser d'autres pour exprimer la même chose.
- Elle ne peut rien contre les mots suspects incorporés dans des images... À moins, bien sûr, de disposer d'un produit antiphishing avec reconnaissance de caractères intégrée, mais ce n'est apparemment pas proposé sur le marché à ce jour.

3.4 L'analyse lexicologique

Une problématique se pose fréquemment dans la lutte antiphishing : la présence d'un mot ou d'une expression suspecte par elle-même ne signifie pas nécessairement que le site en question est frauduleux : il faut donc éviter qu'il soit reconnu frauduleux. À la différence de l'analyse par mots-clés, l'analyse lexicologique analyse le contexte de tous les mots et les expressions dans un domaine particulier. À chaque mot ou expression est assigné un poids qui dépend principalement du contexte dans lequel on le trouve.

3.5 Le filtrage bayésien

Le filtrage bayésien est une technique dite adaptative, qui reflète notre propre définition de ce qu'est et n'est pas un phishing. Il se situe parmi les techniques de détection du phishing les plus efficaces, ce qui le rend très populaire. Ce que l'on appelle la « classification naïve bayésienne » ne date pas d'aujourd'hui, mais de 1763, basée sur la théorie statistique du scientifique anglais T. Bayes.

Le principe de tout filtre bayésien est d'apprendre par les exemples. En effet, lors d'une première utilisation, il peut paraître insatisfaisant. Cependant, après quelques jours d'entraînement, il devient extrêmement précis. Bien que l'entraînement puisse être légèrement gênant, comparé aux efforts requis par les autres méthodes, cela reste trivial, et les avantages pèsent bien plus lourd que le coût exigé.

L'intérêt incontestable de cette méthode est qu'elle bénéficie d'un taux élevé de détection de phishing, tout en garantissant un nombre très bas de faux-positifs, les filtres bayésiens bloquent plus de 96% des sites de phishing, avec 0,9% de faux-positif. Une solution comme 'GFI MailEssentials' à base de filtre bayésien, estime son taux de reconnaissance du phishing à 98% après une période de seulement deux semaines.

* Fonctionnement d'un filtre bayésien

Imaginons un courrier candidat au filtrage bayésien. Supposons que ce courrier contienne certains mots qui avaient déjà été repérés auparavant dans des courriers considérés comme *spam*.

Supposons également que ces mots ne sont encore jamais apparus dans un courrier valide. Alors, il est légitime de considérer que ce courrier électronique est un spam ou phishing.

C'est ainsi qu'un filtre bayésien accumule sans cesse les résultats de ses analyses, qui sont eux mêmes utilisés par la suite pour aider à démasquer des courriers futurs, comme le montre le *schéma suivant* :

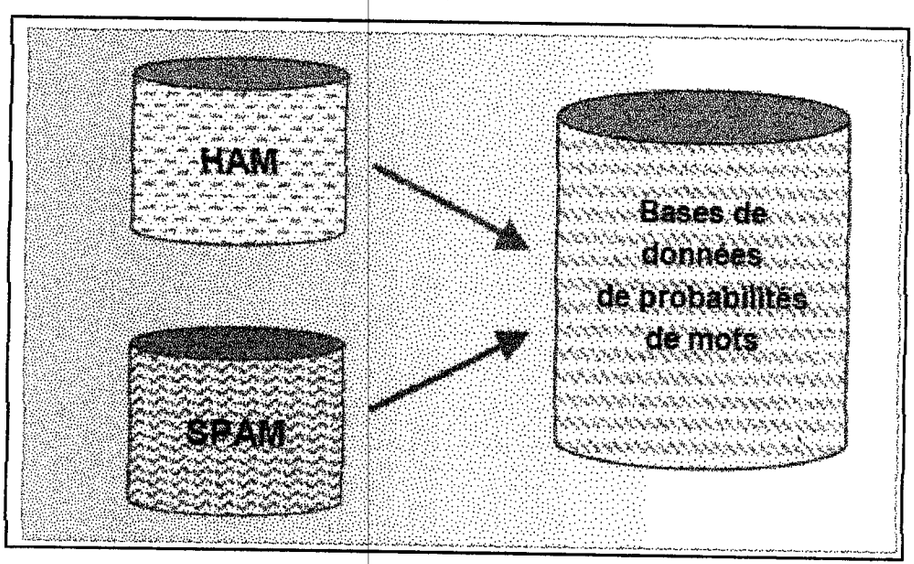


Figure 2.5 : La base de données probabiliste.

C'est une valeur de probabilité qui est affectée à chaque mot ou unité lexicale. Celle-ci est basée sur des calculs qui tiennent compte du nombre de fois que ce mot se présente en tant que spam, par opposition au « ham » qui est le courrier valide. Cela se fait en analysant d'une

part le courrier sortant des utilisateurs, et d'autre part les spams connus : tous les mots et unités lexicales des deux regroupements de courrier sont analysés pour définir la probabilité pour qu'un courrier soit un spam.

Cette probabilité par mot est calculée de la façon suivante : si par exemple le mot « mortgage »21 apparaît dans 400 des 3.000 messages phishing, et dans 5 des 300 messages légitimes, alors sa probabilité d'être un phishing serait de 0,8889. (22)

Il est alors logique de concevoir qu'un filtre bayésien a besoin d'un minimum de temps pour devenir pleinement efficace. C'est ce que l'on appelle le « temps d'apprentissage » du filtre bayésien. Le produit GFI MailEssentials est un exemple de solution antiphishing utilisant le filtre bayésien comme technique de défense principale. En effet, la société GFI recommande de laisser au filtre le temps de s'adapter à sa messagerie pendant au moins une semaine, durant laquelle l'utilisateur est sollicité pour aider le système à classifier le courrier en « spam / pas spam ». Selon GFI, c'est seulement après cette période qu'il devient utile d'activer le filtrage.

