h e g

Haute école de gestion
Genève

Mécanismes de Social Engineering (phishing) : étude technique et économique

Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES

par :

Kelvin DEUSS

Conseiller au travail de Bachelor :

David BILLARD, professeur HES

Genève, 25 avril 2016

Haute École de Gestion de Genève (HEG-GE)

Filière Informatique de Gestion

Hes·so GENÈVE
Haute Ecole Spécialisée de Suisse occidentale

Déclaration

Ce travail de Bachelor est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre de Bachelor en Informatique de Gestion.

L'étudiant atteste que son travail a été vérifié par un logiciel de détection de plagiat.

L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de Bachelor, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de Bachelor, du juré et de la HEG.

« J'atteste avoir réalisé seul le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Genève, le 25 avril 2016

Kelvin DEUSS

Remerciements

Je tiens tout d'abord à remercier mon directeur de mémoire, le professeur David Billard, pour avoir accepté de suivre ce travail de Bachelor et pour les conseils qu'il m'a prodigués.

Je souhaite également remercier ma famille ainsi que mes amis pour leur soutien et encouragement tout au long de mes études.

Résumé

Les escroqueries sur internet sont nombreuses et variées. Toute personne est susceptible d'être la cible d'une attaque lors d'une navigation sur le net. De plus en plus d'escrocs n'hésitent pas à recourir au Social Engineering comme levier pour acquérir des données sensibles de manière déloyale en exploitant les failles humaines. Le phishing est une technique de Social Engineering employée par ces pirates. Il est utilisé pour subtiliser des informations personnelles dans le but de commettre une usurpation d'identité à l'insu de leurs victimes. La force de persuasion de ces escrocs est la clé de voûte d'une attaque réussie.

Le but de ce travail est tout d'abord d'explorer les différentes techniques de phishing utilisées par les pirates pour ensuite identifier les mesures de protection disponibles contre ce phénomène. Enfin, nous aborderons les moyens de lutte mis en œuvre par des organismes pour tenter de combattre ce fléau.

Table des matières

Liste des figures

1. Introduction

Depuis des siècles, des escroqueries en tout genre ont été imaginées et orchestrées par des gens peu scrupuleux dans le but de tromper la confiance d'autrui et ainsi en obtenir des biens de manière frauduleuse.

En remontant au XVIe siècle, on constate l'apparition d'une escroquerie appelée l'arnaque de « La prisonnière espagnole ». Cette escroquerie avait pour nature d'extorquer de l'argent à de riches bourgeois par une combine qui consistait à leur faire croire qu'une très belle et riche princesse espagnole était détenue prisonnière par les turcs et qu'une rançon était exigée pour sa libération.

A la fin du XVIIIe siècle, une autre fraude se basant sur les mêmes effets psychologiques que cette dernière fit son apparition, il s'agit de : « La lettre de Jérusalem ». Le principe étant que l'escroc fait croire à une victime, par une série de lettres adressées à celle-ci, qu'il possède un fabuleux trésor mais pour des raisons indépendantes de sa volonté, il n'a plus la possibilité d'y accéder. L'escroc fait appel alors à la bonté de sa victime pour solliciter son aide afin de récupérer ce trésor. Celle-ci alléchée par la perspective de ce trésor, commence à débourser de l'argent afin que l'escroc puisse le récupérer. Malheureusement pour la victime, l'escroc trouvera toujours une excuse pour légitimer l'impossibilité de rapatrier le pactole tout en incitant la victime à s'acquitter d'une nouvelle somme d'argent afin de continuer la quête du trésor.

A la fin du XXe siècle, l'apparition d'internet donna une descendance à cette escroquerie, appelée cette fois « Fraude 4-1-9 ». Basée sur le même principe que « La lettre de Jérusalem », cette filouterie abusant de l'ingénuité de ses victimes, s'opère désormais par des moyens de communication modernes à savoir par messagerie électronique, principalement par courriel mais parfois aussi par SMS.

Le point commun de toutes ces escroqueries est leur exploitation des failles psychologiques de l'être humain. Une victime est manipulée par un escroc qui abuse de sa confiance et de sa crédulité pour lui soutirer ce dont il a besoin. La démocratisation de l'accès à internet a étendu les possibilités d'arnaque en tout genre sur la toile. Les escroqueries recourant notamment à l'ingénierie sociale sont devenues nombreuses et variées.

On constate encore chez nombre d'internautes, un manque de connaissances spécifiques à ce sujet, ce qui peut déboucher sur la divulgation d'informations

personnelles permettant ainsi à des personnes malveillantes d'usurper leur identité afin d'en retirer un avantage.

A l'heure actuelle, aucun anti-virus n'est capable de protéger totalement les utilisateurs contre leurs propres faiblesses. Le bon sens de chacun est la règle de d'or pour ne pas se faire piéger.

2. L'ingénierie sociale en termes de sécurité de l'information

Le terme d'ingénierie sociale, en anglais « social engineering », fait référence aux techniques de manipulation psychologique de personnes utilisées par des criminels souhaitant contourner des dispositifs de sécurité dans le but de soutirer frauduleusement des informations confidentielles. Ces techniques sont principalement basées sur l'abus de confiance, la bonne foi et la naïveté mais aussi sur l'insécurité et l'ignorance des personnes.

Généralement, les victimes tombant dans le piège ne se doutent de rien. Les attaquants, quant à eux, n'ont pas toujours de connaissances techniques spécifiques mais profitent de la croissance exponentielle de l'utilisation des messageries électroniques et de la popularisation des réseaux sociaux.

Au-delà de tout système de protection technologique, l'être humain reste l'unique maillon faible. Cependant, l'ingénierie sociale ne s'étend pas forcément qu'au seul domaine de l'informatique, elle peut survenir dans n'importe quelle situation de la vie de tous les jours.

2.1 Une manipulation psychologique

Toute la puissance de ces techniques repose sur l'usage de la force de persuasion. Le principe de base de cette manipulation se fonde sur l'image renvoyée par l'attaquant. Notre éducation nous apprend à bâtir des relations avec nos semblables tout en respectant un certain nombre de codes sociaux.

Il s'agit en fait d'accorder plus facilement notre confiance aux personnes physiques ou morales ayant une représentation spécifique d'autorité comme par exemple la police, un médecin, un informaticien du support technique ou encore une institution bancaire.

Les attaquants recourant à l'ingénierie sociale savent être convaincants en se camouflant. Ils connaissent les leviers à actionner permettant d'obtenir les informations désirées en créant ce cadre de confiance. Ces méthodes de collecte illicite de données à l'insu d'une personne sont définies par le terme de processus d'élicitation, de l'anglais *elicit*[1] : obtenir quelque chose de quelqu'un.

[1] Source : http://www.wordreference.com/enfr/elicit

2.2 Principales méthodes d'approche

En règle générale, les tactiques d'approche s'exécutent souvent selon un scénario prédéfini. Cela commence par un premier contact de l'attaquant vers sa victime en usurpant l'identité d'une personne morale ou physique permettant ainsi de déjouer sa vigilance. Ce procédé permet de mettre la victime en confiance.

Ensuite, l'attaquant va prétexter une situation qui va susciter l'intérêt de sa victime afin de la désorienter. La victime va suivre les indications de l'attaquant et c'est à ce moment précis qu'elle est piégée, en divulguant des informations sensibles. Pour finir, l'attaquant va prétexter, grâce aux informations récoltées, que la situation est rentrée dans l'ordre, ce qui aura pour but de rassurer la victime et éviter qu'elle ne reste concentrée sur le précédent problème.

2.3 Principales formes d'approche

Il existe différentes formes d'approche utilisées par les attaquants pour piéger leur victime. Ci-dessous une liste non exhaustive des méthodes pratiquées :

- Par téléphone
- Par courrier écrit
- Par courrier électronique
- Par messagerie instantanée
- Par réseaux sociaux

3. Le phishing : une méthode d'ingénierie sociale

3.1 Origine

Étymologiquement, le mot « phishing » est une contraction du mot « fishing » signifiant « pêche » en anglais et du mot « phreaking » désignant le piratage téléphonique. En français, le phishing est traduit par le mot « hameçonnage ». Il est apparu aux alentours de l'année 1995. Encore méconnu à cette époque, ce type d'arnaque sur internet commençait déjà à causer quelques problèmes.

Selon les archives d'internet, il semblerait que la première mention du mot phishing date du 2 janvier 1996. Elle est apparue dans un groupe de discussion Usenet[2] appelé alt.online-service.america-online à la suite des mesures prises par America Online (AOL) pour empêcher l'ouverture de comptes par l'utilisation de faux numéro de cartes de crédit algorithmiquement générés.

En effet, à cette époque, AOL étant le leader des fournisseurs d'accès à internet, des millions de personnes utilisaient leurs services ce qui en faisait une cible naturelle pour des attaques. Les pirates créaient des algorithmes de génération aléatoire de numéros de cartes de crédit afin d'ouvrir des comptes AOL pour ensuite les utiliser à des fins frauduleuses. Lorsque AOL introduira des mesures de sécurité destinées à empêcher l'utilisation de cette technique, les pirates orienteront leurs attaques vers les systèmes de messageries, définissant ainsi l'orientation qu'allaient prendre les attaques de phishing à l'avenir.

Pendant près d'une dizaine d'années, le phishing resta très méconnu des internautes sans pour autant en être moins dangereux. A partir des années 2000, les attaques de phishing évoluent pour s'orienter dans un premier temps vers les sites de paiement en ligne puis vers des sites bancaires, développant ainsi de plus en plus de méthodes plus sophistiquées les unes que les autres.

3.2 Explications

Le phishing est une technique frauduleuse employée par des pirates informatiques pour tenter d'acquérir des données sensibles d'internautes afin de commettre une usurpation d'identité. Ces renseignements personnels sont souvent des :

- identifiants
- mots de passe
- noms

[2] Source : https://fr.wikipedia.org/wiki/Usenet

- prénoms
- dates de naissance
- numéros de carte de crédit
- numéros de client et de compte bancaire

Les pirates se font passer pour une entité digne de confiance en piégeant les internautes sans méfiance au moyen de copies conformes de sites internet et courriers électroniques usurpant le nom du tiers de confiance. Ces entités dignes de confiance revêtent couramment la forme de :

- banque
- administration publique
- réseaux sociaux populaires
- service de paiement en ligne
- sites d'enchères
- site de commerce en ligne
- plates-formes d'échanges commerciaux
- administrateur informatique

Les courriers électroniques envoyés par ces pirates invitent les utilisateurs à cliquer sur un lien hypertexte afin d'être redirigés sur une page web falsifiée permettant de prétendument se connecter en ligne. Une fois l'internaute arrivé sur ce site internet contrefait, sous un prétexte fallacieux, il lui est proposé de remplir un formulaire avec ses informations personnelles. C'est ainsi que le pirate accapare les données de sa victime. Le phishing concerne toutes les interfaces où une authentification est nécessaire. Il est possible aussi que le lien hypertexte contenu dans le courrier électronique soit infecté par un logiciel malveillant de type malware. La plupart des cas de phishing sont effectué par la technique d'email spoofing[3] (technique d'usurpation d'identité consistant à envoyer des messages en se faisant passer pour autrui) ou par le biais des messageries instantanées. Lorsqu'un courrier électronique de phishing d'une entité de confiance spécifique est envoyé à un grand nombre de destinataires, en sachant que les adresses électroniques de ceux-ci ont été collectées de manière aléatoire sur internet, le message n'a généralement aucun impact car le destinataire n'a souvent aucun lien avec le tiers de confiance mentionné dans le courrier électronique.

[3] Source : https://en.wikipedia.org/wiki/Email_spoofing

Cependant, sur la quantité de message transmis, la probabilité que le destinataire ait un lien direct avec l'entité de confiance est élevée. Le phishing est une menace perpétuelle et le risque est d'autant plus important dans les réseaux sociaux tels que Facebook, Twitter et Google+.

3.3 Techniques de phishing

3.3.1 Courrier électronique et spam

Le pirate envoie un courrier électronique similaire à plusieurs millions d'internautes. Ce message contient un lien redirigeant sur un site internet prétendument de confiance avec un formulaire demandant des informations personnelles. Les données récoltées seront utilisées par le pirate pour ses activités illégales. L'utilisation du courrier électronique ou du spam est une technique de phishing très utilisée.

En général, les messages font référence à une situation urgente à régler (mise à jour du service, intervention du support technique, vérification du propriétaire du compte, blocage de compte ou de carte de crédit, perte d'argent, plainte pénale, malchance,…) l'utilisateur entre ainsi des informations d'identification dans le but de régler cette situation et d'éviter le pire. Parfois, afin d'accéder à un prétendu nouveau service, l'utilisateur peut être invité à remplir un formulaire pour accéder à celui-ci par le biais d'un lien hypertexte fourni dans le courrier électronique.

3.3.2 Messagerie instantanée

Dans cette méthode, l'utilisateur reçoit un message par messagerie instantanée avec un lien le dirigeant vers un site internet corrompu où il sera invité à fournir des renseignements personnels. Si l'utilisateur n'est pas suffisamment attentif à l'URL, il lui sera difficile de faire la différence entre le site internet original et une copie créée par un pirate.

3.3.3 Manipulation de lien

La manipulation de lien est la technique de phishing la plus classique. En effet, la majorité des procédés de phishing emploient cette forme de tromperie. Cette technique consiste à proposer un lien semblant appartenir à un organisme de confiance mais qui en réalité redirige l'internaute vers un site internet falsifié. Lorsque l'utilisateur clique sur ce lien, il ouvre le site internet du pirate au lieu du site internet officiel.

3.3.4 Phishing par QR-Code

Le QR-Code permet de contenir des sources d'informations supplémentaires lisibles uniquement au moyen d'une application (de smartphone par exemple) spécifiquement prévu pour le scanner. Le problème réside dans le fait que l'œil humain n'est pas en

mesure de pouvoir décoder d'emblée ce code. Les fraudeurs l'ont bien compris et profitent de cette faille pour attirer dans leur piège des utilisateurs peu regardants en masquant les QR-Codes authentiques par leur propre QR-Code. En effet, lors du scan d'un code QR, il est souvent difficile pour les utilisateurs de distinguer les bonnes des mauvaises URL ce qui a pour conséquence de les rediriger vers de faux sites internet ou encore d'exécuter des scripts et de débuter des téléchargements à leur insu.

3.3.5 Phishing par moteur de recherche

Les moteurs de recherche peuvent être indirectement impliqués dans une attaque de phishing. En effet, les pirates créent de faux sites internet de commerce électronique proposant des produits ou des services avec des offres attractives dans le but qu'ils soient référencés par les moteurs de recherche. Lorsqu'un internaute veut acheter un produit, il entre naïvement les numéros de sa carte de crédit qui sont immédiatement recueillis par le pirate. Ainsi, il existe une multitude de faux sites bancaires proposant des cartes de crédit ou des prêts à faible taux où les victimes sont invitées à transférer les détails du compte.

3.3.6 Phishing par logiciel malveillant

Le phishing par logiciel malveillant requière l'exécution de celui-ci sur l'ordinateur de l'utilisateur. Le logiciel malveillant est habituellement présenté comme une pièce jointe dans un courrier électronique envoyé par le pirate ou en tant que fichier téléchargeable à partir d'un site internet piraté. Une fois que l'utilisateur clique sur le lien, le malware commencera à fonctionner. En conséquence, lorsque l'internaute tentera d'accéder à une page web authentique, il sera automatiquement redirigé vers une page web falsifiée à son insu.

3.3.7 Phishing par téléphone

La technique du phishing par téléphone, appelé aussi vishing, est une méthode pour collecter les données confidentielles d'une victime par contact téléphonique utilisant la technologie d'appel VoIP. Pour les fraudeurs, l'avantage de cette technologie réside dans son faible coût d'utilisation et sa flexibilité. En effet, le fraudeur peut profiter d'utiliser des serveurs vocaux interactifs permettant une interaction avec l'interlocuteur grâce à l'utilisation de messages préenregistrés en voix de synthèse selon un schéma préprogrammé. De plus, il peut aussi facilement usurper le numéro de l'appelant et ainsi garder son anonymat. Il existe plusieurs variantes de vishing, ci-dessous des exemples de ces variantes :

Pour la première variante, les victimes sont contactées par un automate téléphonique délivrant un message préenregistré se faisant passer pour un organisme de confiance

(institution bancaire, financière…). Ce message incite les victimes à révéler leurs informations confidentielles sous un prétexte imaginaire comme par exemple un problème de compte.

La seconde variante consiste en la réception d'un courrier électronique d'un tiers de confiance incitant le destinataire à composer le numéro de téléphone mentionné dans celui-ci. L'attaquant se faisant passer par exemple pour une institution financière, prétexte au destinataire qu'il a été victime d'une fraude à la carte de crédit et doit immédiatement le contacter afin de rétablir la situation. Malheureusement lorsque la victime compose le numéro, elle est invitée à s'identifier en communiquant des renseignements personnels comme le numéro de sa carte de crédit par exemple.

