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 :

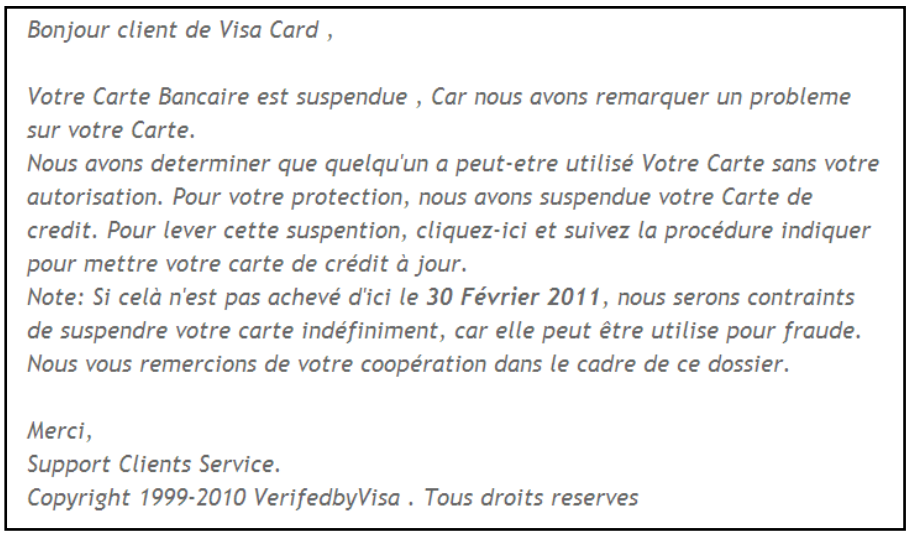
phishing = spam + mail spoofing + social engineering + URL spoofing + scam + URL cloaking + pratique mafieuse