1 La mise à jour d'une base de données bayésienne

Beaucoup de logiciels à base de filtre bayésien rendent possible d'utiliser une mise à jour de dictionnaires de probabilités de mots à partir d'un serveur centralisé sur Internet, donc commun aux entreprises du monde entier qui utilise ce logiciel. Cela revient du partage d'informations.

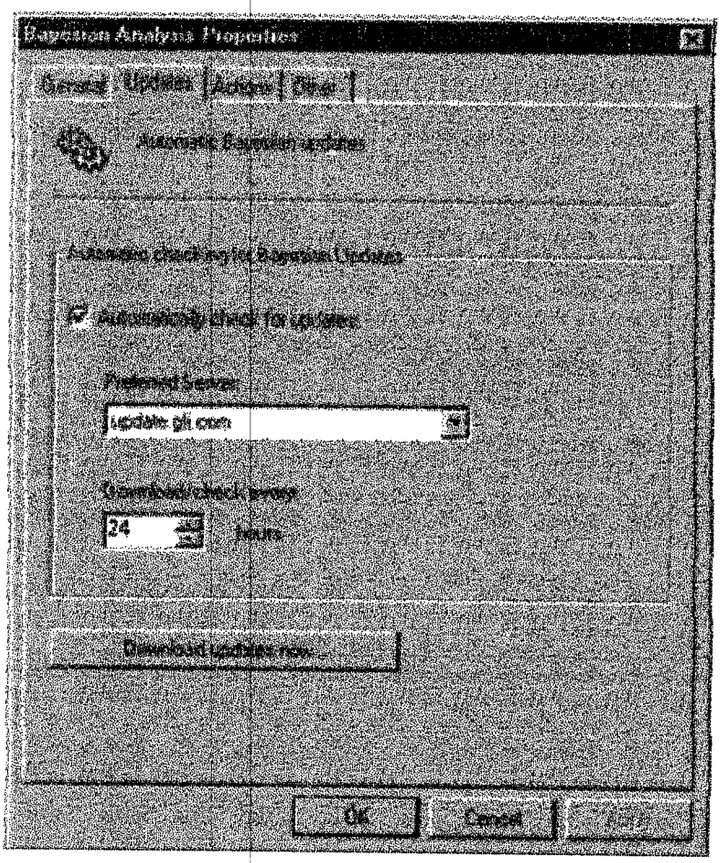
part le courrier sortant des utilisateurs, et d'autre part les spams connus : tous les mots et unités lexicales des deux regroupements de courrier sont analysés pour définir la probabilité pour qu'un courrier soit un spam.

Cette probabilité par mot est calculée de la façon suivante : si par exemple le mot « mortgage »21 apparaît dans 400 des 3.000 messages phishing, et dans 5 des 300 messages légitimes, alors sa probabilité d'être un phishing serait de 0,8889. (22)

Il est alors logique de concevoir qu'un filtre bayésien a besoin d'un minimum de temps pour devenir pleinement efficace. C'est ce que l'on appelle le « temps d'apprentissage » du filtre bayésien. Le produit GFI MailEssentials est un exemple de solution antiphishing utilisant le filtre bayésien comme technique de défense principale. En effet, la société GFI recommande de laisser au filtre le temps de s'adapter à sa messagerie pendant au moins une semaine, durant laquelle l'utilisateur est sollicité pour aider le système à classifier le courrier en « spam / pas spam ». Selon GFI, c'est seulement après cette période qu'il devient utile d'activer le filtrage.

1 La mise à jour d'une base de données bayésienne

Beaucoup de logiciels à base de filtre bayésien rendent possible d'utiliser une mise à jour de dictionnaires de probabilités de mots à partir d'un serveur centralisé sur Internet, donc commun aux entreprises du monde entier qui utilise ce logiciel. Cela revient du partage d'informations.



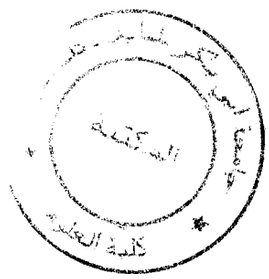


Figure 2.6 : La mise à jour de la base de données bayesienne

2 Les limites du filtrage bayésien

Si les filtres bayésiens sont actuellement réputés pour leur efficacité, cela ne durera peut-être pas :

- La phase d'apprentissage d'un filtre bayésien dure souvent longtemps.
- Ils sont facilement contournables par les pirates et ne peuvent pas analyser les sites dans toutes les langues, et particulièrement ceux à base d'images
- Ces filtres sont inefficaces contre la fraude. Par exemple, un spam connu est celui d'une fausse banque (Citibank) nous conviant à saisir sur leur site notre numéro de carte bleue ainsi que notre code confidentiel. De plus, ce spam est à base d'image, ce qui nous renvoie de toute façon à l'inconvénient détaillé dans le point précédent. Ceux qui sont en mode texte contiennent un vocabulaire commercial non suspect, et n'ont donc pas de raison d'être interceptés par un filtre bayésien.

- Les filtres bayésiens sont souvent utilisés avec une mise à jour régulière auprès d'une base de données centralisée commune à tous les utilisateurs d'un même produit. C'est un probleme, car là se situe justement l'intérêt d'un filtre bayésien : pouvoir s'adapter à un contexte unique.

3.6 Sécurisation de la session

Avec la plupart des navigateurs Web, tels que Microsoft Internet Explorer et Netscape Navigator, l'affichage d'une icone de cadenas fermé ou d'une clé non brisée dans le coin inférieur droit ou gauche de la fenêtre du navigateur signale une session chiffrée et sécurisée. Vous pouvez également vérifier la barre d'adresse de votre navigateur. Si l'adresse du site commence avec un « https:// » plutôt qu'avec le « http:// » habituel, alors la session est sécurisée.