3.3.8 Phishing par SMS

La technique du phishing par SMS, appelé aussi SMishing, est une méthode de collecte de renseignements confidentiels par SMS. Elle utilise le même stratagème que le phishing par courrier électronique à savoir l'incitation de la victime à venir se rendre sur le site internet mentionné dans le message afin que celle-ci fournisse ses informations personnelles. Cette technique peut être associée à celle du vishing si le message incite la victime à composer un numéro de téléphone.

3.3.9 Tabnabbing

Le Tabnabbing est une technique de phishing qui profite de la navigation par onglet dans un navigateur. La victime cliquant sur un lien corrompu d'un premier site internet est redirigée sur une autre page web piégée d'apparence classique traitant d'un sujet quelconque. Lorsque la victime consulte un autre de ses onglets ouverts, un bout de code contenu dans la page piégée permettant de détecter les changements d'onglets fait rafraîchir ladite page pour changer son apparence et la transformer en site internet de réseaux sociaux ou de courrier électronique par exemple. La victime ne prêtant pas attention à l'URL dans la barre d'adresse va se connecter naturellement et le pirate n'aura plus qu'à récupérer ses identifiants.

3.3.10 Evil Twin

Evil twin est une technique de phishing se basant sur les réseaux sans fil Wi-Fi. Le principe est simple, le pirate crée un point d'accès sans fil ressemblant à un réseau public légitime que l'on trouve ordinairement dans les lieux publics tels que les cafés, hôtels ou aéroports et espionne tout le trafic y circulant. Lorsqu'un utilisateur du réseau pirate tente de se connecter à un compte non sécurisé (non-HTTPS), le pirate aura alors accès à l'ensemble des transactions et pourra s'emparer des informations

confidentielles. Cette technique est facile à mettre en place dès lors que chaque ordinateur portable avec une carte réseau sans fil peut devenir un point d'accès.

3.3.11 Key Loggers

Les Keys Loggers sont des malwares enregistreurs de frappes qui identifient chaque entrée faite à partir du clavier. Les pirates récoltent ces informations (mot de passe ou autres données confidentielles) transmises afin de les déchiffrer. Certain sites internet utilisent une parade pour contourner ce problème, ils fournissent un clavier virtuel afin que chaque entrée se fasse par ce biais.

3.3.12 Vol de session

Le pirate exploite le mécanisme de contrôle de session pour voler des informations à l'utilisateur. Les activités de l'utilisateur sont surveillées par le pirate à l'aide d'un analyseur de paquets[4] (sniffer). De cette manière, dès que l'utilisateur tente de se connecter à un compte, le pirate peut intercepter les informations utiles pour accéder au serveur web.

3.3.13 Reconfiguration du système

Un message provenant d'une adresse ressemblant à une source fiable invite l'utilisateur à reconfigurer les paramètres du système d'exploitation de son ordinateur.

3.3.14 Injection de contenu

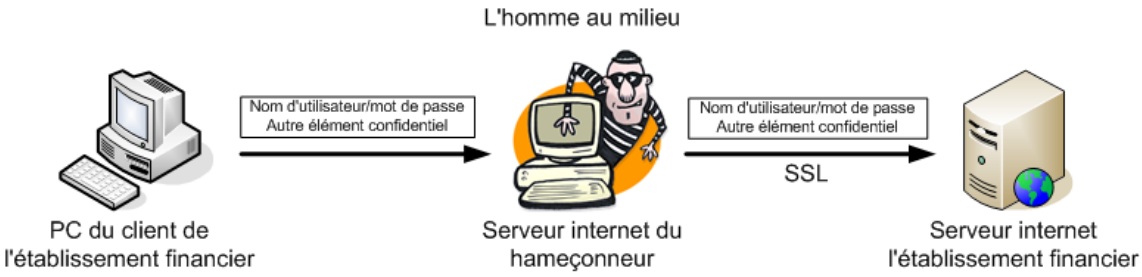
L'injection de contenu est la technique où le pirate insère du contenu malveillant dans un site internet authentique. Le contenu malveillant peut rediriger vers un autre site ou installer un logiciel malveillant sur l'ordinateur de l'utilisateur. Ceci permet d'induire en erreur l'utilisateur afin de le rediriger vers une page en dehors du site internet officiel où il sera invité à saisir des informations personnelles.

3.3.15 Attaque de l'homme du milieu

Cette technique est l'une des plus élaborées. En effet, le pirate s'interpose entre le site internet original et l'utilisateur. Le pirate écoute la communication entre les deux parties et falsifie les échanges entre eux de manière transparente. Tandis que l'utilisateur continue à transmettre des informations, le pirate s'empresse de les recueillir à l'insu de celui-ci.

[4] Source : https://fr.wikipedia.org/wiki/Analyseur_de_paquets

Figure 1 : Attaque de l'homme du milieu



(https://www.ebankingabersicher.ch/images/stories/ihrBeitrag/phishing/fr/Phishing_MITM.png)

3.3.16 Pharming

Le pharming est une technique de phishing plus sophistiquée. Le principe reste le même que pour une attaque de phishing classique pour ce qui est du vol d'informations confidentielles à travers un faux site internet.

Sauf qu'au lieu d'inciter les victimes à cliquer sur un lien dans un faux courrier électronique, le pirate exploite directement la vulnérabilité du serveur DNS en créant une attaque de type « DNS cache poisoning[5] », qui aura pour effet de rediriger les victimes vers le faux site internet malgré le fait qu'elles aient tapé correctement l'adresse du site désiré. Les serveurs DNS sont responsables de résoudre des noms de domaine dans leur véritable adresse IP. Lors d'une attaque de pharming, lorsqu'une requête DNS pour un nom de domaine est effectuée, ce n'est pas l'adresse IP réelle de ce nom de domaine qui est résolue mais celle créée par le pirate.

3.4 Formes spécifiques de phishing

3.4.1 Spear phishing

A l'inverse du phishing traditionnel, consistant en l'envoi d'un message générique à un nombre élevé d'internautes en espérant que quelques-uns d'entre eux tombent dans le piège, le spear phishing cible un nombre restreint de victimes, souvent un certain groupe de personnes ayant un point commun avec un profil généralement intéressant. Ce qui rend cette technique encore plus insidieuse, c'est qu'elle consiste en l'envoi d'un message fortement personnalisé aux victimes en se faisant passer pour une personne ou un organisme avec qui elles ont habituellement des relations de type professionnelles par exemple.

Pour rendre ces attaques convaincantes et ainsi augmenter la probabilité de succès, le pirate s'attachera à récolter le maximum d'informations personnelles sur sa cible par l'entremise de sources publiques comme des réseaux sociaux ou des registres publics

[5] Source : https://fr.wikipedia.org/wiki/Empoisonnement_du_cache_DNS

ainsi que de sources privées corrompues par des attaques antérieures. Les attaques de spear phishing sont des attaques sophistiquées du point de vue des moyens engagés pour les réaliser, ce qui traduit une vraie détermination du pirate à vouloir obtenir des renseignements extrêmement précis.

3.4.2 Whaling

Le whaling est une forme de spear phishing encore plus pointue. Signifiant littéralement « chasse à la baleine » ces attaques sont spécifiquement dirigées contre des cibles de haut niveau. Ces cibles sont généralement des personnes ayant un revenu élevé comme des cadres ou directeurs d'entreprises, des célébrités ou encore des personnalités du monde politique.

La technique reste similaire à une attaque de spear phishing, un message fortement personnalisé d'un destinataire de confiance est envoyé à une victime. Ce message incitant la victime à cliquer sur un lien ou à ouvrir une pièce jointe aura pour effet d'installer un logiciel malveillant recueillant la moindre information confidentielle sur l'ordinateur de celle-ci. Dans certains cas, le message demandera directement d'effectuer une opération spécifique comme un transfert de fonds vers un compte externe par exemple. Dans leurs messages, les pirates se dissimulent à travers des noms de domaine usurpés pour piéger leur victime. Le niveau de sophistication est extrêmement élevé ce qui rend ces attaques encore plus difficiles à détecter.

3.5 Les méthodes utilisées par les attaquants

Les méthodes d'attaques de phishing employées par les pirates deviennent de plus en plus sophistiquées. Non seulement les pirates rivalisent d'ingéniosité pour imaginer des nouvelles techniques, mais encore ils s'attachent à maîtriser de mieux en mieux les outils informatiques disponibles dans l'intention de rendre leur identification de plus en plus ardue. Ainsi, pour perpétrer leurs méfaits sur internet de manière anonyme, les pirates auraient recours au réseau Tor[6] et aux services VPN. De plus, pour enregistrer des noms de domaines et héberger des sites de phishing, ces cybercriminels utiliseraient des services d'hébergement Bulletproof[7] (services d'hébergement inatteignables par les autorités en raison de leur localisation géographique). Les sites de phishing devenant davantage indétectables car quasi identiques aux sites officiels, seules des personnes expérimentées peuvent faire la différence.

La Suisse n'est pas épargnée par les offensives de phishing et reste une cible privilégiée en raison de sa richesse. Pour contourner les systèmes antivirus et pare-feu

[6] Source : https://fr.wikipedia.org/wiki/Tor_(r%C3%A9seau)
[7] Source : https://en.wikipedia.org/wiki/Bulletproof_hosting

et donner un aspect légitime, les pages web de phishing peuvent être hébergées sur des comptes piratés ou non ou sur des services de cloud tel que Google Drive ou Dropbox. Un autre moyen de rediriger les internautes vers un site de phishing est d'injecter un code malicieux dans un site internet authentique.

3.5.1 Le partage d'information

La tendance actuelle consistant à partager les moindres détails de sa vie sur internet comme sa géolocalisation, son humeur par l'intermédiaire de statuts ou son curriculum vitae et celle du tout connecté, sont une mine considérable d'informations pour les cybercriminels. La quantité de renseignements accumulés est profitable à l'élaboration de fraudes toujours plus sophistiquées, ceci aux dépens des internautes. Mais pas seulement, les entreprises sont aussi touchées, de la PME à la grande entreprise.

En effet, les pirates effectuent un vrai travail de fourmi pour collecter des informations sur l'environnement de l'entreprise visée tel que les modèles d'adresses de courrier électronique, le secteur d'activité, l'organigramme et les postes clés. Ils se renseignement notamment sur les employés ayant des contacts avec les banques et fiduciaires et les modalités de paiement de l'entreprise afin de déclencher des ordres de paiement ou des transferts d'argent en se faisant passer pour la société.

3.5.2 Scénario d'attaque possible

Avec toutes ces données, un scénario plausible d'une attaque peut être imaginé. Le pirate envoie un courrier électronique à l'attention d'un employé de la comptabilité en se faisant passer pour un cadre dirigeant de l'entreprise. Le courrier électronique imitant parfaitement celui que pourrait potentiellement envoyer le cadre, prétexte une opération commerciale en cours, insistant sur le degré de confidentialité de la transaction et l'urgence de la situation.

Afin d'effectuer le versement, l'employé du service comptabilité est mis en relation avec un cabinet juridique existant mais créé par le pirate lui-même. Parfois le pirate prend contact directement par téléphone avec l'employé en question dans l'intention de de se rendre plus crédible. Les établissements bancaires sont évidemment une cible de choix pour les cybercriminels.

Les pirates ayant accès à des comptes de messagerie piratés de particuliers recherchent toutes correspondances que le propriétaire du compte aurait pu entretenir avec sa banque. Une fois tombé sur les coordonnées d'un employé de l'établissement bancaire, le pirate usurpant l'identité du client, demande à effectuer un transfert d'argent vers un compte qu'il possède à étranger.

4. Les victimes du phishing

Les attaques de phishing se basant sur l'ingénierie sociale se servent de la bonne foi et de la crédulité des personnes pour accéder à des données confidentielles ou les forcer à réaliser des opérations spécifiques en vue d'obtenir un versement d'argent. Partant de ce constat, il est possible d'affirmer que n'importe quel citoyen recourant à tout type de services en ligne sur internet est susceptible d'être une victime potentielle d'attaque de phishing.

A plus large échelle, de la PME à la multinationale, indépendamment de son secteur d'activité, en passant par les organisations et gouvernements, tous sont désormais considérés comme des cibles possibles. Ainsi, toute entité susceptible d'enrichir les escrocs par ses fonds ou ses informations est une victime potentielle. Pour les attaques destinées à infiltrer ces grandes structures, le pirate doit procéder à des attaques extrêmement ciblées pour gagner la confiance de ses interlocuteurs.

4.1.1 Les conséquences d'une attaque réussie

Les conséquences d'une attaque de phishing sont indéniablement fâcheuses pour les victimes. En effet, une de ces attaques provoque toujours deux victimes, à savoir la victime directe, celle qui a été prise pour cible et la victime collatérale, celle dont l'identité a été usurpée. Pour les particuliers, la conséquence majeure est la perte financière directe subie suite au vol de données mais aussi la perte de temps que cela va engendrer. Assurément, lorsque les données personnelles sont dans les mains d'un pirate, la victime devra consacrer de son temps pour toutes les mesures relatives à l'endiguement de son problème de manière à limiter l'usurpation de son identité. A ce moment-là, la victime ressent comme une perte de contrôle sur ses propres informations.

Pour les entreprises les dommages peuvent être lourds de conséquence. L'atteinte subie à son image provoque une perte de crédibilité pour sa clientèle. En effet, les clients devenant de plus en plus méfiants, perdent peu à peu la confiance qu'ils ont envers l'entreprise. La communication entre le client et l'entreprise devient plus difficile et elle devra sans cesse trouver des moyens permettant de justifier de l'authenticité de ses messages. Suivant le type d'attaque orchestrée, il est possible que l'entreprise subisse une perturbation de sa production, une divulgation de ses secrets industriels voire même une cessation d'activité partielle ou totale dans les cas les plus graves.

4.1.2 Ce que font les attaquants des données récoltées

Assurément, l'objectif principal des cybercriminels est de s'enrichir rapidement par des moyens illégaux. Les données récoltées par des attaques de phishing sont majoritairement utilisées pour extorquer les fonds des victimes sans que celle-ci ne s'en aperçoivent immédiatement. Une fois l'identité d'une victime volée, le pirate pourra s'en servir pour propager des logiciels malveillants voire même pour tromper les contacts de sa victime dans le but de perpétrer d'autres attaques. A un niveau supérieur, ces données peuvent être utilisées comme avantage économique dans le cadre de sabotage concurrentiel visant à monnayer des secrets industriels, diplomatiques voire militaires.

Ainsi, toutes les données et informations recueillies de manière frauduleuse servent à alimenter une économie parallèle souterraine, celle des marchés noirs du Darknet. Sur ce réseau virtuel privé anonyme, les données confidentielles de millions de victimes sont mises en vente par des cybercriminels sur des sites de vente et toutes les transactions y sont effectuées en Bitcoins. Sur ces sites de vente d'un genre particulier, il est possible d'acheter des données de cartes de crédit, des comptes de messageries piratés voire même des identités complètes. Par ailleurs, il est aussi possible, sur ces marchés noirs, de se procurer des kits complets de phishing comprenant imitations de page web et courrier électronique d'entreprise.

4.1.3 Les démarches à entreprendre suite à une attaque

Une victime de phishing doit impérativement prendre des mesures afin d'endiguer le problème le plus rapidement possible. Pour ce faire, il faut commencer par atteindre le service en ligne légitime afin de modifier le mot de passe enregistré, éventuellement en utilisant la question secrète. Dans l'hypothèse où cette manœuvre reste impossible, afin de reprendre le contrôle du compte, il est impératif de prendre directement contact avec le fournisseur de services concerné (banque, adresse de messagerie,…) de façon, d'une part, à les avertir de la situation et d'autre part, leur demander de bloquer le compte corrompu ainsi que de réinitialiser le mot de passe. Le fournisseur de services étant averti de l'attaque de phishing en cours, il pourra prendre les dispositions nécessaires de manière à lutter contre celle-ci. Le cas échéant, il est vivement conseiller de modifier le mot de passe volé dans tous les services en ligne où celui-ci est utilisé.

5. Les mesures de protection contre le phishing

5.1.1 Mesures comportementales

5.1.1.1 Se tenir informé au sujet des techniques de phishing

Il est essentiel de se tenir informé des nouvelles techniques et tentatives de phishing déployées dans la mesure où de nouvelles menaces apparaissent à tout moment. En restant sensibilisé aux nouvelles apparitions le risque de se faire avoir est nettement diminué. De plus, ne pas hésiter à informer son entourage lorsqu'une nouvelle attaque a été découverte.

5.1.1.2 Rester méfiant quant aux liens hypertextes et QR-Code

Cliquer sur un lien hypertexte sur un site web de confiance ne pose en principe aucun souci dans la mesure où ce site reste absolument authentique en n'ayant pas été piraté. En revanche, cliquer sur un lien hypertexte provenant d'un courrier électronique douteux ou par l'intermédiaire de messagerie instantanée peut s'avérer être fatal. Les liens hypertextes sont ainsi couramment utilisés pour rediriger les internautes peu méfiants vers des sites de phishing.

