NOGEN'TERNET formation	Gare aux arnaques sur le net !	Mars 2019

Objectif de ce chapitre

Vous aider à éviter de vous faire piéger par les arnaques nombreuses sur le net.

"Une arnaque est un délit consistant à obtenir le bien d'autrui par des manœuvres trompeuses et frauduleuses". Les arnaques antérieures à Internet se sont répandues aussi sur le net.

Quelques exemples d'arnaques "classiques", dont :

Le "Phishing"

Le Phishing est une technique consistant à amener les internautes à révéler des informations personnelles ou financières via un message électronique ou un site web frauduleux.

Cette arnaque, assez répandue, peut coûter cher, car on transmet à un inconnu des informations confidentielles : compte bancaire, numéro de carte bancaire, mot de passe etc.

Qu'est-ce que l'hameçonnage ?

L'hameçonnage (appelés également « phishing ») est une approche détournée qu'utilisent les cyber-escrocs pour vous pousser à révéler des informations personnelles, comme des mots de passe ou des numéros de carte de crédit, de sécurité sociale ou de compte bancaire. Ils le font en vous envoyant des e-mails contrefaits ou en vous dirigeant sur un site web contrefait.

D'où provient l'hameçonnage ?

Les messages d'hameçonnage semblent provenir d'organisations légitimes comme Paypal, UPS, une administration ou votre banque ; cependant, il s'agit en fait d'habiles escroqueries. Les messages demandent poliment l'actualisation, la validation ou la confirmation d'informations sur un compte, en suggérant fréquemment qu'un problème est survenu. Vous êtes alors redirigé vers un faux site où l'on vous pousse à entrer des informations sur le compte. Il peut en résulter un vol d'identité.

Comment reconnaître l'hameçonnage ?

Vous recevez des messages vous demandant de révéler des informations personnelles, en général par e-mail ou au travers d'un site web.

Comment supprimer l'hameçonnage ?

Les leurres de l'hameçonnage ne peuvent pas être « supprimés », mais ils peuvent assurément être détectés. Surveillez votre site web et soyez conscient de ce qu'y doit s'y trouver ou pas. Si possible, changez régulièrement les fichiers fondamentaux de votre site web

.

Comment empêcher l'hameçonnage ?

- Ayez de bonnes habitudes et ne répondez pas aux liens dans les e-mails non sollicités ou sur Facebook.
- N'ouvrez pas les pièces jointes des e-mails non sollicités.
- Protégez vos mots de passe et ne les révélez à personne.

- Ne donnez pas d'informations sensibles, que ce soit au téléphone, en personne ou par e-mail.
- Vérifiez l'URL (adresse web) des sites web. Dans de nombreux cas d'hameçonnage, l'adresse web peut sembler légitime, mais l'URL peut comporter une faute d'orthographe ou le domaine peut être différent (.com au lieu de .gov).
- Maintenez votre navigateur à jour et appliquez les correctifs de sécurité.

Protégez-vous contre l'hameçonnage

Il n'y a pas de meilleure façon de reconnaître et supprimer l'hameçonnage et de s'en préserver que d'utiliser un outil antivirus et anti-hameçonnage, et le meilleur outil de ce type est sans doute Avast.

Comment bien se faire arnaquer ?

Tout commence par la réception d'un mail. Vous recevez de votre banque, de votre fournisseur d'accès ou d'un cyber-marchand un message de forme tout à fait habituelle et rassurante (avec le logo et les couleurs de l'entreprise) vous informant qu'il est indispensable et urgent de mettre à jour vos coordonnées. Vous êtes invité à cliquer sur un lien vous menant au site de l'entreprise en question pour ressaisir soit votre nom, votre adresse, vos identités bancaires et pourquoi pas votre numéro de carte bleue, vos identifiants et mot de passe de connexion. Vous êtes en confiance et suivez attentivement les consignes...

Patatras ! Vous venez de fournir volontairement votre numéro de compte ou vos mots de passe à un escroc qui va s'empresser de les utiliser pour son compte.

Pourtant, tout semblait des plus normal. Le message était à l'entête de la banque ou du fournisseur d'accès, l'expéditeur semblait correspondre et le site était la copie conforme de votre banque.

Réalités du Phishing

Le Phishing est une arnaque efficace : ces mails sont envoyés par dizaines de milliers et leur vraisemblance font que quelques milliers de destinataires tombent dans le piège et fournissent aux escrocs des informations confidentielles.