3.7 Détection de la langue

Il faut citer en dernier lieu, l'adaptation multi-langues d'un filtre antispam, ce qui est de plus en plus requis étant donné que le spam est de moins en moins anglophone en proportion par rapport aux quantités de spams envoyés dans le monde.

Reprenons à titre d'exemple le même logiciel (GFI MailEssentials) et, plus précisément, l'onglet 'langages' dans la boîte de dialogue de ses propriétés du contrôle d'en-tête. Celle-ci contient les options de détection de langue :

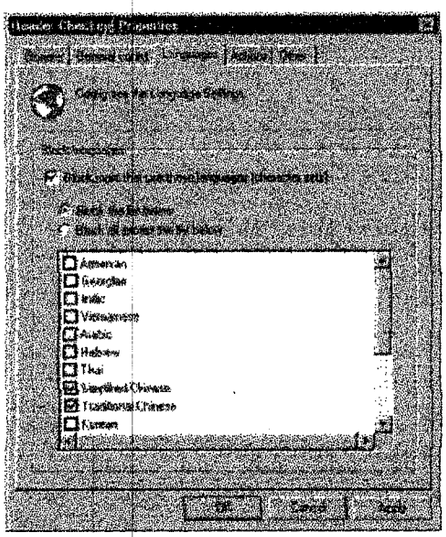


Figure2.7 :Blocage de langages dans le filtre antiphishing.

Beaucoup de ces courriers indésirables ne sont même pas dans la langue de l'utilisateur, ce qui signifie qu'ils peuvent très simplement réduire le spam en bloquant le courrier écrit en chinois ou en vietnamien, par exemple. En fait, avec ce critère on peut bloquer le courrier selon qu'il utilise tel ou tel jeux de caractères : GFI MailEssentials, par exemple, ne peut pas distinguer l'italien du français parce que ces deux langues utilisent le même jeu de caractères… ce qui, d'un certain point de vue, constitue une limite.

4. DES APPROCHES COMPLÉMENTAIRES AUX FILTRES TRADITIONNELS

À l'image des tentatives de traque des spammeurs (qui, au demeurant, se révèlent inefficaces) il existe des moyens de lutte contre le spam complémentaires aux techniques traditionnelles de filtrage exposées précédemment dans ce rapport. Cela peut aller de simples recommandations sur les habitudes à prendre en tant qu'utilisateur, jusqu'aux méthodes récentes (brevetées ou non) de filtrage du spam.

4.1 Confirmation de l'expéditeur (Challenge Response)

C'est une astuce devenue relativement populaire : l'idée est d'envoyer un "challenge" à l'expéditeur du message, lequel devra y répondre. Si une réponse est reçue, l'expéditeur est ajouté à la liste blanche et ne sera plus questionné. Dans le cas contraire, les messages de cet expéditeur ne seront plus affichés dans la boîte de réception, car mis en liste noire.
Cependant, la recommandation est de ne jamais utiliser cette méthode, car, quoi qu'en disent les partisans de cette technologie ou l'impression positive qu'elle peut laisser, ce n'est pas un moyen sûr. Cette technique a des conséquences fortement indésirables ; voici une liste non exhaustive des inconvénients de la technique challenge-response :
- Elle est inamicale et impolie pour les expéditeurs légitimes ;
- Les expéditeurs légitimes peuvent, à l'occasion, utiliser une autre adresse email, qui elle n'a pas été ajoutée à la liste blanche. Elle aussi devra être confirmée, ce qui est encore plus frustrant ;
- Les expéditeurs légitimes peuvent oublier de répondre ou recevoir le message seulement quelques jours plus tard, lorsqu'ils sont en déplacement ou n'ont pas accès à leurs ordinateurs.

Dans ce cas, le message original (éventuellement très important) peut être significativement retardé ;

- Si l'expéditeur et le destinataire installent tous deux un logiciel basé sur le principe de confirmation, ils pourraient obtenir une boucle sans fin de confirmations, laquelle paralyserait le système ;

- Les messages provenant de services automatiques, telles les confirmations d'enregistrement ou de transaction (utilisées par des sites comme Amazon ou e-Bay), ne parviendront jamais à atteindre la boîte de réception de l'utilisateur : les messages de ce type sont envoyés par des robots... qui ne répondent jamais aux confirmations ;

- Les souscripteurs de bulletins d'informations seront bombardés de messages de confirmation

- Pour les gros FAI, les nombreux messages de confirmation doubleront leur trafic et pénaliseront significativement leurs systèmes. C'est certain que ces FAI ne seraient pas très heureux de voir leurs systèmes, déjà bien lésés, doublement alourdis à cause des spammeurs.

Steve Atkins, un consultant antispam à Redwood City, Californie, affirme ce qui suit (traduit de l'anglais) : « Cette technologie est suffisamment tentante pour que les gens l'utilisent et ne réalisent pas toutes les mauvaises choses qui commenceront à se produire ». Ainsi, si l'on est très heureux de voir sa boîte de réception propre après avoir utilisé cette technique, il est très souhaitable d'examiner

la liste ci-dessus afin de voir si on n'est pas affecté d'une quelconque façon par un de ces inconvénients.

Réfléchir à deux fois, donc, avant d'utiliser cette trouvaille aux effets souvent indésirables.

4.2 Se désabonner ou invalider les messages (Bounce back)

Certains produits antiphishing offrent la possibilité de renvoyer à l'expediteurs les messages non désirés, spécifiant que l'adresse email est fausse ou n'existe pas, et dans l'espoir d'être retiré de sa liste de diffusion. Mais cette méthode peine à stopper le phishing, car d'une part les spammeurs ne vérifient pas les emails retournés, et d'autre part cela confirme que l'adresse destinataire existe, cela peut donc empirer le phénomène. De plus, dans les cas « d'usurpation d'adresse », cela risque de polluer des innocents, puisque l'adresse de l'expéditeur peut être celle d'un ami qui, lui, n'a pas envoyé ce message. Il n'est donc pas particulièrement conseillé d'utiliser cette méthode.