Afin d'éviter de tomber dans ce piège, ne jamais cliquer sur un lien hypertexte provenant de l'une des sources citées ci-dessus. Il est préférable d'ouvrir un nouveau navigateur et de saisir manuellement l'URL d'accès au service. De plus, dans le message, en pointant le curseur de la souris sur le lien hypertexte, sans cliquer dessus, l'URL complet s'affiche à l'écran. Le lien affiché dans le courrier électronique peut rediriger l'utilisateur vers une destination différente de ce qui est indiqué. Lorsqu'il s'agit d'un QR-Code, il faut faire preuve de la même méfiance que pour les liens hypertextes. Malheureusement, l'utilisateur ne peut pas connaître à l'avance la page web sur laquelle il sera conduit avant de scanner le QR-Code.

5.1.1.3 Vérifier si le site internet visité est sécurisé

La règle d'or sur internet serait de ne jamais se fier aveuglément à un site web, d'autant plus si le site en question ne montre aucune preuve de sécurité. Il est donc de rigueur d'être vigilant et réticent à vouloir fournir des d'informations personnelles en ligne. En principe, un site internet sécurisé ne devrait poser aucun problème lorsque des renseignements confidentiels y sont introduits. Mais étant donné le nombre de fraudes perpétrées sur la toile et la sophistication toujours plus pointue de celles-ci, il est indispensable de rester attentif même si le site en question paraît sécurisé.

Il est tout à fait envisageable que des pirates puissent créer des sites sécurisés afin de mieux tromper les victimes. Quelques indices, permettent de reconnaître un site

sécurisé. Il faut tout d'abord vérifier dans la barre d'adresse du navigateur si l'URL du site visité commence par « https ». Ceci a pour but de garantir, en principe, la confidentialité et l'intégrité des données transmises entre le client et le serveur.

De plus, une petite icône ressemblant à un cadenas fermé s'affichera aussi dans la barre d'adresse. Ce cadenas ainsi que le « https » indiquent que la connexion entre le navigateur et le site est chiffrée afin d'empêcher toute tentative d'interception de données transmises. Lorsque l'on clique sur ce petit cadenas, cela permet d'afficher le certificat de sécurité. Si le nom de l'organisation ou de l'entreprise s'affiche en vert conjointement au cadenas cela indique que le site en question a recours à un certificat de validation étendue.

Ce type de certificat sollicite un processus de contrôle largement plus drastique en comparaison aux autres types de certificats. En affichant en toutes lettres le nom de l'organisation ou de l'entreprise directement dans la barre d'adresse, l'internaute est informé directement sur le propriétaire du certificat.

5.1.1.4 Se méfier des pop-up

Un pop-up est une fenêtre intruse qui s'affiche devant la fenêtre principale du navigateur sans avoir forcément été sollicité par l'utilisateur. Les fenêtres pop-up sont régulièrement utilisées pour des tentatives de phishing en se faisant passer pour des fenêtres officielles du site web visité. La plupart des navigateurs proposent des options permettant de bloquer ces pop-up.

Si malgré tout un pop-up s'affiche, il vivement recommandé de ne pas cliquer sur les boutons affichés à l'intérieur de celui-ci car ils redirigent souvent l'internaute vers des sites malveillants. Pour fermer le pop-up, ne jamais cliquer sur un bouton annuler ou fermer mais cliquer directement sur le bouton croix en haut à droite du pop-up.

5.1.1.5 Ne jamais divulguer de renseignements personnels

En règle générale, les utilisateurs ne devraient jamais partager des informations d'ordre personnelles ou financières sur internet ou par téléphone. Ce sont des données sensibles qui peuvent être utilisées à mauvais escient dans la mesure où elles seraient interceptées par des personnes malintentionnées. Sur internet en particulier, il faut éviter de remplir sans discernement des formulaires demandant des renseignements confidentiels de type bancaire ou autre, si le site internet en question n'est pas sécurisé.

En cas de doute, il est judicieux de se renseigner sur la société du site internet exigeant ces informations voire même de les appeler depuis leur page web officielle si

un numéro de téléphone est disponible. Les entreprises sérieuses ne demandent jamais de renseignements confidentiels par courrier électronique ou par téléphone.

5.1.1.6 Se connecter régulièrement à ses comptes en ligne

Se connecter à ses différents comptes en ligne régulièrement, même si cela n'est pas nécessaire, permet de vérifier si toutes les données y sont restées intactes. Par ailleurs, il est judicieux de prendre l'habitude de changer fréquemment de mot de passe en optant toujours pour un mot de passe non trivial.

5.1.1.7 Vérifier le message reçu avec précaution

Un courrier électronique de phishing peut certifier être d'une entreprise authentique et fournir un lien qui redirige vers un site internet qui peut ressembler à s'y méprendre au site officiel de celle-ci. Afin de garantir la crédibilité du piège, le lien peut en outre conduire vers la politique de confidentialité de l'entreprise ou sur d'autres pages non pertinentes. La plupart du temps, les courriers électroniques génériques de phishing ne contiennent jamais le nom du destinataire mais commencent souvent par une formule impersonnelle de type « Cher client » suivi par un avis d'alerte demandant une réponse rapide.

En revanche, il est possible que soit mentionné dans ce courrier électronique des noms de personnes fictives qui travaillent soi-disant dans l'entreprise en question. Pour savoir si la personne dont le nom est présent dans le message existe effectivement dans l'entreprise, il est judicieux de contacter directement l'entreprise elle-même. Cependant, il ne faut jamais appeler avec un numéro de téléphone potentiellement affiché dans le courrier électronique mais au contraire utiliser les formulaires de contact disponibles sur le site officiel de l'entreprise.

Par ailleurs, lors de la réception d'un courrier électronique, il est primordial de s'interroger d'abord sur la probabilité que l'on ait communiqué son adresse de messagerie à l'établissement expéditeur du message. Si l'expéditeur est un ami ou une connaissance, il préférable de rester aussi aux aguets, car il se peut que cette personne ait été infectée ou son compte compromis. Dans la mesure du possible, vérifier avec cette personne l'authenticité du message.

Enfin, il faut être vigilant par rapport aux messages contenant d'éventuelles fautes d'orthographe ou de grammaire. En cas de doute, il est préférable de supprimer le message. Un expéditeur légitime ne recevant pas de réponse aura toujours la possibilité de relancer le destinataire en cas de non réponse de sa part.

5.1.1.8 Consulter ses relevés de compte régulièrement

Vérifier ses relevés de compte bancaire et de carte de crédit régulièrement permet contrôler si l'on n'a pas été victime d'une attaque. Il est important d'examiner chaque transaction afin de s'assurer qu'aucune transaction frauduleuse n'a été perpétrée à son insu. Si une irrégularité est détectée, il faut la signaler immédiatement à l'institution bancaire en téléphonant au numéro indiqué sur le relevé de compte.

5.1.1.9 Ne jamais télécharger des fichiers de sources peu fiables

La plupart des navigateurs proposent des paramètres afin de limiter l'accès aux pages web douteuses en affichant un message d'alerte pour avertir l'internaute. Lorsque le navigateur affiche un message indiquant que le site internet visité peut contenir des fichiers malveillants, il vivement conseillé ne de pas poursuivre la navigation sur ce site. De plus, il ne faut jamais télécharger des fichiers à partir de sites internet ou courriers électroniques suspects.

5.1.2 Mesures techniques

5.1.2.1 Utiliser un logiciel antivirus à jour

Un des premiers principes de sécurité sur internet est de recourir à un logiciel antivirus. Cela parait être une évidence mais il est important de rappeler que l'utilisation d'un logiciel antivirus protège contre les attaques quotidiennes que la navigation sur internet engendre. Il est important de bien mettre à jour son logiciel antivirus.

5.1.2.2 Garder son navigateur à jour

Fréquemment, des correctifs de sécurité sont publiés afin de corriger les failles de sécurité découvertes et exploitées par les pirates. Il est fortement conseillé de ne pas ignorer les messages de mise à jour émis par le navigateur de sorte que celui-ci soit toujours à sa dernière version.

5.1.2.3 Activer le filtre anti-spam de son client de courrier électronique

Etant donné que les attaques de phishing classiques consistent en l'envoi d'un message générique à un nombre élevé d'internautes, il est vraisemblable que ce type de message soit automatiquement reconnu comme spam par le client courrier électronique et marqué en fonction. Cependant, afin que les spams soit identifiés comme tels par le client courrier électronique, il est conseillé de vérifier dans ses paramètres si l'option filtre anti-spam est activée. Si aucun filtre n'est disponible, il est vivement conseillé d'installer un logiciel anti-spam sur son ordinateur.

5.1.2.4 Utiliser des pare-feu

Un pare-feu est un système de protection, logiciel ou matériel, pour ordinateur protégeant des intrusions externes provenant d'internet ou de réseaux tiers. Selon les paramètres définis, il empêche ou autorise les informations à accéder à l'ordinateur, de même qu'il peut empêcher un ordinateur d'envoyer des contenus logiciels malveillants à d'autres ordinateurs. Le pare-feu agit en quelque sorte comme un tampon entre l'ordinateur de l'utilisateur et les intrusions extérieures.

Il est recommandé d'utiliser les deux différents types de pare-feu. A savoir, le pare-feu de bureau qui est de type logiciel et le pare-feu de réseau qui est de type matériel. Utiliser conjointement ces deux types de pare-feu réduit considérablement les chances des pirates d'infiltrer l'ordinateur d'un utilisateur.

5.1.2.5 Activer le filtre anti-phishing des navigateurs

Certains navigateurs populaires comme Internet Explorer, Google Chrome et Mozilla Firefox proposent des fonctions intégrées de protection contre des sites internet répertoriés comme sites de phishing. En activant ce filtre dans les paramètres du navigateur, un message de mise en garde sera affiché lorsque l'utilisateur tentera d'accéder à un site soupçonné de pratiquer du phishing.

5.1.2.6 Installer une barre d'outil anti-phishing

Des modules anti-phishing peuvent être proposés dans des barres d'outils pour navigateurs populaires. En comparant le site internet visité aux listes de sites de phishing connus, ces barres d'outils effectuent un contrôle systématique afin de vérifier le risque de fraude. L'internaute est immédiatement informé par notification lorsqu'un site répertorié dans la liste noire est visité. Ci-dessous, quelques exemples de barres d'outils disponibles en téléchargement sur le web :

5.1.2.6.1 WOT

WOT, signifiant « Web of Trust », est une extension compatible avec les navigateurs Mozilla Firefox, Internet Explorer, Google Chrome et Opera permettant d'évaluer le niveau de fiabilité d'un site internet. A chaque recherche ou consultation de site internet, WOT émettra pour l'internaute une évaluation sous forme de notes et de classification ainsi qu'un avertissement lorsqu'il y a un risque potentiel sur le site en question. Principalement basé sur les avis des internautes eux-mêmes, les évaluations de WOT fonctionnent grâce à un système collaboratif. Il transmet le nom de domaine du site au serveur WOT pour obtenir des informations concernant le site.

5.1.2.6.2 TrafficLight de Bitdefender

TrafficLight est une extension développée par Bitdefender pour les navigateurs Mozilla Firefox, Google Chrome et Safari permettant d'intercepter, de traiter et filtrer le trafic web afin de bloquer le contenu malveillant. Chaque page web visitée par l'internaute est scrutée par TrafficLight pour détecter les tentatives de phishing et d'installation de malwares. De plus, les liens des sites de réseaux sociaux sont également analysés et bloqués s'ils s'avèrent être douteux.

5.1.2.6.3 Link Extend

Link Extend est une extension pour le navigateur Mozilla Firefox apparaissant sous la forme d'une barre d'outils munie d'une barre de recherche avertissant contre les tentatives de connexion aux sites internet répertoriés comme risqués. Les pages web considérées comme à haut risque sont bloquées. Chaque résultat de recherche Google, établi à travers la barre de recherche ou non, est annoté par des messages prévenant l'internaute s'il s'agit d'un site internet malveillant.

5.1.2.6.4 McAfee Site Advisor

Mcafee Site Advisor est un module pour les navigateurs avertissant l'utilisateur de la fiabilité d'un site internet lorsqu'il est visité. Le niveau de fiabilité est affiché sous forme d'icônes de différentes couleurs dans la barre d'outils ainsi qu'à la suite de chaque lien dans les résultats d'un moteur de recherche.

5.1.2.6.5 AVG Link Scanner

AVG Link Scanner est un module pour navigateurs Internet Explorer et Mozilla Firefox qui analyse pendant la navigation l'URL et les liens des sites internet visités en alertant l'utilisateur des potentielles menaces cachées. Les liens contenus dans les courriers électroniques et messages instantanés sont également surveillés.

5.1.2.6.6 Netcraft Toolbar

Netcraft Toolbar est un module de protection contre les sites de phishing à intégrer au navigateur. Il s'apparente à une barre d'outils disposant d'une jauge à risque qui évalue en temps réel le taux de danger présent sur la page web visitée. Cet outil s'appuie sur une base de données des sites frauduleux très performante alimentée notamment par une communauté d'utilisateurs actifs.

5.1.2.6.7 PhishTank SiteChecker

PhishTank SiteChecker est une extension pour Mozilla Firefox qui utilise les données provenant du site internet anti-phishing www.phishtank.com afin de prévenir les utilisateurs si le site internet visité est référencé comme dangereux.

5.1.2.6.8 Web Security Guard

Web Security Guard est une extension pour les navigateurs Google Chrome et Mozilla Firefox qui informe l'internaute sur la réputation d'un site internet avant que celui-ci n'entame une navigation.

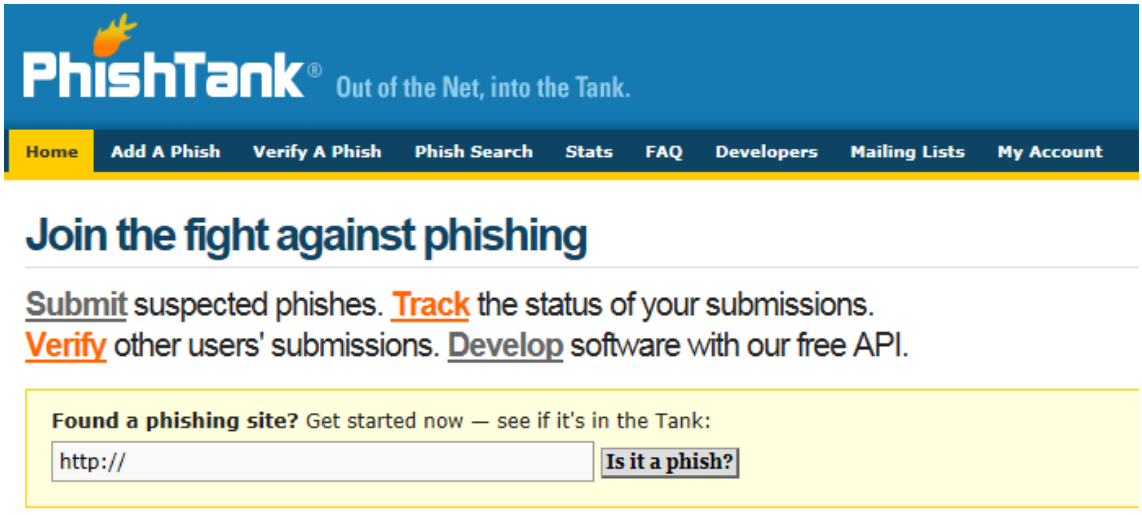
5.1.2.7 Vérifier la réputation d'un site internet à partir de son URL

Dans la lutte contre le phishing, des éditeurs ont publié sur leur site des outils gratuits de détection de liens frauduleux en ligne. Ces outils effectuent une analyse en temps réel du niveau de dangerosité d'un site internet en comparant son URL à une base de données de liens malicieux. Il suffit de copier et coller le lien d'un site suspect dans l'outil de détection et de lancer la recherche pour que le résultat s'affiche instantanément. De cette manière, l'internaute est averti immédiatement s'il encourt un risque potentiel en visitant un site.

5.1.2.7.1 PhishTank

PhishTank est un site collaboratif pour lutter contre le phishing. Il propose un système de vérification de site de phishing basé sur une communauté d'internautes qui soumettent des sites de phishing présumés tandis que d'autres les évaluent comme menaces potentielles ou non. Un des avantages de cet outil est qu'il propose d'afficher une capture d'écran du site recherché.