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

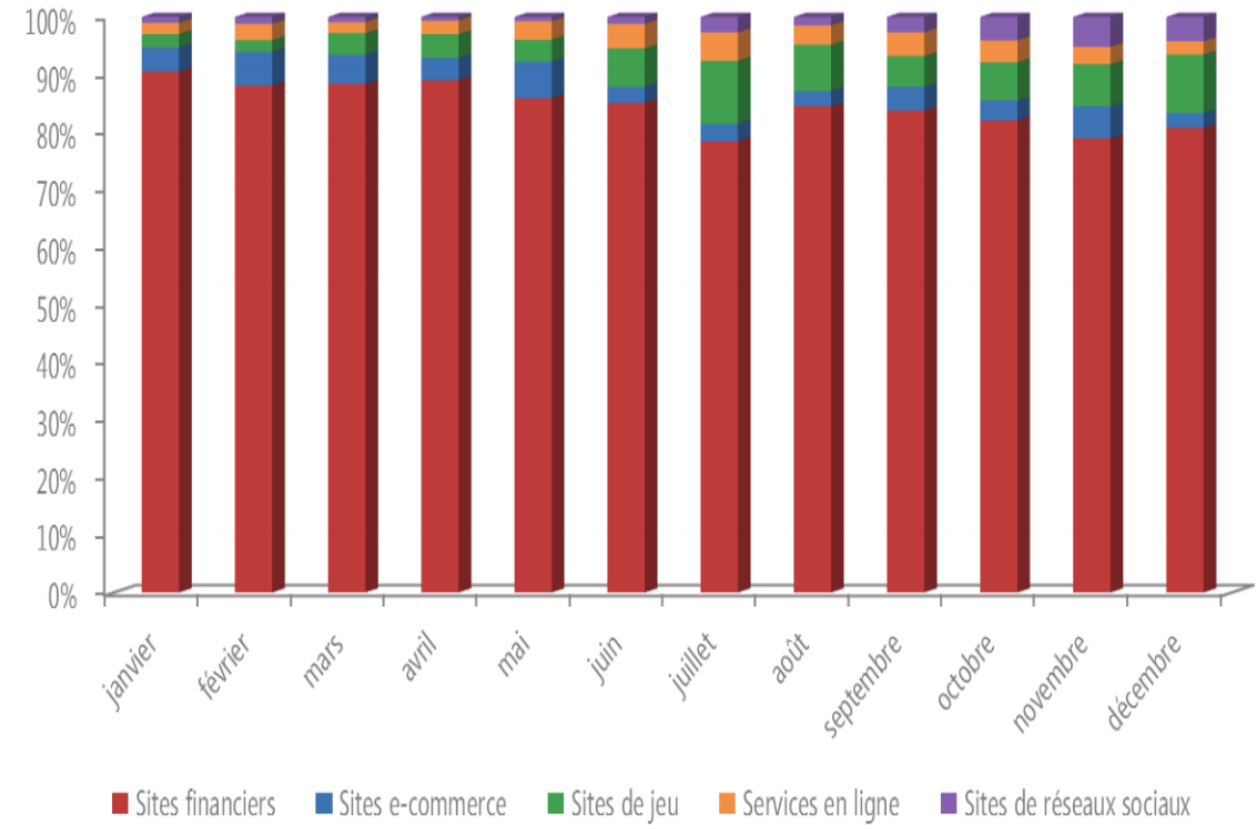


Figure 1.2 : Sites d'hameçonnage actifs observés chaque mois de 2010

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.