4.3 Réseaux anti-phishing collaboratifs

Les partisans de la technologie antiphishing collaborative affirment que les expediteurs envoient généralement le même message à des millions de personnes. Ainsi, si un utilisateur trouve un message de phishing, il peut utiliser un « réseau communautaire » afin d'envoyer une "signature" du message à tous les utilisateurs ayant souscrit au même service. L'intérêt c'est que l'action d'un utilisateur empêchera les autres utilisateurs d'être dérangés par le même message.

Cette technologie fonctionne. Elle comporte cependant quelques inconvénients :

1) Le taux de détection des réseaux communautaires n'est pas toujours aussi élevé qu'il est sensé l'être.

4.4 La technologie ne suffit pas : précautions de base

On ne sera pas sans rappeler l'importance de « prévenir plutôt que guérir », et cet autant que possible. Dans le domaine de la lutte antiphishing, certaines précautions de bases devraient être en effet le réflexe de tout utilisateur de courrier électronique. Elles sont les suivantes :

- La première des recommandations aux utilisateurs est de ne pas cliquer sur un lien suspect.
- Éviter de communiquer son adresse e-mail sur un site dont on n'est pas sûr. Sinon, c'est prendre inévitablement le risque qu'elle finisse un jour dans les mains des phisheurs. Ainsi, si on est amené à communiquer son adresse électronique pour bénéficier d'un service, recevoir des bulletins d'information, effectuer un achat en ligne ou accéder à une partie à accès restreint d'un site Web, il faut à tout prix être prudent, et donner le moins possible son adresse.
- Utiliser une adresse jetable. Pour éviter toute pollution de son adresse principale, il est bon d'en avoir une qui soit annexe, ou temporaire (qui s'autodétruit ou que l'on supprime manuellement).

4.5 Laisser la main aux utilisateurs

Malgré une automatisation certaine du filtrage du spam rendu possible par des outils comme les filtres bayésiens, il est toutefois utile pour les administrateurs de laisser le contrôle aux utilisateurs, en leur permettant de faire savoir au système ce qu'ils considèrent, eux, comme spam. C'est en particulier lors de la phase d'apprentissage d'un filtre bayésien que cette étape

est hautement recommandée. De la même façon, si un système laisse les utilisateurs ajouter eux-même leurs sites préférés à des listes blanches, alors le risque de faux-positifs sera diminué.

4.6 Utilisation des certificats numériques

Les certificats numériques sont délivrés par des autorités de certification soumis à des vérifications et à des contrôles intensifs avant d'authentifier un site Web ou les éléments qu'il contient. Ce certificat identifie l'origine du site, tout en vérifiant que le site n'a subi aucune violation. Lorsque votre navigateur Web est assorti d'un certificat, il vérifiera si celui-ci a été délivré par une autorité de certification légitime.
S'il y a correspondance, votre session se poursuivra. Autrement, votre navigateur affichera un avertissement et l'annulation de la session sera le geste le plus sûr à poser.

4.7 Sécurisation de liaison entre utilisateur et le site

Les navigateurs Web utilisent des protocoles de sécurité standard, tels que le protocole SSL (couche de sockets sécurisés) et le protocole S-HTTP sécuritaire pour permettre la transmission sécuritaire de l'information de nature privée sur Internet. Lorsque vous visitez un site Web utilisant un protocole SSL, une connexion sécuritaire est créé entre votre ordinateur et le serveur du site Web en question. Une fois la connexion établie, vous pouvez transmettre toute l'information voulue au serveur Web en toute sécurité. Le protocole S-HTTP est au contraire conçu pour l'envoi sécuritaire de messages uniques.

V CONCLUSION

Pour ce chapitre nous avons vu de manière générale la pratique du phishing, ainsi que son forte relation avec le spam vis-à-vis les méthodes de propagation

Nous avons vu les différents types d'attaques utilisées pour détourner l'attention des utilisateurs comme l'empoisonnement du cache, la désactivation des barres d'adresses.

Pour la deuxième partie du chapitre nous avons vu un nombre de solutions qui peut aider les utilisateurs à éviter de tomber dans le piège du phishing.

Pour le prochain chapitre nous allons développer un coté des solution et l'implémenter en pratique.

CHAPITRE III

APPLICATION

I INTRODUCTION

Les pages de phishing sont l'un des problèmes majeurs de sécurité sur internet. La majorité des attaques utilisent des méthodes sophistiquées comme les fausses pages pour tromper les utilisateurs afin d'acquérir des informations sensibles.

La méthode la plus simple pour éviter la visite des sites frauduleux est l'utilisation des listes noires si ces listes sont maintenues a jour immédiatement âpres qu'un site frauduleux est créé ce qui est pratiquement impossible a mettre en place.

Dans ce chapitre nous allons étudier une méthode pratique d'anti-phishing, ce qui consiste à un système de classification automatique.

II APPROCHE

Pour l'application nous avons utilisé l'approche d'analyse d'URLs pour dire qu'un site est sans risque sans avoir a examiner son contenu, cette approche cherche a éviter de télécharger le contenu puis faire l'analyse ce qui crée une importante latence qui dérange l'utilisateur.

L'URL tout seul peut contenir un lot important d'informations qui nous donne la possibilité de juger d'une façon proactive son contenu.

Nous avons réalisé un système de classification qui peut analyser une base d'URLs étiquetés selon un nombre d'heuristiques qui peuvent détecter les techniques utilisées pour tromper les utilisateurs.