Figure 2 : PhishTank

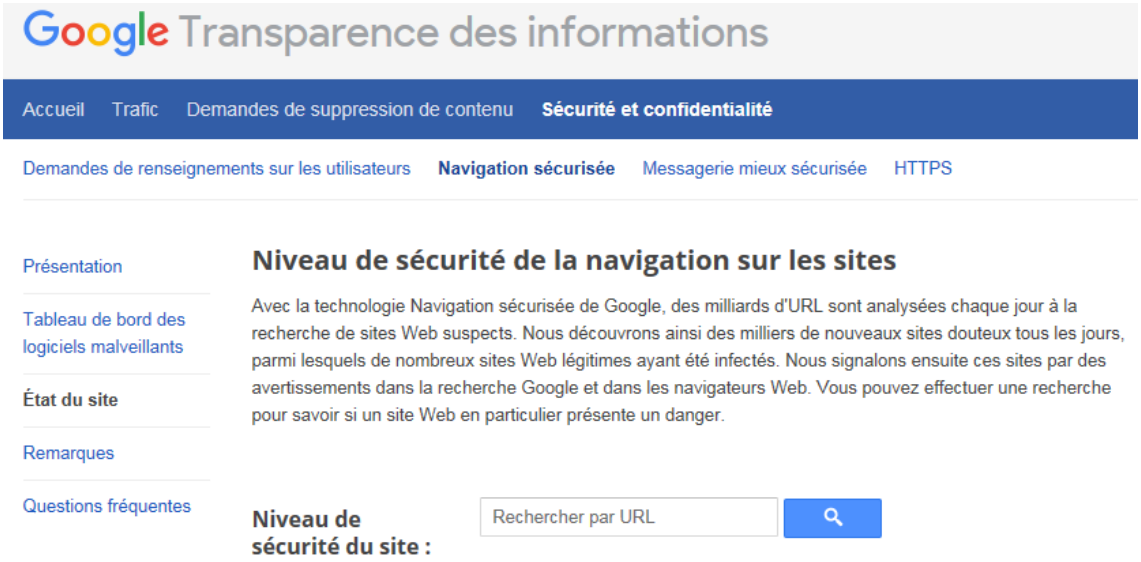


(http://www.phishtank.com/)

5.1.2.7.2 Google Safe Browsing Diagnostic

Google Safe Browsing est service fourni par Google qui enregistre dans une liste noire des URL de sites internet dont le contenu s'apparente à du phishing. Les navigateurs Google Chrome, Apple Safari et Mozilla Firefox se servent des informations contenues dans cette liste pour évaluer les menaces potentielles.

Figure 3 : Google Safe Browsing Diagnostic

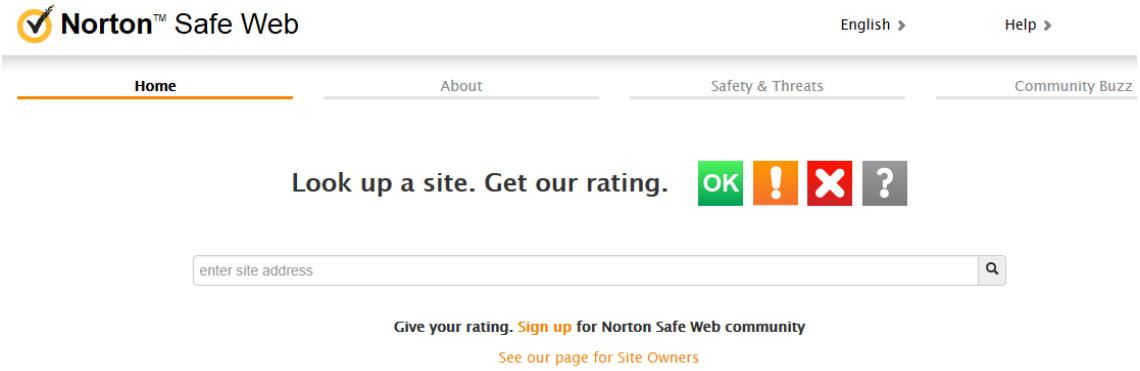


(https://www.google.com/transparencyreport/safebrowsing/diagnostic/)

5.1.2.7.3 Norton Safe Web

Norton Safe Web est un service développé par la société Symentec créé pour aider les utilisateurs à identifier les sites internet douteux. Il fournit des renseignements basés sur l'analyse automatisée ainsi que les commentaires des internautes.

Figure 4 : Norton Safe Web



(https://safeweb.norton.com/)

5.1.2.7.4 Is It Phishing

Is It Phishing est un service offert par la société Vade Retro, fournisseur de solutions de sécurité pour messagerie électronique, destiné d'une part à aider les utilisateurs identifier les sites malveillants et d'autre part à prévenir les entreprises victimes d'attaques. Ce service permet non seulement d'évaluer l'URL d'un site mais aussi de savoir si le nom d'une entreprise est associé à une attaque de phishing. De plus, il conserve dans sa base de données toutes les sociétés ayant été victimes d'une attaque en incluant une capture d'écran et la date de détection de celle-ci.

Figure 5 : Is It Phishing

(http://isitphishing.org/)

5.1.2.7.5 Scan URL

Scan URL est un site proposant d'analyser la réputation d'un site internet à partir de son URL. Ses résultats sont basés sur les analyses fournies par les services de Google Safe Browsing Diagnostic, PhishTank et Web of Trust (WOT).

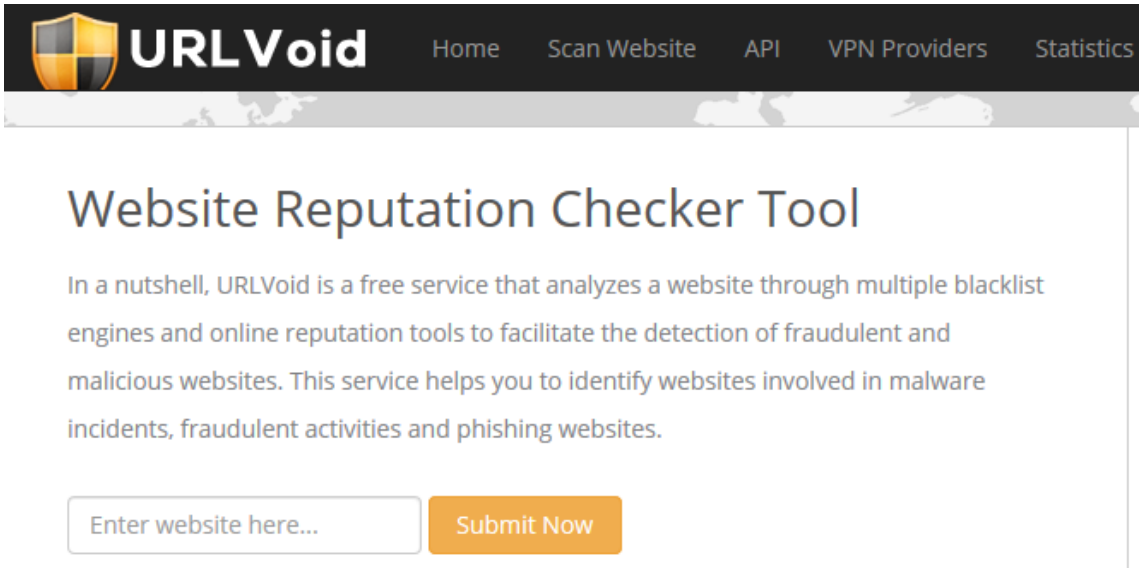
Figure 6 : Scan URL

(http://scanurl.net/)

5.1.2.7.6 URL Void

URL Void est un service d'analyse de réputation de site internet aidant les utilisateurs à identifier ceux impliqués dans des activités frauduleuses de phishing. Pour cela, il se base sur plusieurs moteurs de liste de noire et d'outils de réputation en ligne pour effectuer la détection.

Figure 7 : URL Void

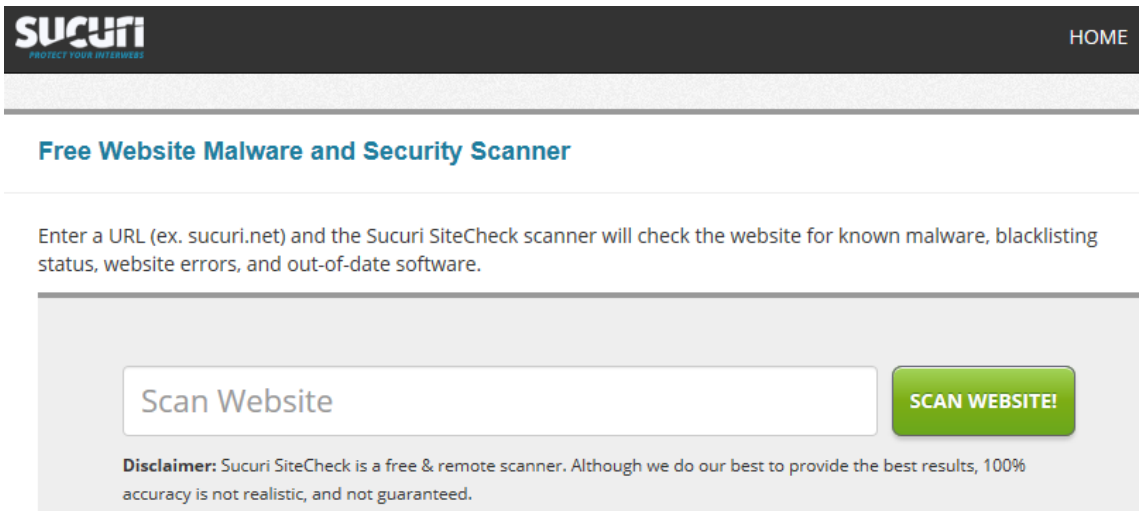


(http://www.urlvoid.com/)

5.1.2.7.7 Sucuri Site Check

Sucuri Site Check est un service développé par la société Sucuri Inc destiné à contrôler le niveau de dangerosité d'un site internet. Son scanner d'URL permet d'évaluer la réputation d'un site internet.

Figure 8 : Sucuri Site Check



(https://sitecheck.sucuri.net/)

5.1.2.7.8 Online Link Scan

Online Link Scan est site fournissant la possibilité aux internautes de scanner l'URL d'un site internet afin d'en connaître sa réputation. Ses résultats sont basés sur les analyses fournies par les services de PhishTank, Google Safe Browsing Diagnostic et Web Security Guard.

Figure 9 : Online Link Scan

(http://onlinelinkscan.com/)

6. Les moyens de lutte mis en œuvre

6.1 En Suisse

6.1.1 MELANI

MELANI, signifiant en allemand, « Melde- und Analysestelle Informationssicherung » est la Centrale d'enregistrement et d'analyse pour la sûreté de l'information de la Confédération suisse opérationnelle depuis le 1er octobre 2004. Elle est chargée par le Conseil fédéral d'assurer la protection des infrastructures nationales critiques et vitales relevant de l'information et de la communication.

Son objectif dans le domaine de la sécurité informatique étant d'anticiper d'éventuelles nouvelles menaces et de résoudre les problèmes existants. Elle est le fruit de la coopération entre le Département fédéral des finances (DFF) et le département fédéral de la défense, de la protection de la population et des sports (DDPS).

Les informations publiées sur le site internet de MELANI sont destinées à toute personne physique ou morale utilisant un ordinateur connecté à internet, du particulier à la PME. Ses informations englobent des formulaires de signalement de problèmes relatif à la navigation sur internet, des rapports sur les principales tendances en matière d'escroquerie sur les technologies de l'information et de la communication ainsi que des renseignements à propos des dangers actuels d'internet. Par ailleurs, MELANI propose des règles comportementales destinées aux internautes afin qu'ils adoptent un comportement adéquat lors de leur navigation sur internet.

Chaque annonce transmise est analysée et évaluée. Dans la mesure où un danger imminent a été découvert, MELANI se charge de prévenir l'hébergeur ainsi que le propriétaire du site internet lorsque la page est hébergée sur un site piraté afin de solliciter la suppression du contenu frauduleux. De plus, afin de contribuer à lutter efficacement contre ces menaces, les URL de pages web estimées comme néfastes sont transmises aux navigateurs web, aux administrateurs de listes noires ainsi qu'à des entreprises actives dans le domaine de la sécurité informatique. N'étant pas rattaché à un corps de police, MELANI n'entreprend aucune investigation pénale en rapport avec les annonces reçues et de ce fait n'engage aucune poursuite à l'encontre des cybercriminels.

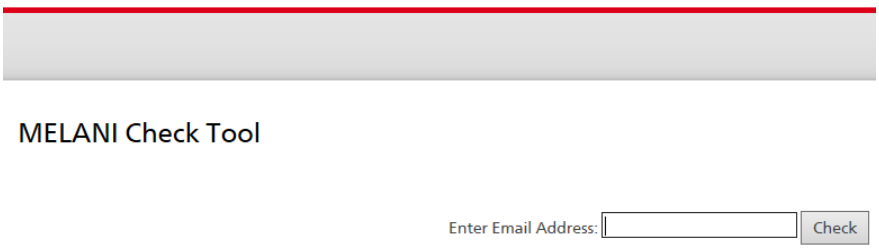
Figure 10 : Formulaire d'annonce MELANI

(https://www.antiphishing.ch/fr/)

6.1.1.1 MELANI Check Tool

La Centrale d'enregistrement et d'analyse pour la sûreté de l'information a recensé une liste d'environ 6000 adresses de comptes de messageries électroniques suisses ayant fait l'objet d'un piratage du mot de passe. Ces comptes qui ont été signalés ont pu potentiellement être utilisés à des fins illicites notamment pour des attaques de phishing. MELANI propose sur son site www.checktool.ch un outil permettant de vérifier si une adresse de messagerie électronique est répertoriée dans sa base de données d'adresses corrompues.

Figure 11 : MELANI Check Tool



(https://www.checktool.ch/)

6.1.2 SCOCI

Le SCOCI est le Service national de coordination de la lutte contre la criminalité sur Internet inhérent à la police judiciaire fédérale (PJF), elle-même division principale de l'Office fédéral de la police (fedpol). Il est chargé d'être l'interlocuteur privilégié pour toute personne désirant communiquer l'existence de sites internet dont le contenu est compromettant. Le SCOCI est le fruit de la collaboration entre le Département Fédéral de Justice et Police (DFJP) et la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP).

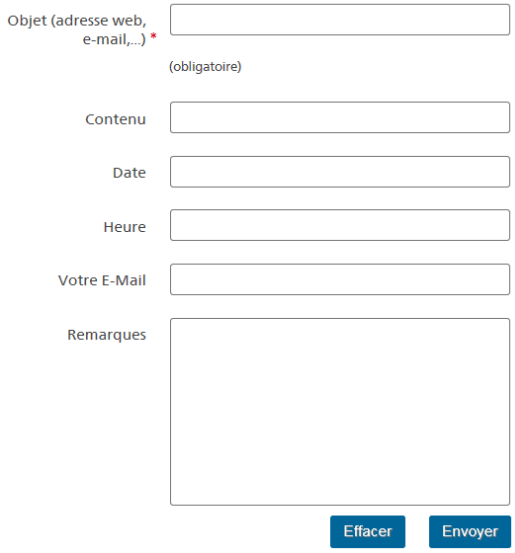
En tant que centre de compétence technique pour le public, les administrations et les fournisseurs d'accès internet dans le domaine de la criminalité sur internet, il s'occupe d'analyser les données suspectes en vue de les transmettre aux autorités de poursuites pénales compétentes en Suisse ainsi qu'aux services étrangers exerçant la même fonction. Pour ce qui a trait à la cybercriminalité sur le plan international, le SCOCI collabore de manière proactive avec Interpol, Europol et le FBI en jouant le rôle d'intermédiaire privilégié entre les cantons et ces organisations. Il est notamment partenaire du Centre européen de lutte contre la cybercriminalité EC3 d'Europol en étant membre du Focal Point (FP) CYBORG.

L'équipe de collaborateurs affiliés au SCOCI est pluridisciplinaire. Elle se compose de spécialistes en matière de protocoles internet et de sécurité de l'information, de techniciens réseau, d'analystes criminels, de juristes et de policiers. Le SCOCI a pour responsabilité de gérer la coordination dans les opérations menées entre les différents corps de police cantonaux en permettant de diffuser de manière efficace les suspicions qui lui sont annoncées.

Ainsi, en termes de cybercriminalité en Suisse, les prérogatives incombant à la police criminelle comme l'enregistrement de plaintes et les investigations, sont essentiellement endossées par les corps de police cantonaux et municipaux offrant par conséquent une meilleure proximité avec les citoyens.

Enfin, le SCOCI met à disposition sur son site internet un formulaire d'annonce permettant de signaler et de dénoncer toutes tentatives d'arnaque sur le web. En se basant sur les annonces transmises au moyen de ce formulaire, le SCOCI publie les alertes sur son site internet et sur les réseaux sociaux participant ainsi à la prévention.