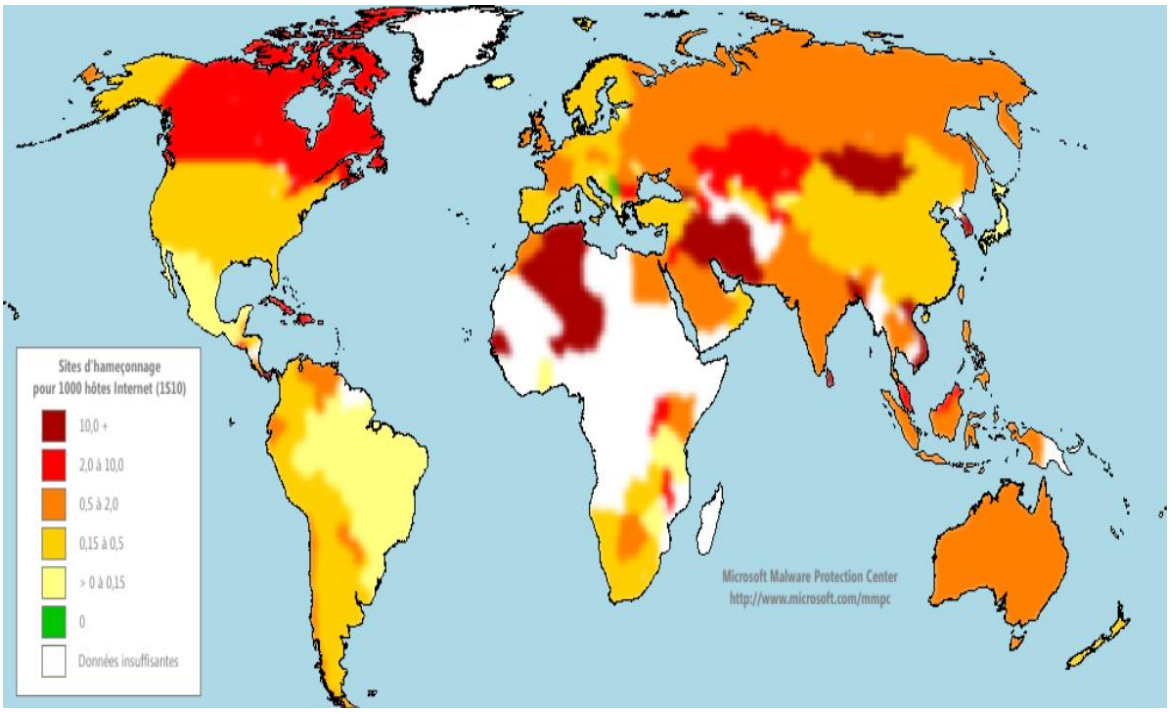


Figure 1.3 : Sites d'hameçonnage pour 1 000 hôtes Internet dans le monde

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

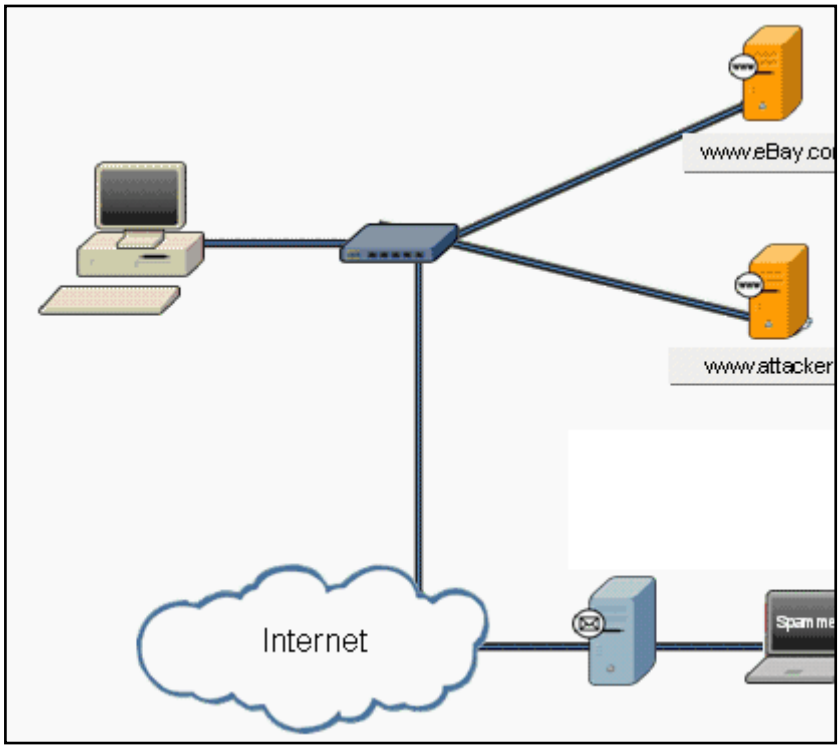


Figure1.4 : les étapes du phishing.

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)