* La présence de formes : Le but d'un site de phishing est d'avoir les informations de la victime ce qui se fait par l'utilisation de formes d'input. Ce paramètre peut être utilisé comme un pré filtre « s'il y a des formes d'input nous faisons l'analyse sinon pas la peine de faire ».

* L'âge du domaine : En général les sites de phishing on une très courte durée de vie avant qu'ils soient fermés par leurs hébergeurs a cause des plaintes d'utilisateurs et des

autorités, alors on peut prendre une durée de vie minimum pour dire qu'un site est sur ou pas.

* La longueur d'URL : Les sites de phishing utilisent deux façons pour tromper les utilisateurs, des URLs avec une importante longueur pour cacher la vraie adresse, dans d'autres cas on utilise des URLs réduites (comme le fait TinyURL.com) pour cacher la vraie adresse et passer l'analyse de la longueur.

Nous avons prit la longueur comme paramètre entier.

* Adresses avec IP : pour détourner l'attention des utilisateurs on utilise des adresses avec juste un IP, ce qui n'est pas très évident pour une importante compagnie qui n'a pas un nom de domaine.

Un paramètre booléen pour designer si l'adresse contient un IP affecter par la valeur 1 sinon 0.

* Points dans l'URL : Les adresses de phishing contiennent généralement un nombre de sous-domaines pour que l'url apparaisse légitime.

Nous avons pris la valeur 3 comme paramètre de division entre phishing ou pas car une valeur importante de nombre de point indique un ou plusieurs sous-domaines.

* Niveau de sécurité : L'utilisation de protocoles sécurisés est un facteur important pour dire est ce sur de visiter un lien ou pas malgré qu'il y a des sites de phishing avec https.

Notre système cherche si l'adresse est sécurisée alors il affecte au paramètre la valeur 1 (pour https) sinon il l'affecte un 0 (en cas de http, ftp ou encas d'absence de protocole dans le lien).

* Caractères spéciaux '@','-' ,'_' : On peut faire une redirection directe d'une adresse a une autre a l'aide de '@', et on utilise '-','_' pour faire faire une adresse ressemblante a la légitime.

Nous avons pris la valeur 1 comme paramètre de division (1 si le nombre est supérieur à 1, 0 sinon).

* Modification d'encodage d'URL: Pour détourner l'analyse on modifie les URLs en changeant des caractères par leurs codes html %20 pour un espace par exemple.

Nous avons pris la valeur 1 comme paramètre de division (1 si le nombre est supérieur à 2, 0 sinon).

III BASE D'URLS UTILISEE

Pour la base de d'URLs nous avons eu recours à une base publique utilisée par OPENDNS, cette base est publiée par leur site phishtank.com (phishtank.com est créé par OPENDNS) qui est un site ou les internautes peuvent signaler les sites suspects. La base rendue publique par le site est vérifiée par des experts qui disent que ces adresses sont effectivement des adresses de phishing. Nous avons utilisé deux versions avec des dates de sorties différentes pour plus de précision.

Pour la base des adresses sures nous avons utilisé, plusieurs sources comme ALEXA.com, et Google ranking spécialisés dans les statistiques du trafique sur internet et qui donnent le classement des sites les plus populaire périodiquement.

Pour le nombre d'instances de la base nous avons

6069 : adresses de phishing. 535 : adresses.

III-I STRUCTURE DE LA BASE DE PHISHING

La base de données est présente sous forme d'un fichier XML, avec les informations suivantes (un exemple d'instance) :

```
<url>http://aerospecialties.aerospecialties.com/osc22/mastercard.number/account.php</url>
<phish_id>1278385</phish_id>
<phish_detail_url>http://www.phishtank.com/phish_detail.php?phish_id=1278385</phish_detail_url>
<ip_address>209.161.24.98</ip_address>
<submission_time>2011-05-20T01:05:01+00:00</submission_time>
<verified>yes</verified>
<verification_time>2011-05-20T01:40:58+00:00</verification_time>
<online>yes</online>
<target>Mastercard</target>
```

Figure3.1 : Base de phishing sous forme XML.

phish_id : ID ou référence du site du phishing.

phish_detail_url : details sur phishtank du site en question.

url : L'url du site

submission_time : la date et l'heure de la déposition d'alarme sur le site.

Verified : site vérifier ou pas mais comme phishtank n'ajoute que les sites vérifies alors tous on une valeur :yes

verification_time : date et temps de vérification

online : statut du site

target : la compagnie ou la marque visée par l'attaque (visa, mastercard…)

IV ENVIRONNEMENT DU TRAVAIL

Pour le coté application de cette recherche nous avons travaillé avec DELPHI 7 Entreprise ce qui est un EDI édité par BORLAND, pour sa rapidité et la facilité de prendre en main, nous l'avons utilisé pour calculer les métriques prisent en considération.

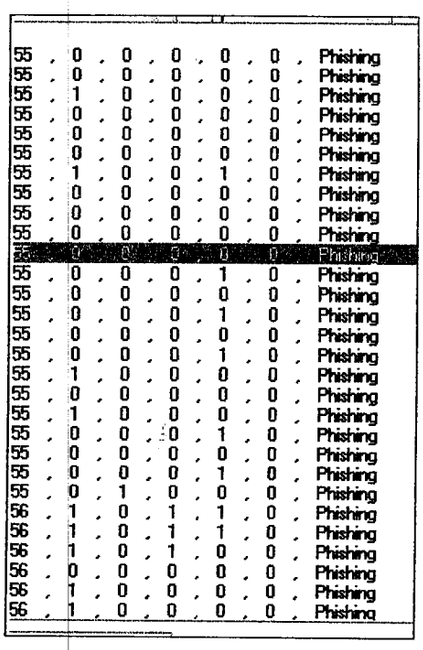
Nous avons utilisé aussi WEKA qui est un ensemble d'outils permettant de manipuler et d'analyser des fichiers de données, et qui implémente beaucoup d'algorithmes d'intelligence artificielle. Il est écrit en Java.