Figure 12 : Formulaire d'annonce SCOCI

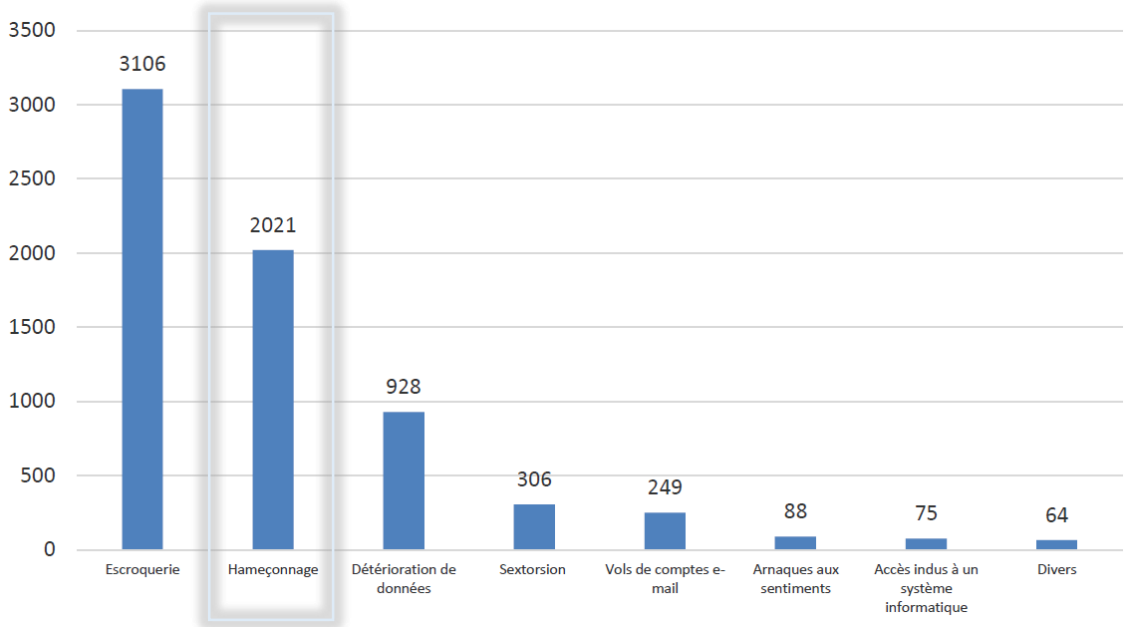


(https://www.cybercrime.admin.ch/kobik/fr/home/meldeformular/meldeformular.html)

6.1.2.1 Statistique d'annonces reçues

Le graphique ci-dessous représente le nombre total d'annonces, relatif aux infractions contre le patrimoine, transmises via le formulaire du Service national de coordination de la lutte contre la criminalité au cours de l'année 2014. Sur un total de 6837 annonces, 2021 annonces se rapportent à du phishing représentant ainsi le deuxième type d'annonce le plus transmis. A titre informatif, le terme « escroquerie » représentant la majorité des annonces fait référence aux fausses annonces publiées sur des sites de petites annonces ainsi que des plateformes d'enchères.

Figure 13 : Statistique d'annonces reçues via le formulaire d'annonce



(Rapport annuel 2014 SCOCI, p. 7)

6.2 En Europe

6.2.1 EC3

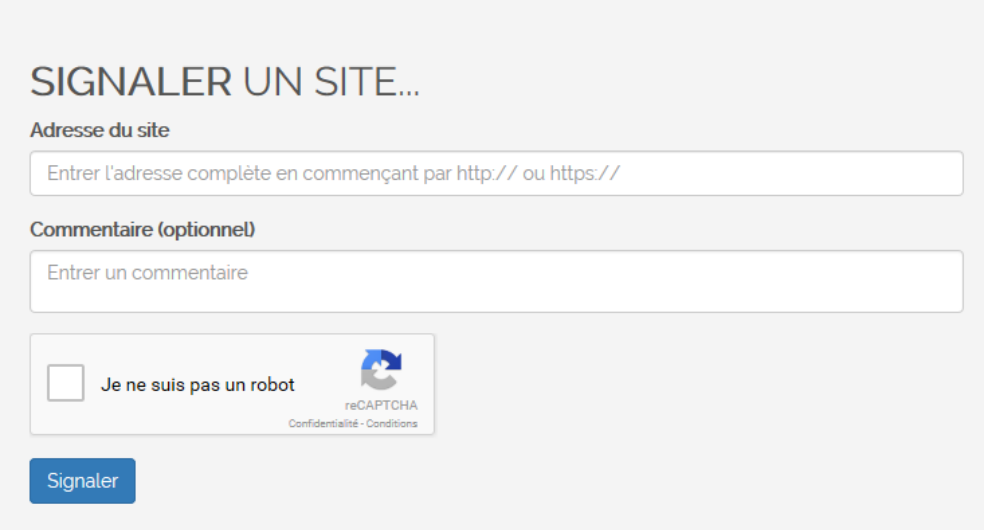
EC3 est le Centre européen de lutte contre la cybercriminalité au sein d'Europol. Fondé en 2013, il a pour objectif de renforcer la protection des citoyens, des entreprises et des gouvernements européens face à la cybercriminalité. Il met à disposition ses compétences et connaissances pour les membres de l'Union européenne et pour les Etat tiers leur fournissant un appui opérationnel et analytique lors d'enquêtes et opérations de police.

Sa division FP CYBORG est spécifiquement orientée sur la lutte contre les différentes formes de cybercriminalité touchant aux systèmes informatiques critiques en mettant l'accent sur les cybercrimes perpétrés par des groupes organisés générant de grands profits criminels. EC3 met à disposition sur son site des liens permettant d'atteindre les sites internet officiels de déclaration de cybercrimes des Etats membres.

6.2.2 Phishing Initiative

Phishing Initiative est un projet européen à but non lucratif de lutte contre les attaques de phishing. Lancé en janvier 2011 par Microsoft, PayPal et LEXSI, il est cofinancé par le programme de Prévention et Lutte contre le Crime de l'Union Européenne[8]. Ce projet offre la possibilité aux internautes de dénoncer par l'entremise d'un formulaire, les sites internet francophones suspectés de pratiquer le phishing. Aussitôt dénoncé, le site suspect fait l'objet d'abord d'une introspection par une équipe d'analystes, suivi d'une validation de son blocage par les navigateurs s'il est jugé frauduleux.

Figure 14 : Formulaire d'annonce Phishing Initiative



(https://phishing-initiative.fr/contrib/)

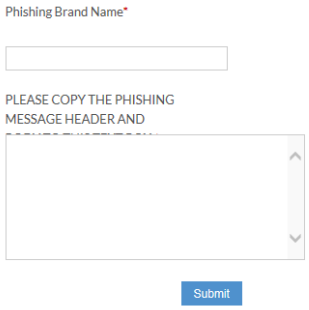
[8] Source : https://phishing-initiative.eu/

6.3 Dans le monde

6.3.1 Anti-Phishing Working Group

L'Anti-Phishing Working Group (APWG) est un consortium international à but non lucratif regroupant des entreprises de services et de produits, des organismes gouvernementaux, des associations commerciales, des organisations internationales, des institutions financières, des fournisseurs d'accès internet et des organisations non gouvernementales. Fondé en 2003, cette association est concentrée sur la lutte contre le vol d'identité et les fraudes inhérentes aux attaques de phishing et dénombre plus de 2000 entreprises et organismes membres dans le monde entier. Le site internet de l'APWG met à disposition un formulaire de rapport pour tous sites et courriers électroniques suspectés de phishing.

Figure 15 : Formulaire APWG



(http://www.antiphishing.org/report-phishing/overview/)

7. Les bases légales suisses

Les bases légales applicables en Suisse en matière de cybercriminalité en rapport avec les attaques de phishing se fondent sur une série d'articles de loi du Code pénal ainsi que sur un article de la Loi fédérale sur la protection des marques et des indications de provenance.

7.1 Code pénal suisse

7.1.1 Infraction contre le patrimoine

7.1.1.1 Article 143 : Soustraction des données

« [1] Celui qui, dans le dessein de se procurer ou de procurer à un tiers un enrichissement illégitime, aura soustrait, pour lui-même ou pour un tiers, des données enregistrées ou transmises électroniquement ou selon un mode similaire, qui ne lui étaient pas destinées et qui étaient spécialement protégées contre tout accès indu de sa part, sera puni d'une peine privative de liberté de cinq ans au plus ou d'une peine pécuniaire.

[2] La soustraction de données commise au préjudice des proches ou des familiers ne sera poursuivie que sur plainte. » *(Art 143, CP)*

7.1.1.2 Article 143 bis : Accès indu à un système informatique

« [1] Quiconque s'introduit sans droit, au moyen d'un dispositif de transmission de données, dans un système informatique appartenant à autrui et spécialement protégé contre tout accès de sa part est, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

[2] Quiconque met en circulation ou rend accessible un mot de passe, un programme ou toute autre donnée dont il sait ou doit présumer qu'ils doivent être utilisés dans le but de commettre une infraction visée à l'al. 1 est puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. »

(Art 143 bis, CP)

7.1.1.3 Article 144 : Dommage à la propriété

« [1] Celui qui aura endommagé, détruit ou mis hors d'usage une chose appartenant à autrui ou frappée d'un droit d'usage ou d'usufruit au bénéfice d'autrui sera, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

[2] Si l'auteur a commis le dommage à la propriété à l'occasion d'un attroupement formé en public, la poursuite aura lieu d'office.

[3] Si l'auteur a causé un dommage considérable, le juge pourra prononcer une peine privative de liberté de un à cinq ans. La poursuite aura lieu d'office. »

(Art 144, CP)

7.1.1.4 Article 144 bis : Détérioration des données

« 1. Celui qui, sans droit, aura modifié, effacé, ou mis hors d'usage des données enregistrées ou transmises électroniquement ou selon un mode similaire sera, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

Si l'auteur a causé un dommage considérable, le juge pourra prononcer une peine privative de liberté de un à cinq ans. La poursuite aura lieu d'office.

2. Celui qui aura fabriqué, importé, mis en circulation, promu, offert ou d'une quelconque manière rendu accessibles des logiciels dont il savait ou devait présumer qu'ils devaient être utilisés dans le but de commettre une infraction visée au ch. 1, ou qui aura fourni des indications en vue de leur fabrication, sera puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. » (Art 144 bis, CP)

7.1.1.5 Article 147 : Utilisation frauduleuse d'un ordinateur

« [1] Celui qui, dans le dessein de se procurer ou de procurer à un tiers un enrichissement illégitime, aura, en utilisant des données de manière incorrecte, incomplète ou indue ou en recourant à un procédé analogue, influé sur un processus électronique ou similaire de traitement ou de transmission de données et aura, par le biais du résultat inexact ainsi obtenu, provoqué un transfert d'actifs au préjudice d'autrui ou l'aura dissimulé aussitôt après sera puni d'une peine privative de liberté de cinq ans au plus ou d'une peine pécuniaire.

[2] Si l'auteur fait métier de tels actes, la peine sera une peine privative de liberté de dix ans au plus ou une peine pécuniaire de 90 jours-amende au moins.

[3] L'utilisation frauduleuse d'un ordinateur au préjudice des proches ou des familiers ne sera poursuivie que sur plainte.

Si l'auteur fait métier de tels actes, le juge pourra prononcer une peine privative de liberté de un à cinq ans. » (Art 147, CP)

7.1.2 Faux dans les titres

7.1.2.1 Article 251 : Faux dans les titres

« 1. Celui qui, dans le dessein de porter atteinte aux intérêts pécuniaires ou aux droits d'autrui, ou de se procurer ou de procurer à un tiers un avantage illicite,

aura créé un titre faux, falsifié un titre, abusé de la signature ou de la marque à la main réelles d'autrui pour fabriquer un titre supposé, ou constaté ou fait constater faussement, dans un titre, un fait ayant une portée juridique,

ou aura, pour tromper autrui, fait usage d'un tel titre,

sera puni d'une peine privative de liberté de cinq ans au plus ou d'une peine pécuniaire.

2. Dans les cas de très peu de gravité, le juge pourra prononcer une peine privative de liberté de trois ans au plus ou une peine pécuniaire. » (Art 251, CP)

7.1.3 Infraction contre le domaine secret ou le domaine privé

7.1.3.1 Article 179 novies : Soustraction de données personnelles

« Celui qui aura soustrait d'un fichier des données personnelles sensibles ou des profils de la personnalité qui ne sont pas librement accessibles sera, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. » (Art 179 novies, CP)

7.2 Loi fédérale sur la protection des marques

7.2.1 Dispositions pénales

7.2.1.1 Article 62 : Usage frauduleux

« [1] Sur plainte du lésé, est puni d'une peine privative de liberté d'un an au plus ou d'une peine pécuniaire celui qui:

a. désigne illicitement des produits ou des services par la marque d'un tiers en vue de tromper autrui, faisant croire ainsi qu'il s'agissait de produits ou de services originaux;

b. offre ou met en circulation comme originaux des produits désignés illicitement par la marque d'un tiers ou offre ou fournit comme originaux des services désignés par la marque d'un tiers.

[2] Si l'auteur de l'infraction agit par métier, il est poursuivi d'office. La peine est une peine privative de liberté de cinq ans au plus ou une peine pécuniaire. En cas de peine privative de liberté, une peine pécuniaire est également prononcée.

[3] Celui qui importe, exporte, fait transiter ou entrepose des produits, dont il sait qu'ils sont destinés à être illicitement offerts ou mis en circulation dans un but de tromperie est, sur plainte du lésé, puni d'une amende de 40 000 francs au plus. » *(Art 62, LMP)*

7.3 L'usurpation d'identité

En Suisse, l'usurpation d'identité en tant que telle n'est pas considérée comme un délit au sens du code pénal. De ce fait, la police n'est pas en mesure de pouvoir enregistrer de plainte pour ce type de cas. C'est actuellement un vide juridique car rien n'indique en droit pénal qu'il est défendu de se faire passer pour quelqu'un d'autre sur internet.

Comme vu précédemment, la loi suisse punit uniquement l'action d'accéder au système informatique d'une autre personne et non pas le fait de se faire passer pour autrui. Cela signifie que l'usurpation d'identité n'est aucunement considérée comme une circonstance aggravante au moment de fixer la peine malgré le fait qu'elle démontre une certaine préméditation.

En revanche, l'usurpation d'identité servant à commettre d'autres délits, la police sera en mesure de pouvoir enregistrer une plainte que cela soit par rapport à une escroquerie, un vol ou d'autres situations. Selon le Conseil fédéral, le droit pénal ne présente aucune lacune en la matière car l'usurpation d'identité n'est pas une fin en soi mais sert à une intention spécifique.

Contrairement à la Suisse, plusieurs pays de l'Union Européenne ont déjà commencé à légiférer sur ce problème, notamment la France qui considère l'usurpation d'identité comme un délit au travers d'une atteinte aux biens. L'article 226-4-1 du code pénal français[9] entré en vigueur le 14 mars 2011 stipule que :

« Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende.

Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne. » *(Art 226-4-1, CP)*

[9] Source : https://www.legifrance.gouv.fr/

8. Cas réels

8.1 Courriers électroniques au nom d'entités de confiance

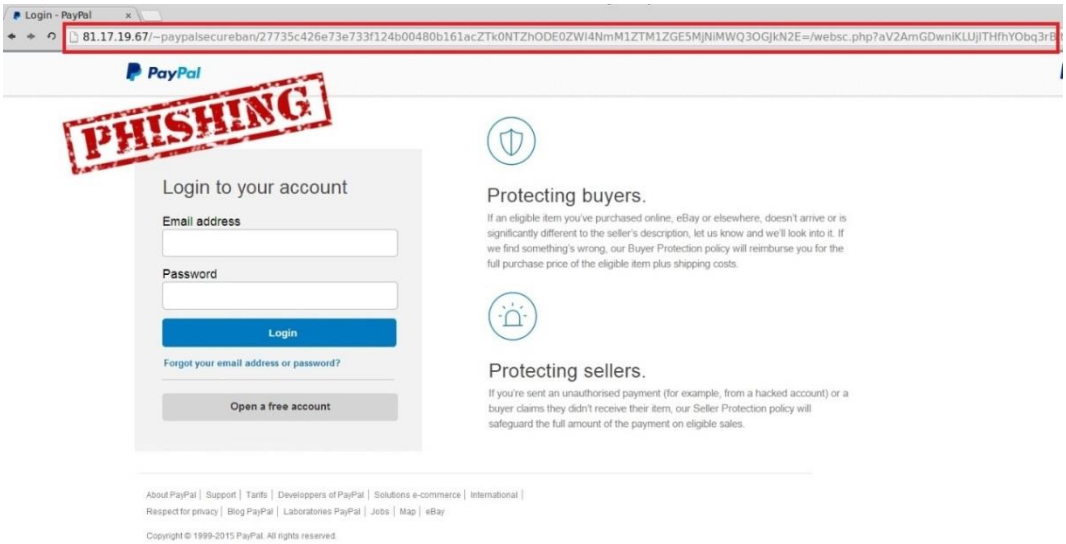
8.1.1 Paypal

Par ce courrier électronique, les fraudeurs informent leurs victimes d'un supposé problème lié à leur compte qui engendrerait une limitation des possibilités d'utilisation de celui-ci. Sous prétexte de régler le problème et pour pouvoir bénéficier à nouveau de l'ensemble des options du compte, les victimes sont invitées à fournir leurs identifiants, à savoir leur nom d'utilisateur et mot de passe.