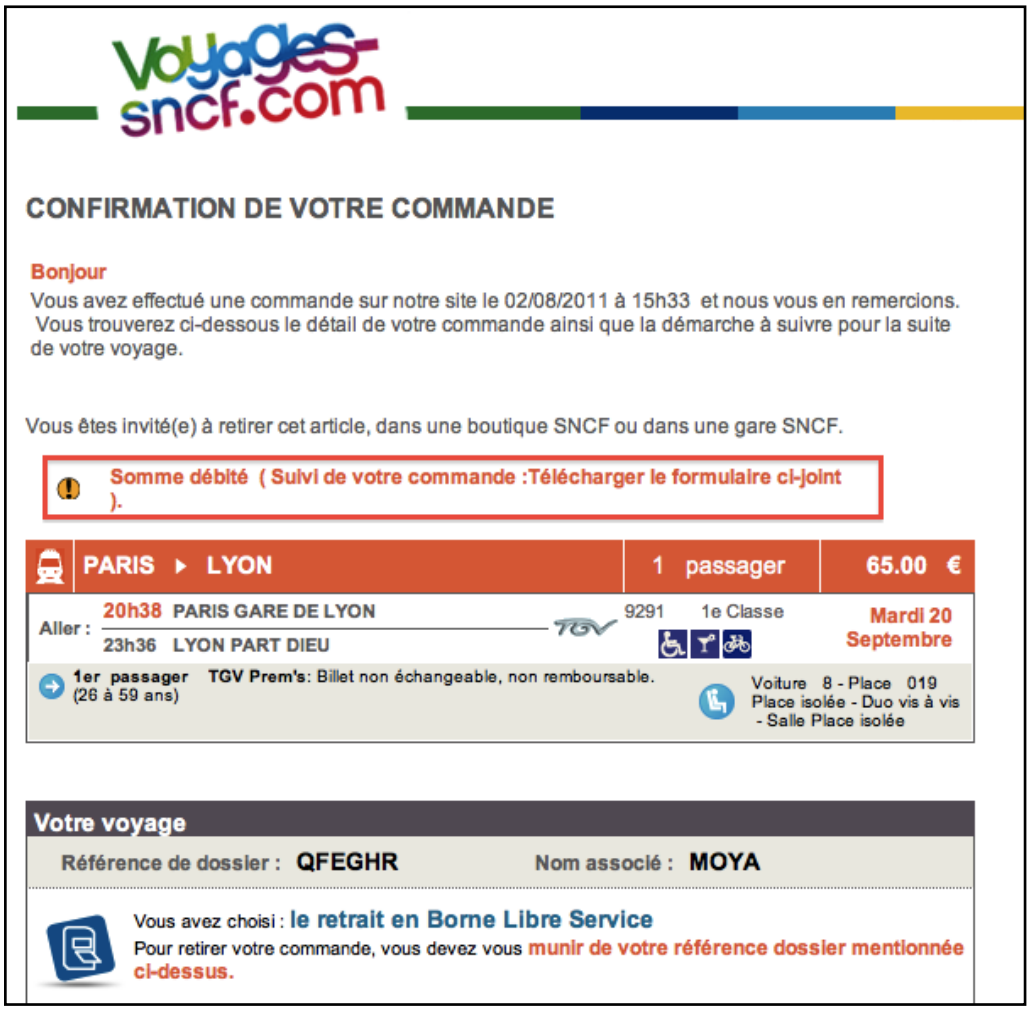
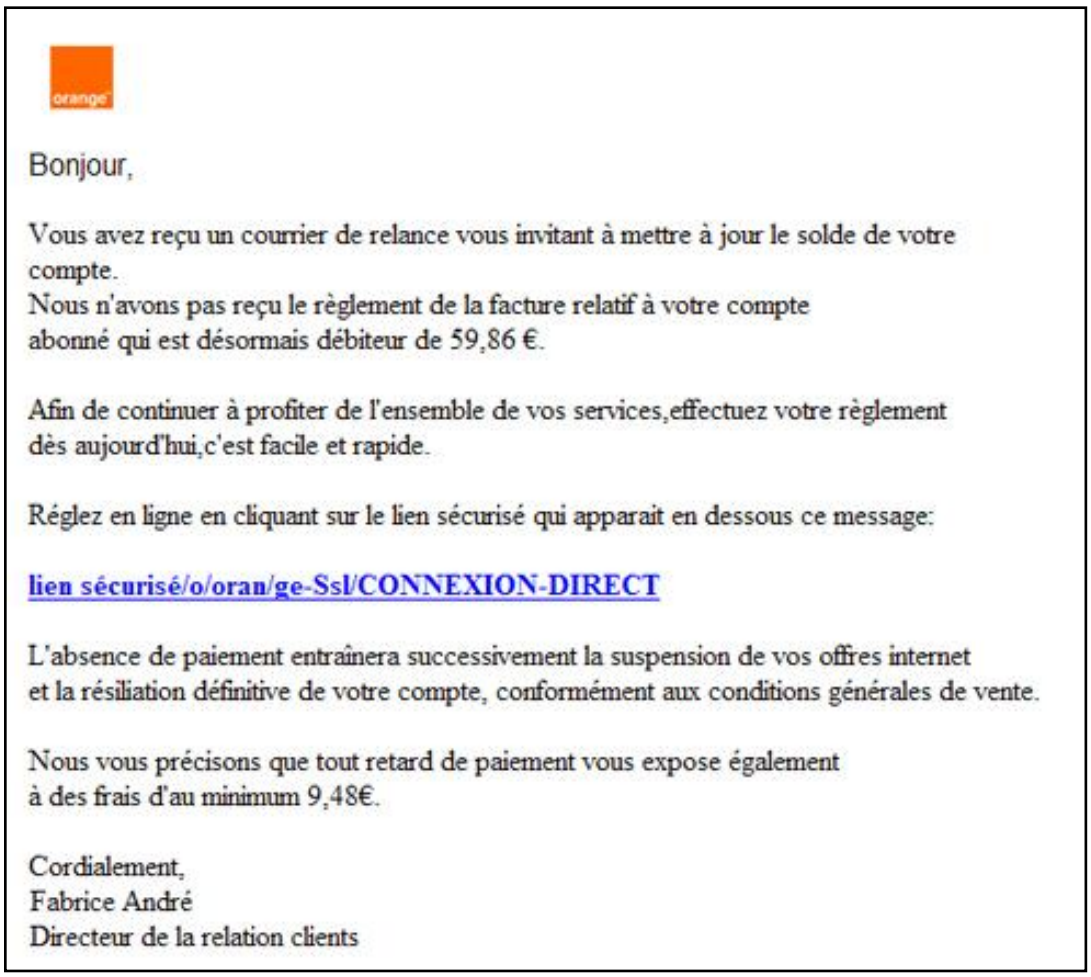


Figure1.5 : Phishing par pièce jointe.

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/oran/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.