V FONCTIONNALITES DE L'APPLICATION

Notre application se constitue de deux parties majeures :

* La première partie (Partie développeur) : contient tout se qui a un lien avec le développement, ainsi nous trouvons l'interface pour le calcul des différents paramètres que nous avons vu précédemment.

* La deuxième partie (Partie utilisateur) : Une partie utilisée par l'utilisateur final, qui peut décider pour lui si c'est le site est légitime ou c'est un phish, son implémentation est une barre d'un navigateur web qui bloque l'accès aux sites sensibles



55	0	0	0	0	0	Phishing
55	0	0	0	0	0	Phishing
55	1	0	0	0	0	Phishing
55	0	0	0	0	0	Phishing
55	0	0	0	0	0	Phishing
55	0	0	0	0	0	Phishing
55	1	0	0	1	0	Phishing
55	0	0	0	0	0	Phishing
55	0	0	0	0	0	Phishing
55	0	0	0	0	0	Phishing
55	0	0	0	0	0	Phishing
55	0	0	0	1	0	Phishing
55	0	0	0	0	0	Phishing
55	0	0	0	1	0	Phishing
55	0	0	0	0	0	Phishing
55	0	0	0	1	0	Phishing
55	1	0	0	0	0	Phishing
55	0	0	0	0	0	Phishing
55	1	0	0	0	0	Phishing
55	0	0	0	1	0	Phishing
55	0	0	0	0	0	Phishing
55	0	0	0	1	0	Phishing
55	0	1	0	0	0	Phishing
56	1	0	1	1	0	Phishing
56	1	0	1	1	0	Phishing
56	1	0	1	0	0	Phishing
56	0	0	0	0	0	Phishing
56	1	0	0	0	0	Phishing
56	1	0	0	0	0	Phishing

Figure 3.2 : aperçu des résultats

VI EVALUATION

Pour la partie d'évaluation nous avons utilisé la suite de logiciel d'apprentissage automatique et d'exploration de données « WEKA », et ce pour avoir plusieurs classifieurs en main, faire la comparaison, et avoir une analyse claire des résultats.
Pour cela nous avons transformé le fichier de sortie de notre application en fichier ARFF de ce format

```
@RELATION phishing   % Nom de l'ensemble de données

@ATTRIBUTE longueur                numeric          % déclaration des
@ATTRIBUTE nombredepoints          {0,1}            % attributs et leurs
@ATTRIBUTE securiteduprotocol      {0,1}            % types
@ATTRIBUTE sansnomdudomaine        {0,1}
@ATTRIBUTE caracteresspeciaux      {0,1}
@ATTRIBUTE caracteresunicodes      {0,1}
@ATTRIBUTE class                   {Phishing,SUR}

@DATA                    % la partie data
55 , 0 , 0 , 0 , 0 , 0 , Phishing     % les instances avec leurs
55 , 0 , 0 , 0 , 0 , 0 , Phishing     % classes
55 , 1 , 0 , 0 , 0 , 0 , Phishing
55 , 0 , 0 , 0 , 0 , 0 , Phishing
55 , 0 , 0 , 0 , 0 , 0 , Phishing
55 , 0 , 0 , 0 , 0 , 0 , Phishing
31 , 0 , 0 , 0 , 0 , 0 , SUR
31 , 0 , 1 , 0 , 0 , 0 , SUR
31 , 0 , 1 , 0 , 0 , 0 , SUR
31 , 1 , 1 , 0 , 0 , 0 , SUR
32 , 0 , 0 , 0 , 0 , 0 , SUR
32 , 0 , 0 , 0 , 0 , 0 , SUR
32 , 0 , 0 , 0 , 0 , 0 , SUR
```

Figure 3.3 : fichier au format ARFF

VI-I RESULTATS SOUS WEKA

Nous avons utilisé plusieurs algorithmes d'apprentissage

* Arbres de décision.
* Classification bayesienne probabiliste (naïve bayes, réseaux bayesiens).

* Machine à vecteur de support(SVM).

Le tableau suivant résume les résultats obtenus avec ces classifieurs

	SVM(SMO)	Arbres (j48)	Randomtree	Réseaux bayesiens	Naïve Bayes
Instances correctement classées	6218 (94.1551 %)	6485 (98.1981 %)	6500 (98.4252 %)	6445 (97.5924 %)	6360 (96.3053 %)
Instances mal classées	386 (5.8449 %)	119 (1.8019 %)	104 (1.5748 %)	159 (2.4076 %)	244 (3.6947 %)

Tableau 3.1: Résultats de classification

Le graphe suivant compare le nombre d'instances correctement classées par rapport au nombre total d'instances.