Figure 16 : Faux courrier électronique de Paypal

(https://www.cybercrime.admin.ch/kobik/fr/home/warnmeldungen/meldungen/2015/2015-05-06.html)

Figure 17 : Fausse page web de Paypal

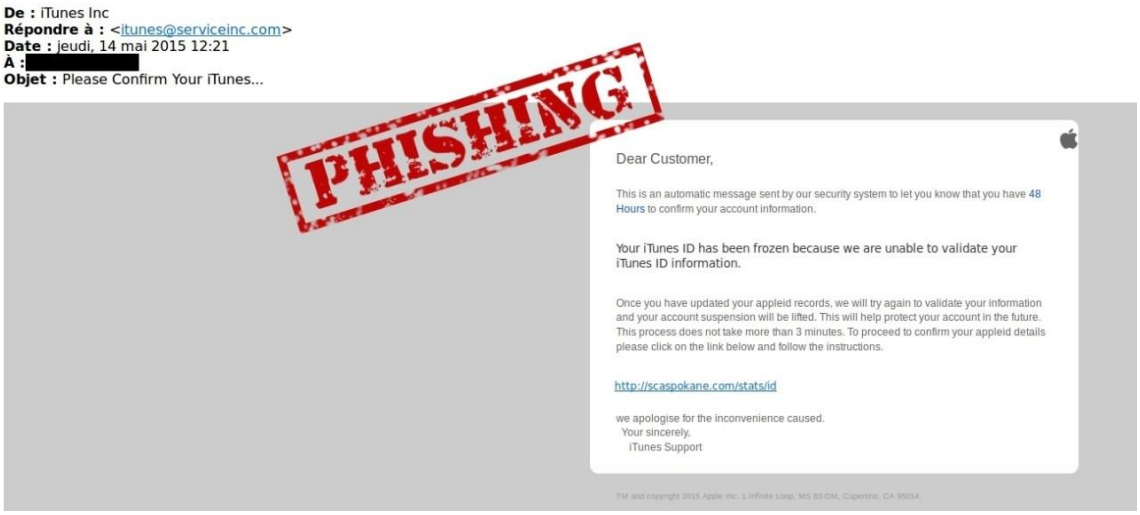


(https://www.cybercrime.admin.ch/kobik/fr/home/warnmeldungen/meldungen/2015/2015-05-06.html)

8.1.2 Apple

Par ce courrier électronique, les fraudeurs font croire à leurs victimes que leur compte iTunes a été bloqué car il n'a pas été validé. Afin de s'emparer des données d'accès au compte, il est demandé à la victime de suivre un lien et de fournir ses identifiants, nom d'utilisateur et mot de passe, sous prétexte de réactivation du compte.

Figure 18 : Faux courrier électronique d'Apple



(https://www.cybercrime.admin.ch/kobik/fr/home/warnmeldungen/meldungen/2015/2015-05-15.html)

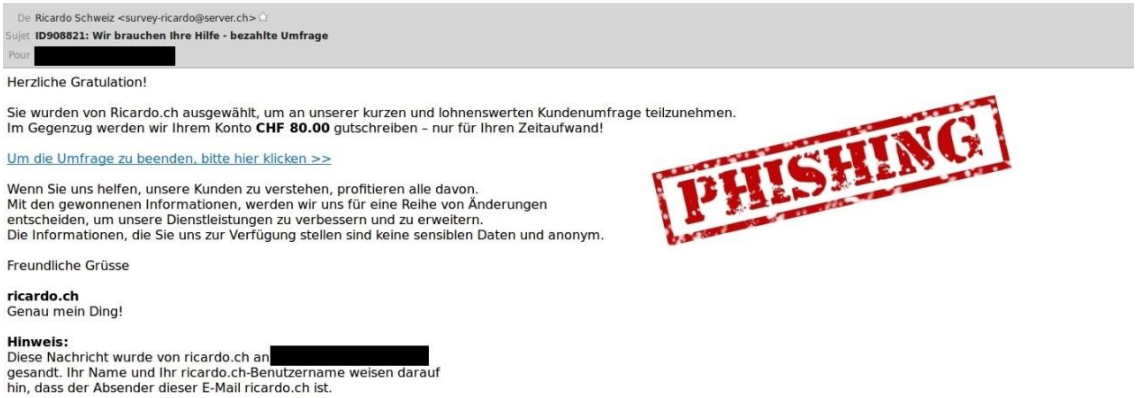
Figure 19 : Fausse page web d'Apple

(https://www.cybercrime.admin.ch/kobik/fr/home/warnmeldungen/meldungen/2015/2015-05-15.html)

8.1.3 Ricardo.ch

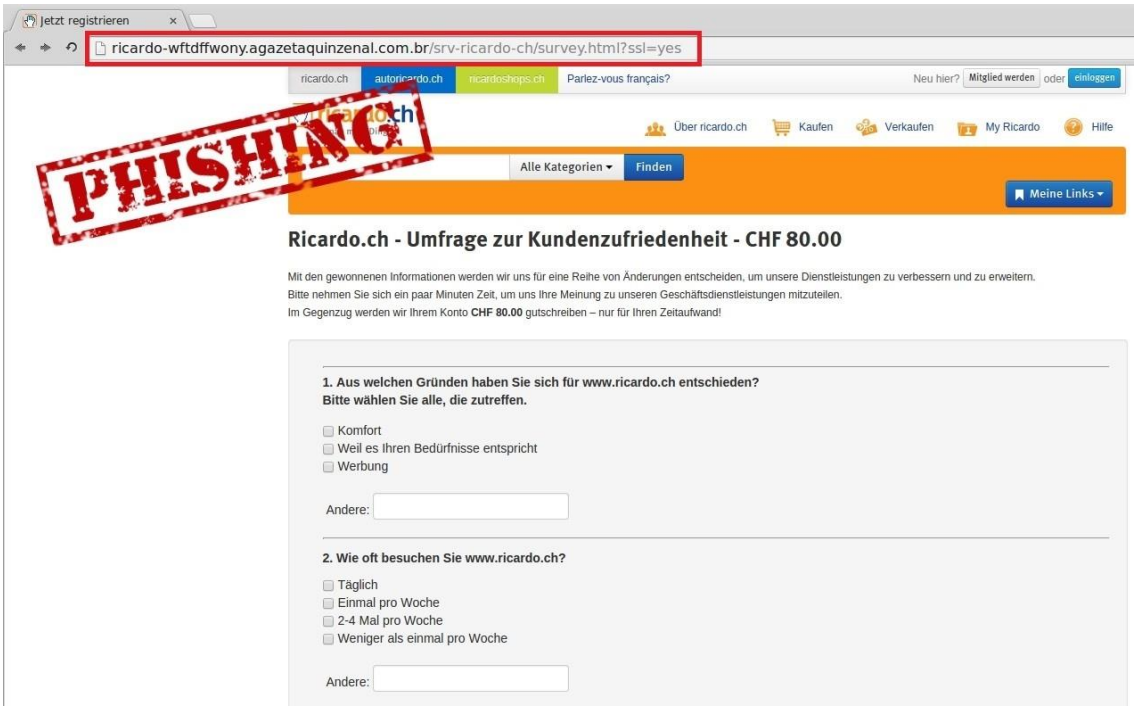
Par ce courrier électronique, les fraudeurs font croire à leurs victimes qu'ils ont été tirés au sort pour participer sur Ricardo.ch à un sondage rémunéré sous forme de questionnaire de satisfaction. Lorsque la victime clique sur le lien et répond à l'intégralité du questionnaire, il lui est demandé d'introduire ses coordonnées personnelles et son numéro de carte de crédit, avec son code sécurité, afin de pouvoir toucher la rétribution.

Figure 20 : Faux courrier électronique de Ricardo.ch



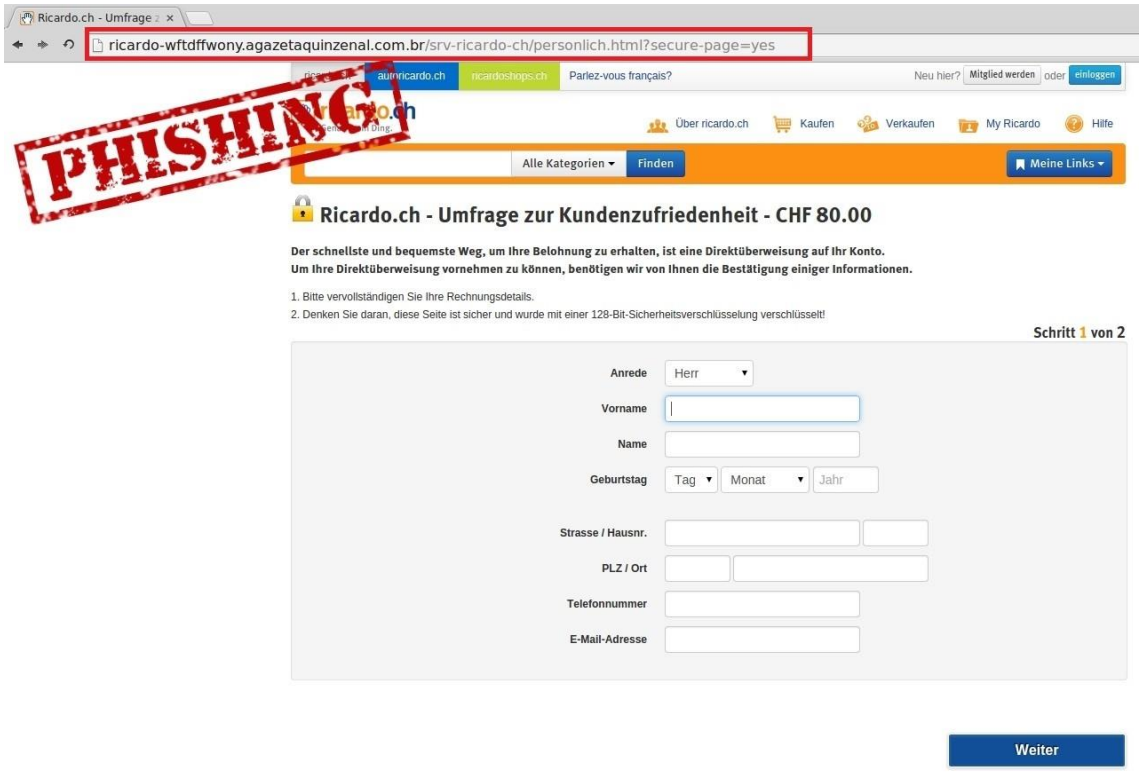
(https://www.cybercrime.admin.ch/kobik/fr/home/warnmeldungen/meldungen/2015/2015-05-19.html)

Figure 21 : Fausse page web de sondage de Ricardo.ch



(https://www.cybercrime.admin.ch/kobik/fr/home/warnmeldungen/meldungen/2015/2015-05-19.html)

Figure 22 : Fausse page web de formulaire de Ricardo.ch

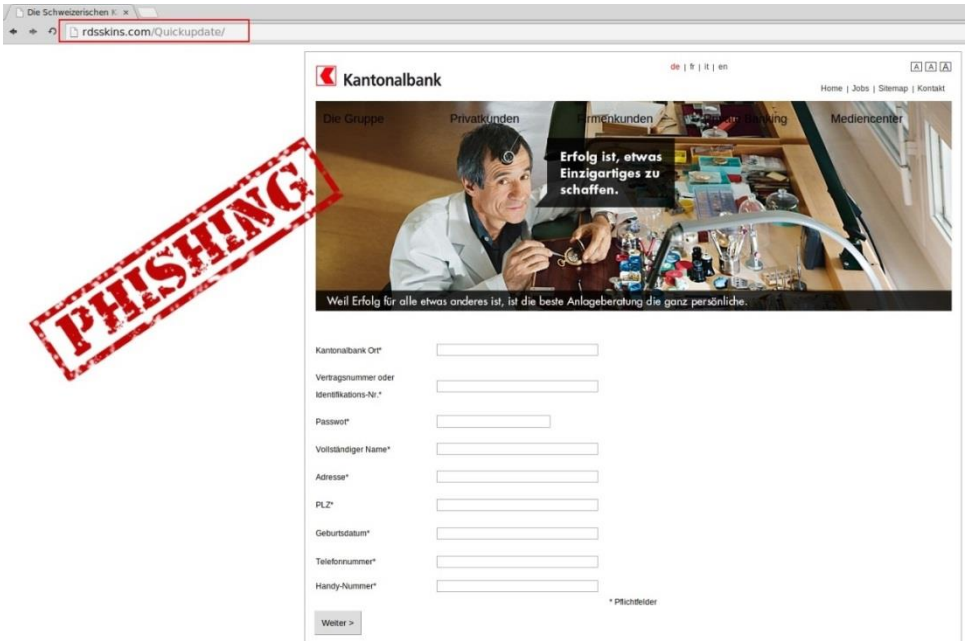


(https://www.cybercrime.admin.ch/kobik/fr/home/warnmeldungen/meldungen/2015/2015-05-19.html)

8.1.4 Groupe des Banques Cantonales

Par ce courrier électronique, les fraudeurs font croire à leurs victimes qu'une personne a tenté, depuis l'étranger, de se connecter à leur compte bancaire. Afin de s'emparer de leurs données personnelles bancaires, les escrocs incitent la victime à cliquer sur un lien la redirigeant vers un formulaire sensé sécuriser l'accès à son e-Banking.

Figure 23 : Fausse page web du Groupe des Banques Cantonales



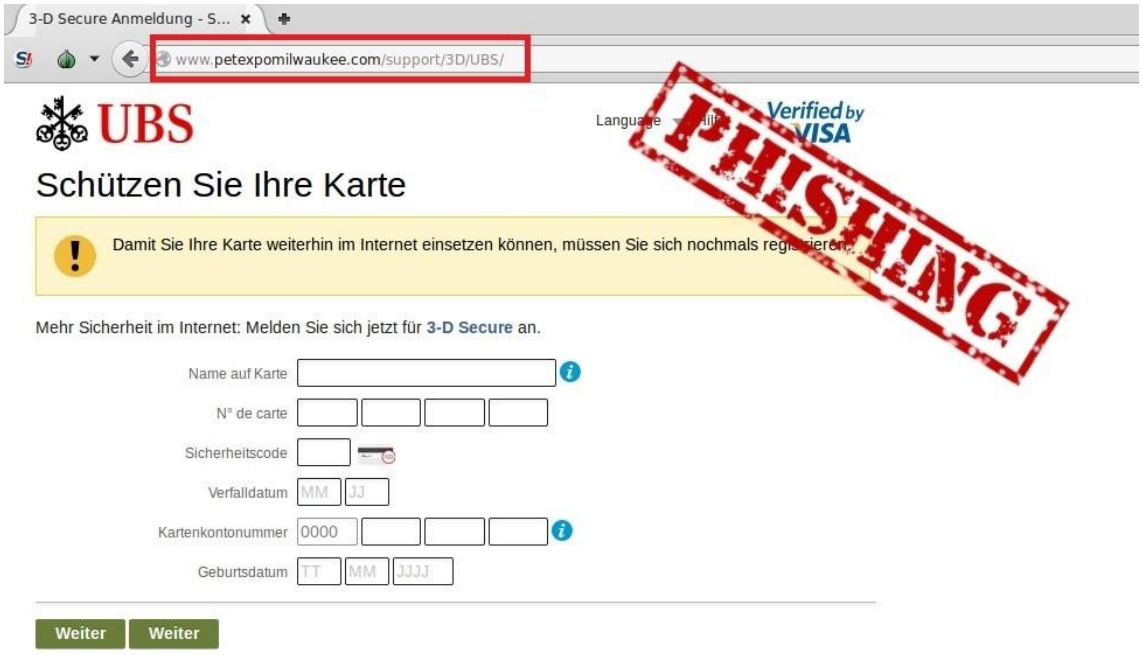
(https://www.cybercrime.admin.ch/kobik/fr/home/warnmeldungen/meldungen/2014/2014-07-09.html)

8.1.5 UBS

Par ce courrier électronique, les fraudeurs font croire à leurs victimes que leur compte va être bloqué si l'activation de 3-D Secure pour leur carte de crédit n'est pas enclenchée dans les 48 heures.