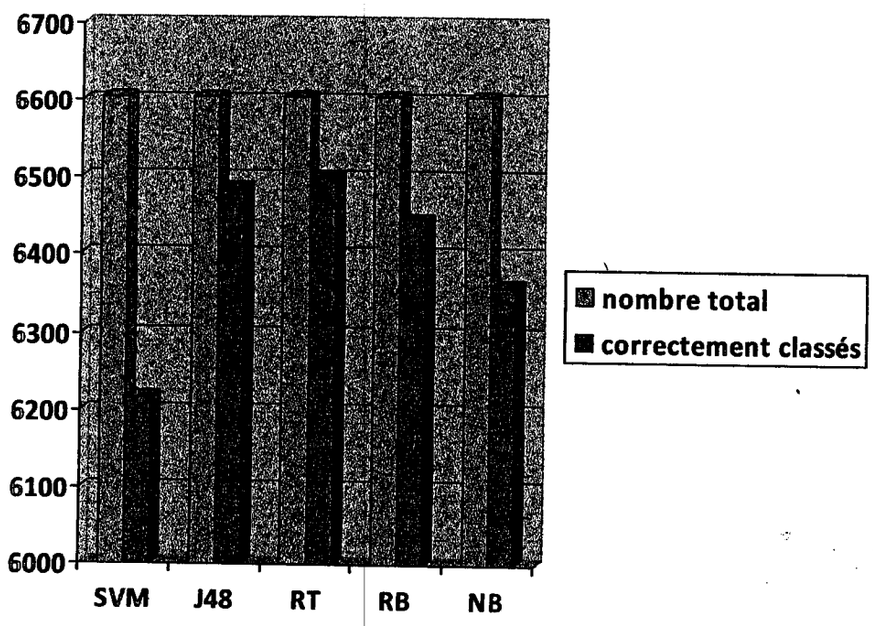


Figure 3.4: nombre d'instances correctement classifiées.

Le tableau suivant récapitule les valeurs de précision, les vrais positifs

	SVM(SMO)		Arbres (j48)		Randomtree		Réseaux bayesiens		Naive Bayes	
Classe	phishing	sur	phishing	sur	phishing	sur	phishing	sur	phishing	sur
Vrai positif	0.995	0.66	0.987	0.925	0.988	0.064	0.98	0.929	0.966	0.931
Faux positif	0.34	0.005	0.075	0.013	0.936	0.012	0.071	0.02	0.069	0.034

Tableau 3.2 : Tableau récapitulatif des précisions.

VI-II CHOIX DU MEILLEUR RESULTATS

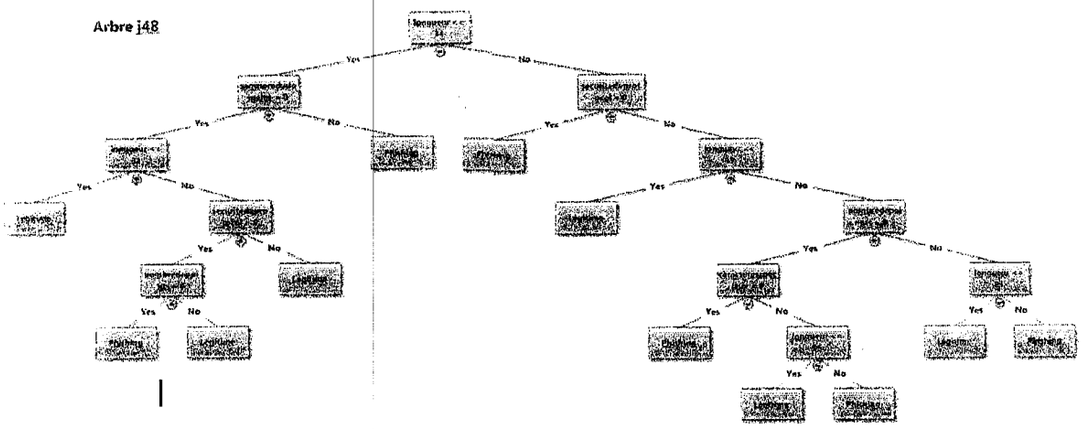
Le but de cette étude est de éliminer voir réduire les faux négatifs pour les deux classes (les adresses phishing classée comme valides et inversement).

Pour cela et après l'analyse de données nous avons trouvé que les réseaux bayesiens et la meilleure solution avec la matrice de confusion.

```
=== Confusion Matrix === (RANDOM TREE)
   a     b     <-- classified as
5999    70 |    a = Phishing
  34   501|    b = SUR
```

Figure3.5 : Matrice de confusion pour les réseaux bayesiens

Voici l'arbre de décision de type J48 que Weka a généré



VI-III DISCUSSION DES RESULTATS

Apres avoir essayé plusieurs classifieurs nous avons trouvé que les réseaux bayesiens et les arbres de décision sont les mieux adaptés, les mieux performants avec une précision avoisinant les 98 %.

En se basant sur la dernière matrice de confusion nous pouvons dire deux choses

1- Le système détecte des faux positifs (fausses alarmes 34 instances), qui n'est pas un vrai problème vis-à-vis l'utilisateur, malgré que c'est un argument de confort pour l'utilisateur.

2- Le problème majeur est qu'il y a un nombre d'instances qui sont passés inaperçus (70 instances confirmées phishing) par le système alors qu'ils constituent un vrai danger pour l'utilisateur inexpérimenté.

VII CONCLUSION

Malgré les bons résultats obtenus par notre système, il y a beaucoup d'améliorations à faire comme l'ajout d'heuristiques, et l'intégration d'autres approches par prendre en considération le corps de l'email et le site en considération.

La base que nous avons utilisée est vraiment réduite (6604 instances) et ne reflète pas vraiment tout les cas possibles, les formes imaginables que peut avoir une adresse phishing. Alors pour faire un système fiable et applicable en réalité il faut avoir beaucoup plus d'instances dans la base d'apprentissage.

CONCLUSION GENERALE

Comme nous avons vu a travers cette étude le phishing est un sérieux danger en ligne, chaque jours en signale des milliers de nouveaux sites de phishing. Les techniques évoluent aussi très vite.

Une vraie guerre ou les mesures de contre attaque restent un pas en arrière car il y a toujours des adresses de phishing qui échappent des filtres quoi que se soit les performances des systèmes ils n'atteindront jamais le maximum.

Pour notre application qui reste un peut simpliste, il y a beaucoup d'améliorations en perspective, comme l'utilisation des techniques anti-spam avec l'intégration de plus d'heuristiques, et prendre en considération le site en lui-même en utilisant différentes méthodes statistique et probabilistes, et l'intégration du Protocol WHOIS qui peut nous donner des informations sur le domaine et son âge.

Le seul élément clef de ce combat reste l'humain utilisant la machine, il faut réveiller son attention pour assister ces systèmes à identifier ces dangers.

Liste de références

CHAPITRE I

1- Rapport Microsoft sur les données de sécurité - Volume 10.
2- Phishing initiative. http://phishing-initiative.blogspot.com/

CHAPITRE II

1- Phishing initiative. http://phishing-initiative.blogspot.com/
2- Rapport Microsoft sur les données de sécurité - Volume 10.
3- J. Hou , Y. Zhang, Constructing good quality web page communities, Australian Computer Science Communications, v.24 n.2, p.65-74, January-February 2002
4- J. Dean , M. R. Henzinger, Finding related pages in the World Wide Web, Proceedings of the eighth international conference on World Wide Web, p.1467-1479, May 1999, Toronto, Canada

CHAPITRE III

SUMMARY

The entire Internet community is familiar with spam and phishing attacks. While spam is an annoyance, phishing can cause major financial disruptions for those involved. The phishing problem is becoming a major concern for the ISP market, and the pressure is coming from both users who are beginning to demand that their service providers take action against the attacks and from financial institutions that are the target of the attacks.

ISPs are being forced to actively participate in the global reduction of phishing attempts to mitigate customer churn and possibility of litigation. There is a lack of consensus as to how an

ISP should attempt to reduce the exposure of its users and the global community to phishing attempts. This document distills the best of the practices used by members of MAAWG to combat phishing attacks.

Nature of phishing attacks

The Internet community and ISPs have a reasonable handle on the spam problem today. In-house technology, third party solutions and industry initiatives have focused on anti-spam for a long time and most ISPs are equipped to combat spam with acceptable efficiency. Phishing is a relatively new threat, a more insidious one at that, which is further exacerbated by its surface similarity to spam. Phishing attacks are relatively sophisticated and logistically different from spam and understanding the differences is critical when considering a framework for protection from these attacks. This section examines the more important differences between spam and phishing.

* Sophisticated

* Targeted

* Transient

* Dynamic

Inbound protection

Several techniques have been developed and are in use for filtration of phishing. These include,

IP based blacklists, Bayesian filters, heuristics engines, content fingerprinting schemes, and sender authentication. While all these techniques are effective to varying degrees against phishing, only some perform well against phishing. Here's a breakdown of what to expect with different techniques:

ملخص

الإصطياد الإلكتروني هو عملية إحتيال يستخدمها لصوص الإنترنت للحصول على المعلومات الشخصية والمهمة للضحايا ككلمة المرور ورقم بطاقة الإئتمان وذلك بغرض سرقة أموال وهويات الضحايا من المستخدمين.

يتم في هذا الإحتيال الدمج ما بين التقنيات و الهندسة الإجتماعية، ولكن الإعتماد الأكبر للصوص هو على الهندسة الإجتماعية كونها ذلك الإحتيال الذي لا يمكن تفاديه بمضادات الفيروسات أو بجدران النار أو غيره من تقنيات الأمن الإلكتروني، فالهندسة الإجتماعية تعتمد وبشكل كبير على مدى التأثير على المستخدم واستغلال ضعف ثقافته ووعيه في أمن المعلومات ومخاطر الإنترنت.

بما أن القانون لا يحمي المغفلين فإن من البديهي على كل من يستخدم الانترنت أن يتحمل عواقب استخدامه له بطريقة أو بأخرى: كمية المعلومات التي يكتبها، أين يكتبها ولماذا يكتبها. استخدام الانترنت يتطلب قدراً من الحذر والوعي بما لك وما عليك، خاصة في حالة الحاجة لإدراج معلومات مهمة مثل المعلومات المطلوبة لإتمام عمليات في مواقع البنوك ومواقع التجارة الالكترونية.

مواقع الاصطياد الالكتروني متنوعة في طريقتها، بعضها يستخدم نوافذ منبثقة التي وإن كانت تحمل شعار واسم المنشأة الحقيقية إلا أنها ليست تابعة لها، يمكن معرفة أن النوافذ غير شرعية في حال طلبت منك إدخال رقم الحساب البنكي واسم المستخدم وكلمة المرور في نفس النافذة.

عمليات الاحتيال قد تحدث أيضاً بالبريد الالكتروني، عند تسجيل الدخول لحسابات شخصية كما في البريد الالكتروني أو الحسابات البنكية يجب التأكد من أن العنوان في وضع الأمان بظهور رمز القفل وانتقاله من بروتوكول http إلى https. الجدير بالذكر أن المواقع الشرعية لا تطلب من عملاءها إرسال معلومات سرية عبر البريد الالكتروني على الإطلاق، وعندما ترسل بريداً إلكترونياً إلى العميل فإنها تخاطبه باسمه وليس بصيغة عامة مثل Dear Member.

أخيراً، الحذر من الروابط التي يحتويها البريد الالكتروني خصوصاً الروابط المختصرة أو المكونة من حروف عشوائية، ولتطبيق نسبة أعلى من الأمان يمكنك استخدام إضافات مثل إضافة LinkPeelr لمتصفح قوقل كروم، أو إضافة LinkExtend لمتصفح فايرفوكس. هذه الإضافات تساعدك على إظهار الرابط الكامل بمجرد وضع المؤشر عليه، وتزداد أهمية هذه الإضافات بعد أخبار متلاحقة عن دودة إلكترونية تنتشر في تويتر بالروابط المختصرة.

ختاماً، المواقع التي يتصفحها المستخدم باستمرار هي التي تحدد نسبة تعرضه للاحتيال والاصطياد الالكتروني، يُفضّل دائماً التعامل مع المواقع الرسمية وعدم البحث عن الأسهل لأنه قد يكلفك أموالاً طائلة في حال تعرضك للاصطياد مثل الابتزاز في مقابل معلومات تمت سرقتها منك.