Figure 24 : Faux courrier électronique d'UBS

(https://www.cybercrime.admin.ch/kobik/fr/home/warnmeldungen/meldungen/2016/2016-01-19.html)

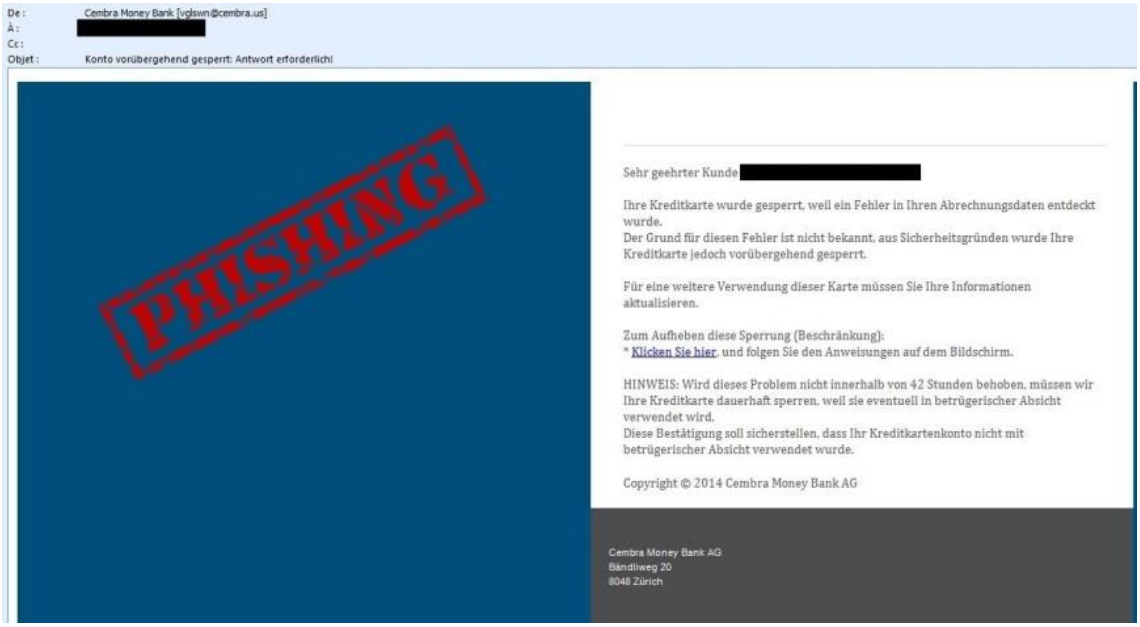


(https://www.cybercrime.admin.ch/kobik/fr/home/warnmeldungen/meldungen/2016/2016-01-19.html)

8.1.6 Cembra Money Bank

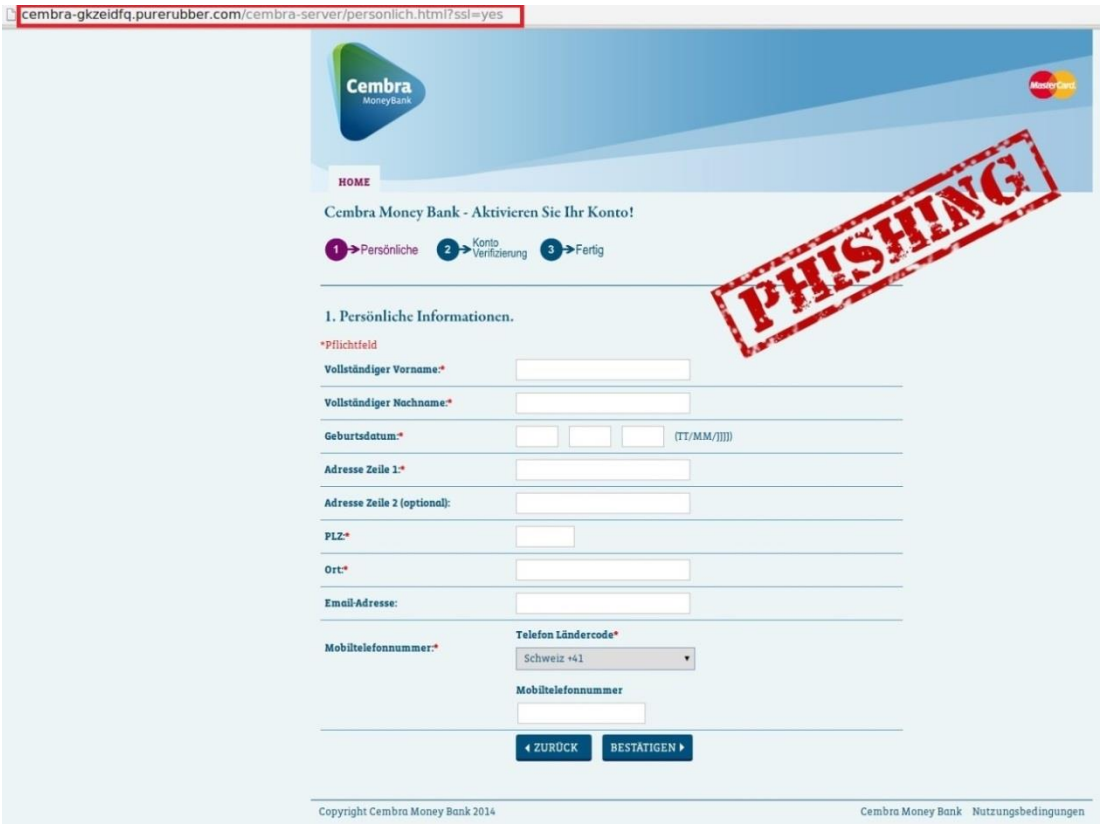
Le faux courrier électronique informe la victime que sa carte de crédit a été bloquée suite à une erreur constatée dans un décompte. Pour débloquer sa carte de crédit, la victime doit suivre un lien et entrer ses données personnelles.

Figure 25 : Faux courrier électronique de Cembra Money Bank



(https://www.cybercrime.admin.ch/kobik/fr/home/warnmeldungen/meldungen/2014/2014-08-26.html)

Figure 26 : Fausse page web de Cembra Money Bank

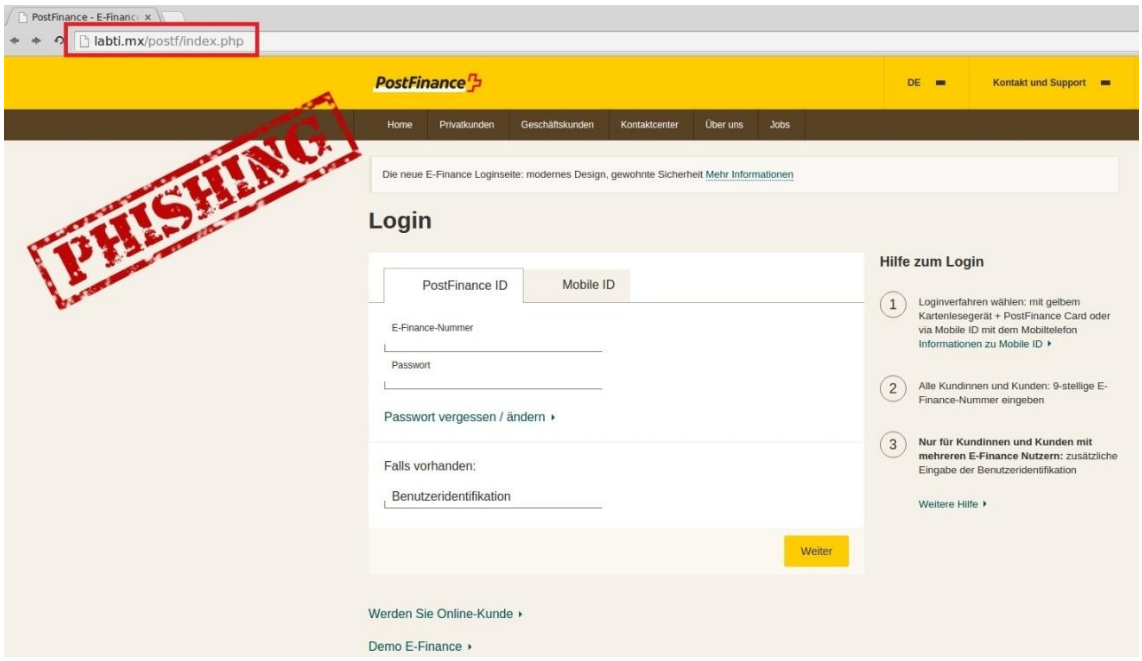


(https://www.cybercrime.admin.ch/kobik/fr/home/warnmeldungen/meldungen/2014/2014-08-26.html)

8.1.7 PostFinance

Par ce courrier électronique, les fraudeurs font croire à leurs victimes qu'une personne s'est connectée depuis un ordinateur non-autorisé à leur compte e-finance. Afin d'effectuer un contrôler de l'identité du détenteur du compte en question, les données personnelles de la victime sont demandées.

Figure 27 : Fausse page web PostFinance

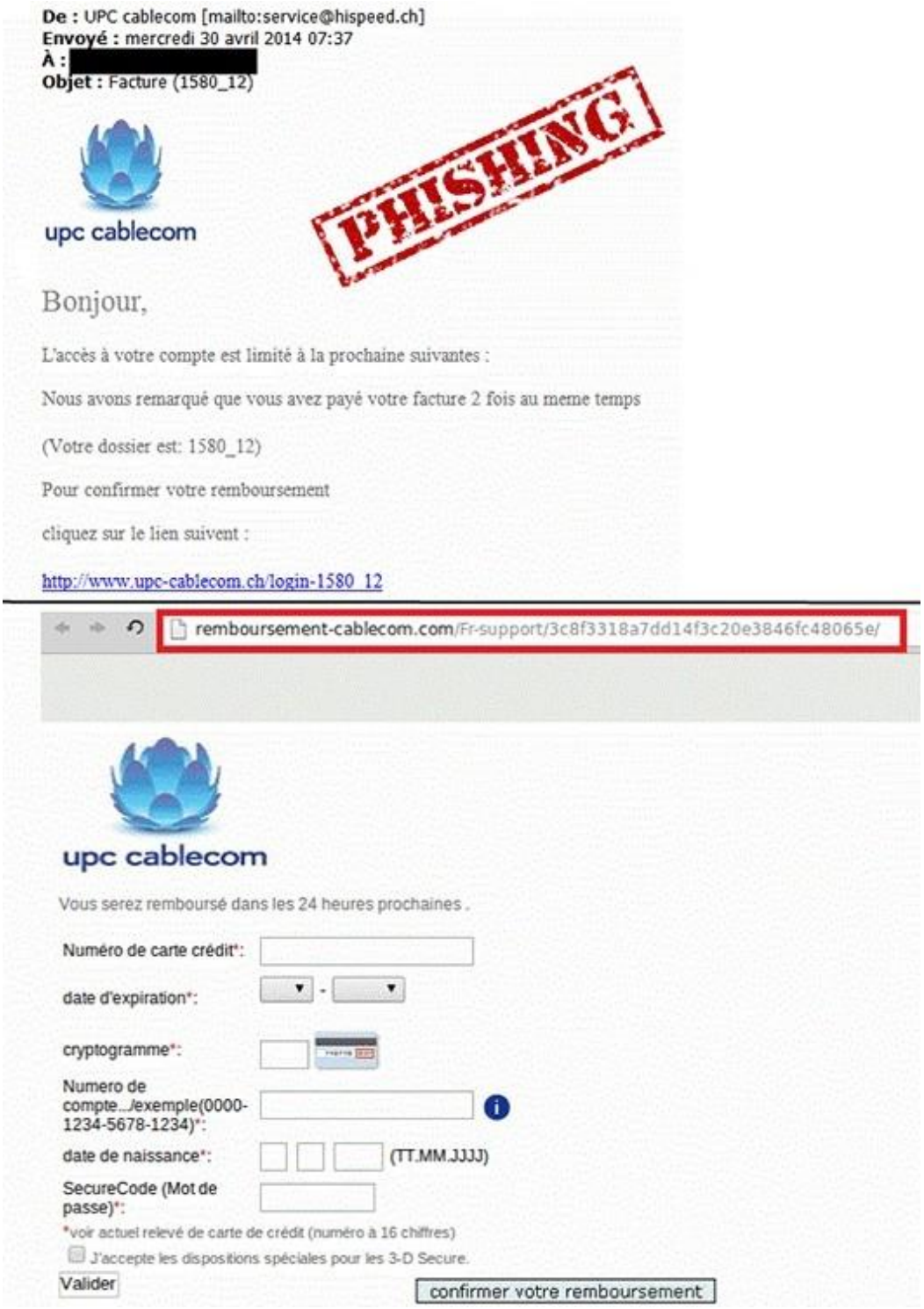


(https://www.cybercrime.admin.ch/kobik/fr/home/warnmeldungen/meldungen/2015/2015-09-15.html)

8.1.8 UPC Cablecom

Pour appâter leurs victimes, les escrocs promettent un remboursement d'une facture payée à double si elles suivent le lien indiqué dans le courrier électronique et insèrent sur une page web reprenant le logo de l'entreprise, leur numéro de carte bancaire, la date d'expiration et le code de sécurité à trois chiffres.

Figure 28 : Faux courrier électronique et page web d'UPC Cablecom

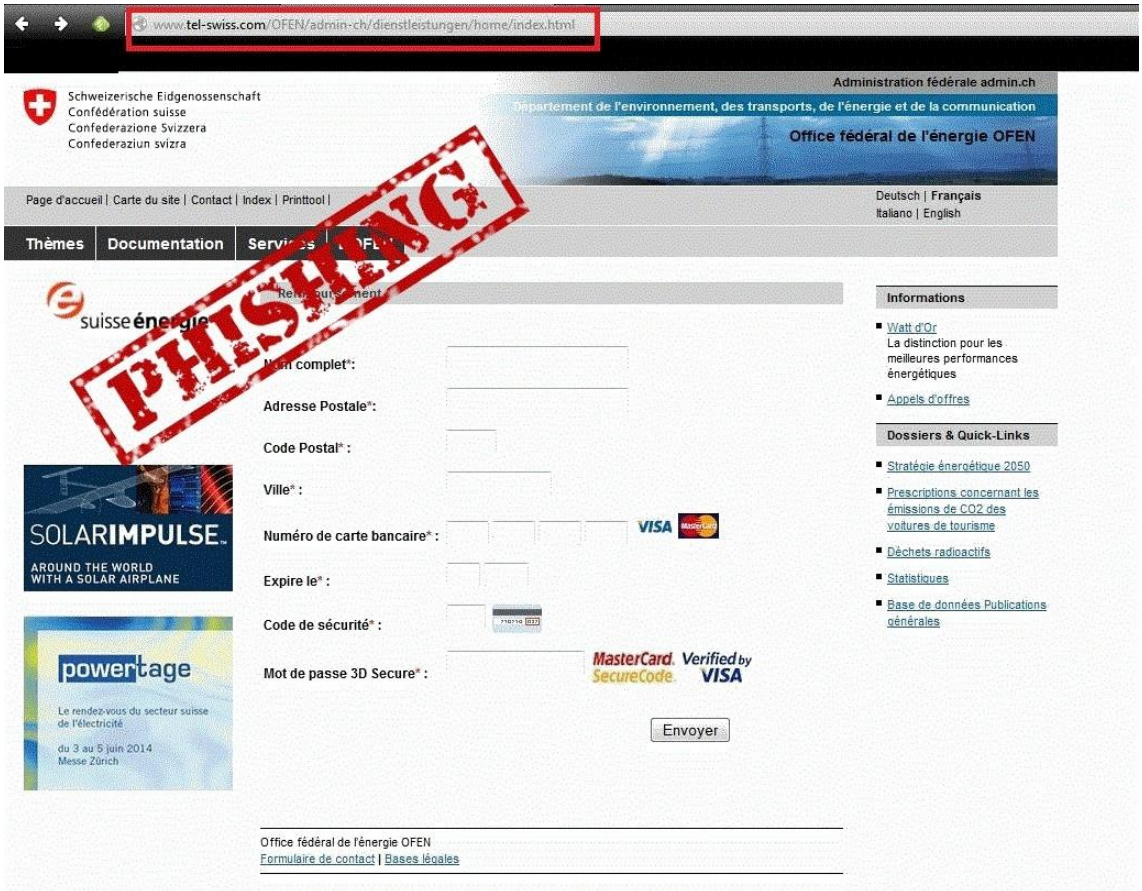


(https://www.cybercrime.admin.ch/kobik/fr/home/warnmeldungen/meldungen/2014/2014-05-01.html)

8.1.9 Office fédéral de l’énergie (OFEN)

Pour appâter leurs victimes, les escrocs promettent un remboursement de CHF 165.- si elles suivent le lien indiqué dans le courrier électronique et insèrent sur une page web leur adresse et données de carte bancaire, autrement dit le numéro de carte, la date d’expiration et le code de sécurité à trois chiffres.

Figure 29 : Fausse page web de l’OFEN



(https://www.cybercrime.admin.ch/kobik/fr/home/warnmeldungen/meldungen/2014/2014-03-24.html)

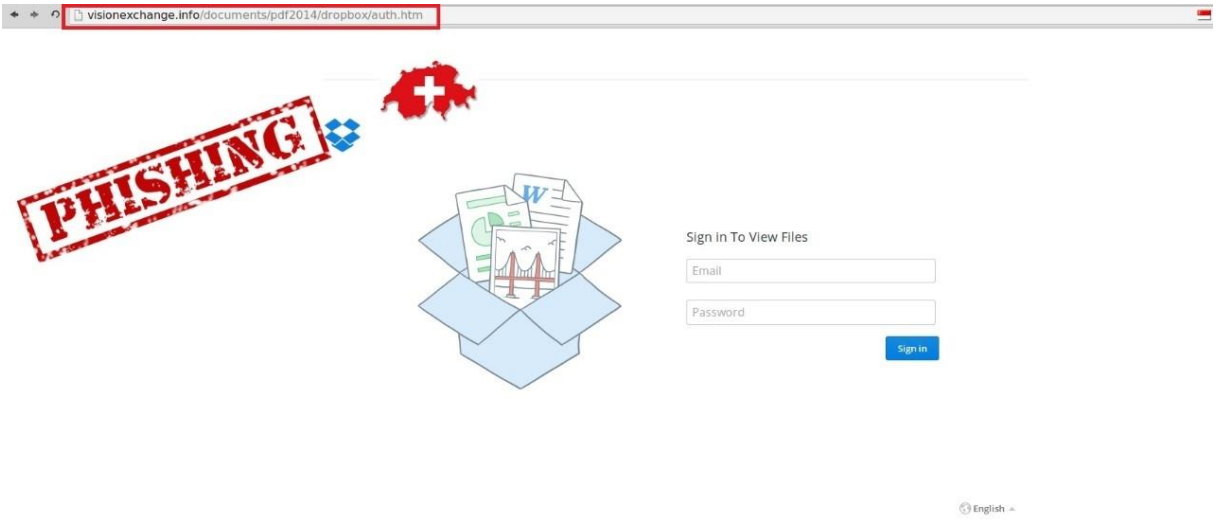
8.1.10 Département fédéral de l'intérieur (DFI)

Par ce courrier électronique, les fraudeurs informent leurs victimes qu'une communication importante émanant du Département fédéral de l'intérieur (DFI) doit être transmise à la population helvétique. Les victimes sont invitées à cliquer sur un lien qui les redirige sur un site sur lequel il est possible de télécharger l'importante communication. Le site internet sur lequel les victimes sont redirigées est en fait une imitation du site officiel de Dropbox sur lequel les victimes sont priées de fournir leurs identifiants, à savoir nom d'utilisateur et mot de passe.

Figure 30 : Faux courrier électronique du DFI

(https://www.cybercrime.admin.ch/kobik/fr/home/warnmeldungen/meldungen/2014/2014-08-18.html)

Figure 31 : Fausse page web de Dropbox



(https://www.cybercrime.admin.ch/kobik/fr/home/warnmeldungen/meldungen/2014/2014-08-18.html)

8.2 Phishing par Whatsapp

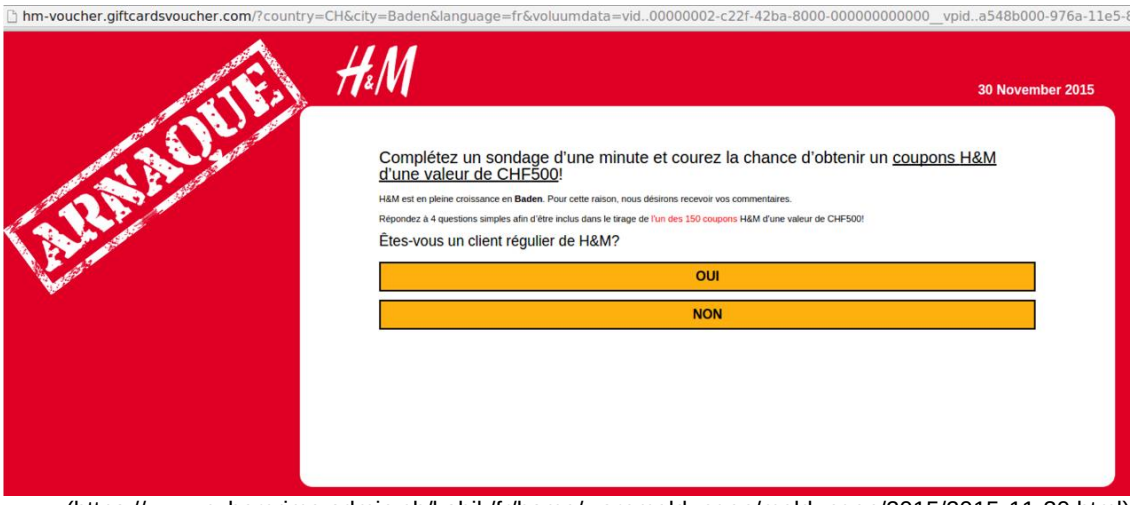
8.2.1 Faux sondage et abonnement piège au nom d'H&M

Diffusée via WhatsApp, cette arnaque consiste à inviter la victime à cliquer sur un lien redirigeant celle-ci vers un prétendu sondage promettant de gagner un bon d'achat d'une valeur de CHF 500.- sous forme de carte cadeau. Après avoir effectué le sondage, la victime est incitée à le partager et à communiquer ses données personnelles pour valider sa participation au concours. Afin d'accréditer l'arnaque, de faux commentaires de prétendus gagnants apparaissent à la fin du questionnaire. Le fait de transmettre ses données personnelles et son numéro de téléphone engage la victime à la souscription d'un abonnement payant. En Suisse, Migros est Ikea ont également été la cible de cette escroquerie.

Figure 32 : Lien sur Whatsapp

(https://www.cybercrime.admin.ch/kobik/fr/home/warnmeldungen/meldungen/2015/2015-11-30.html)

Figure 33 : Fausse page web d'H&M



(https://www.cybercrime.admin.ch/kobik/fr/home/warnmeldungen/meldungen/2015/2015-11-30.html)

9. Conclusion

Le phénomène du phishing n'est pas fondamentalement nouveau comme nous avons pu le constater à travers cette étude. Se basant sur l'ingénierie sociale, il exploite principalement les failles psychologiques de l'être humain en profitant de sa crédulité et de sa bonne foi. Les modes opératoires et techniques employés par les pirates quant à eux ne cessent d'évoluer pour devenir de plus en plus sophistiqués. Par ailleurs, il est facile de constater une augmentation notable de la qualité des contenus délictueux. Cela signifie que la présentation visuelle des pages web et des courriers électroniques ainsi que la grammaire et l'orthographe se sont nettement améliorés rendant la tâche plus difficile à l'internaute pour discerner le vrai du faux.

Les attaques de phishing ne se limitent pas seulement aux particuliers mais sont aussi dirigées à l'encontre les entreprises, avec bien entendu, de fâcheuses conséquences pour l'un comme pour l'autre. Ces cibles font l'objet d'usurpation d'identité de la part des pirates et sont ensuite victimes d'extorsion de fonds provocant ainsi de lourdes pertes financières.

Lors de la navigation sur internet, il est judicieux pour l'internaute d'observer certaines mesures comportementales afin de ne pas tomber dans un piège potentiel. De plus, afin de pallier au manque de vigilance de certains utilisateurs, il existe des mesures techniques permettant de connaître la réputation d'un site internet avant même d'y accéder. Des organismes de lutte contre la cybercriminalité opérant en Suisse, en Europe et dans le monde travaillent de manière opérationnelle pour protéger les internautes et tenter d'endiguer le problème.

Malgré tout, la meilleure protection pour l'être humain contre ce type de cybercriminalité basée sur l'ingénierie sociale reste l'être humain lui-même. Pour améliorer la lutte contre ce type de criminalité, je pense qu'il faudrait orienter davantage la protection par la prévention et ceci à plusieurs échelons. Tout d'abord, au niveau des systèmes d'exploitation sous forme d'un tutoriel animé démontrant les dangers de la navigation sur internet, cela forcerait les utilisateurs à s'informer. Ensuite sous forme d'un logiciel inclus dans le système d'exploitation qui analyserait chaque site internet consulté, en se basant sur les différentes bases de données des sites de mauvaises réputations. Enfin, je pense qu'il serait judicieux que les entreprises, les écoles et les universités s'attardent davantage à promouvoir la sensibilisation contre ce type de cybercriminalité afin de mieux informer les personnes utilisant internet des dangers auxquels elles peuvent être confrontées.

Bibliographie

SITES WEB :

ANTIPHISHING. *Centrale d'enregistrement et d'analyse pour la sureté de l'information MELANI* [En ligne]. [Consulté le 29 mars 2016]. Disponible à l'adresse suivante : https://www.antiphishing.ch/fr/

APWG. *Anti Phishing Working Group* [En ligne]. [Consulté le 9 mars 2016]. Disponible à l'adresse suivante : http://www.antiphishing.org/

ARNAUD, Jacques. Le social engineering : un espionnage sans compétences techniques. *SécuritéInfo.com* [En ligne]. [Consulté le 27 février 2016]. Disponible à l'adresse suivante : https://www.securiteinfo.com/attaques/divers/social.shtml

BARRE DE PROTECTION POUR SON NAVIGATEUR. *CCM* [En ligne]. [Consulté le 25 mars 2016]. Disponible à l'adresse suivante : http://www.commentcamarche.net/faq/29065-barres-de-protection-pour-son-navigateur

CARDERSECURITY, 2011. *CarderSecurity* [En ligne]. 7 Juillet 2011 [Consulté le 30 mars 2016]. Disponible à l'adresse suivante : https://cardersecurity.wordpress.com/

CHARLET François, 2014. Usurpation d'identité : Le Conseil fédéral ne légiférera pas, et il a tort. *Le blog de François Charlet* [En ligne]. 14 Novembre 2013. 30 Mars 2014 [Consulté le 8 Avril 2016]. Disponible à l'adresse suivante : https://francoischarlet.ch/2013/usurpation-didentite-le-conseil-federal-ne-legiferera-pas-et-il-a-tort/

COMBATTING CYBERCRIME IN A DIGITAL AGE, 2013. *Europol* [En ligne]. [Consulté le 1 avril 2016]. Disponible à l'adresse suivante : https://www.europol.europa.eu/ec3

COURS : LE SOCIAL ENGINEERING, 2013. *Le blog du Hacker* [En ligne]. 29 Mars 2013 [Consulté le 24 février 2016]. Disponible à l'adresse suivante : http://www.leblogduhacker.fr/cours-le-social-engineering/

ELICITATION. *Portail de l'IE* [En ligne]. [Consulté le 27 février 2016]. Disponible à l'adresse suivante : http://www.portail-ie.fr/lexiques/read/79

EVIL TWIN. *Wikipédia, l'encyclopédie libre* [En ligne]. [Consulté le 11 mars 2016]. Disponible à l'adresse suivante : https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks)

FRAUDE 4-1-9. *Wikipédia, l'encyclopédie libre* [En ligne]. [Consulté le 29 mars 2016]. Disponible à l'adresse suivante : https://fr.wikipedia.org/wiki/Fraude_4-1-9

FRAUDE EN LIGNE : PHARMING, 2015. *Norton* [En ligne]. [Consulté le 11mars 2016]. Disponible à l'adresse suivante : http://fr.norton.com/cybercrime-pharming

GENERAL PHISHING INFORMATION AND PREVENTION TIPS. *Phishing.org* [En ligne]. [Consulté le 8 mars 2016]. Disponible à l'adresse suivante : http://www.phishing.org/

HAMEÇONNAGE. *Wikipédia, l'encyclopédie libre* [En ligne]. [Consulté le 24 février 2016]. Disponible à l'adresse suivante : https://fr.wikipedia.org/wiki/Hame%C3%A7onnage

INGENIERIE SOCIALE, 2016. *CCM* [En ligne]. [Consulté le 25 février 2016]. Disponible à l'adresse suivante : http://www.commentcamarche.net/contents/55-ingenierie-sociale

INGENIERIE SOCIALE, 2016. *eBanking en toute sécurité* [En ligne]. [Consulté le 25 février 2016]. Disponible à l'adresse suivante : https://www.ebankingabersicher.ch/fr/5-mesures-pour-votre-securite?catid=114&id=114:social-engineering

INGENIERIE SOCIALE. *Wikipédia, l'encyclopédie libre* [En ligne]. [Consulté le 24 février 2016]. Disponible à l'adresse suivante : https://fr.wikipedia.org/wiki/Spear_phishing

INTRODUCTION AU PHISHING. *CCM* [En ligne]. [Consulté le 11 mars 2016]. Disponible à l'adresse suivante : http://www.commentcamarche.net/contents/65-le-phishing-hameconnage

LETTRE DE JERUSALEM. *Wikipédia, l'encyclopédie libre* [En ligne]. [Consulté le 29 mars 2016]. Disponible à l'adresse suivante : https://fr.wikipedia.org/wiki/Lettre_de_J%C3%A9rusalem

MELANI. *Centrale d'enregistrement et d'analyse pour la sureté de l'information MELANI* [En ligne]. [Consulté le 29 mars 2016]. Disponible à l'adresse suivante : https://www.melani.admin.ch/melani/fr/home.html

MÉTHODES RAFFINÉES D'INGÉNIERIE SOCIALES ET ATTAQUES DE PHISHING AJUSTÉES À LA SUISSE, 2014. *Centrale d'enregistrement et d'analyse pour la sureté de l'information MELANI* [En ligne]. 23 Septembre 2014 [Consulté le 7 mars 2016]. Disponible à l'adresse suivante : https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/methodes-raffinees-dingenierie-sociale-et-attaques-de-phishing-a.html

NOUS AVONS SANS DOUTE ACHETE VOTRE ADRESSE EMAIL, 2014. *Rue89* [En ligne]. 4 Août 2014 [Consulté le 29 mars 2016]. Disponible à l'adresse suivante : http://rue89.nouvelobs.com/2014/09/04/marche-noir-avons-sans-doute-achete-adresse-e-mail-verifiez-254607

PENETRATION TESTERS. *Security through education* [En ligne]. [Consulté le 27 février 2016]. Disponible à l'adresse suivante : http://www.social-engineer.org/framework/general-discussion/categories-social-engineers/penetration-testers/

PHISHING : LE TEMPS EST VENU DE PRENDRE SES RESPONSABLITES ET D'AGIR, 2015. *Le journal du net* [En ligne]. 4 Novembre 2015 [Consulté le 29 mars 2016]. Disponible à l'adresse suivante : http://www.journaldunet.com/solutions/expert/62908/phishing---le-temps-est-venu-de-prendre-ses-responsabilites-et-d-agir.shtml

PHISHING, *Cases.lu* [En ligne]. [Consulté le 7 mars 2016]. Disponible à l'adresse suivante : https://www.cases.lu/fr/phishing.html

PHISHING. *Security through education* [En ligne]. [Consulté le 25 février 2016]. Disponible à l'adresse suivante : http://www.social-engineer.org/framework/general-discussion/real-world-examples/phishing/

PHISHING*. Service de coordination de la lutte contre la criminalité sur internet SCOCI* [En ligne]. [Consulté le 30 mars 2016]. Disponible à l'adresse suivante : https://www.cybercrime.admin.ch/kobik/fr/home/gefahren/vermoegensdelikte/phishing.html

PHISHING. *SKPPSC* [En ligne]. [Consulté le 8 mars 2016]. Disponible à l'adresse suivante :http://skppsc.ch/10/fr/2betrug/1praevention_betrugsmethoden/40206phishing.php

PONTIROLI, Santiago, 2013. L'ingénierie sociale ou le piratage du système d'exploitation humain. *Kasperky Lab* [En ligne]. 29 décembre 2013 [Consulté le 25 février 2016]. Disponible à l'adresse suivante : https://blog.kaspersky.fr/lingenierie-sociale-ou-le-piratage-du-systeme-dexploitation-humain/2168/

QUEL EST LE PRIX DE VOS DONNÉES SUR LE BLACK MARKET, 2015. *Le journal du geek* [En ligne]. 9 Juin 2015 [Consulté le 29 mars 2016]. Disponible à l'adresse suivante : http://www.journaldugeek.com/2015/06/09/prix-donnees-black-market/

SCOCI*. Service de coordination de la lutte contre la criminalité sur Internet (SCOCI) de fedpol* [En ligne]. [Consulté le 30 mars 2016]. Disponible à l'adresse suivante : https://www.cybercrime.admin.ch/kobik/fr/home.html

SPEAR PHISHING. *Wikipédia, l'encyclopédie libre* [En ligne]. [Consulté le 29 mars 2016]. Disponible à l'adresse suivante : https://fr.wikipedia.org/wiki/Spear_phishing

WHAT ARE THE DIFFERENT TYPES OF PHISHING ATTACKS? *Innovateus* [En ligne]. [Consulté le 9 mars 2016]. Disponible à l'adresse suivante : http://www.innovateus.net/science/what-are-different-types-phishing-attacks

RAPPORTS :

MELANI RAPPORT SEMESTRIEL, 2014. *Situation en Suisse et sur le plan international*. [Consulté le 10 mars 2016]. Disponible à l'adresse suivante : https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation.html

MELANI RAPPORT SEMESTRIEL, 2015. *Situation en Suisse et sur le plan international*. [Consulté le 10 mars 2016]. Disponible à l'adresse suivante : https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation.html

SCOCI RAPPORT ANNUEL, 2014. *Service de coordination de la lutte contre la criminalité sur internet.* [Consulté le 1 mars 2016]. Disponible à l'adresse suivante : https://www.cybercrime.admin.ch/kobik/fr/home/publiservice/berichte.html