Ces escrocs se font souvent passer pour des banques, mais leurs cibles sont aussi des sites de paiement comme Paypal et des sites d'annonces ou d'enchères comme ebay.

Le montant des escroqueries par Phishing peut être estimé à des millions d'euros.

Le bon comportement face au Phishing

Il importe donc d'être très soupçonneux et de prendre en compte les recommandations suivantes :

- Les banques, les fournisseurs d'accès et les cyber-marchands NE DEMANDENT JAMAIS des informations confidentielles comme votre numéro de carte bancaire et son code, ni votre compte e-mail principal, et son mot de passe. Aussi, si vous recevez de tels messages, soi-disant, de votre organisme bancaire ou fournisseur d'accès, détruisez-les.
- Si le message est en anglais, que votre anti-spam ne l'a pas filtré et que vous n'avez pas affaire à des organismes anglo-saxons ou américains, détruisez le mail. Répondriez-vous à un appel téléphonique en anglais vous demandant la communication de données confidentielles ?
- Dans tous les cas vous devez :
  - Vous poser les questions : est-il normal que cet organisme me sollicite ? Est-il normal qu'il me demande cela ?
  - Ne surtout pas utiliser les liens présents dans le mail car ceux-ci peuvent être détournés et vous envoyer sur une fausse page sans que vous ne vous en aperceviez.
  - En aucune façon fournir, des informations et données confidentielles.
  - Ne jamais vous identifier ou fournir une quelconque information sur un site web atteint depuis un lien figurant dans un mail.

- Lorsque vous êtes amené à vous identifier ou à fournir des données confidentielles, il faut impérativement passer par la page d'accueil du site (de la forme "www.nomdusite.com" et saisie manuellement) pour atteindre la page de saisie des données.
  De même, il faut être très attentif à l'écriture des adresses (exemple : www.societe-generale et www.societe_generale.com ne sont pas les mêmes sites…)

  Recommandation : lorsqu'un site demande une saisie d'information, vérifiez que la page est sécurisée en suivant les indications suivantes :

  - Les sites "sécurisés" sont reconnaissables par le début de leur adresse :
    1. Le "**http://**" classique est remplacé par **https://**
    2. Un petit **cadenas** apparaît à la droite de l'adresse

  - **Rappels de précautions élémentaires**

- Se méfier des adresses de sites qui vous sont envoyées par mail
- Changer régulièrement son (ses) mot(s) de passe
- Se méfier des "SPAMS" (courriers indésirables d'origine douteuse)
- Utiliser un anti-spam (proposé par les messageries réputées)
- En cas de doute sur l'origine d'un message dont l'origine pourrait être celui d'un site de confiance :
  - Ne pas hésiter à contacter directement ce site bancaire ou de paiement
  - Vérifier le sérieux de l'expéditeur en copiant son adresse mail et en la collant dans la barre de recherche Google : s'il s'agit d'un mail douteux, il aura sans doute été déjà identifié par un site dénonçant les escroqueries…
  - Enfin, n'hésitez pas à transmettre ce mail au service "abuse" de votre messagerie ou de votre fournisseur d'accès.

Autres arnaques classiques :

Propositions de remboursement

Un autre moyen pour l'escroc pour obtenir des informations bancaires est d'imiter l'identité d'une société (Orange par exemple) ou d'un organisme officiel (impôts, Sécu…) qui vous annonce un "trop perçu" et vous propose un remboursement par virement bancaire sur le compte dont vous êtes invité à donner le détail des coordonnées.

Des milliers de gens se sont fait piéger…

Escroqueries "419"

La fraude 419 (aussi appelée "scam 419", ou "arnaque nigériane") est une escroquerie répandue sur Internet. (La dénomination 4-1-9 vient du numéro de l'article du code nigérian sanctionnant ce type de fraude).

Un **scam** se présente généralement sous la forme d'un pourriel (**spam**) dans lequel une personne affirme posséder une importante somme d'argent (plusieurs millions de dollars en héritage, pots-de-vin, fonds à placer à l'étranger suite à un changement de contexte politique, etc.) et fait part de son besoin d'utiliser un compte existant pour transférer rapidement cet argent.

La personne à l'origine du scam demande de l'aide pour effectuer ce transfert d'argent, en échange de quoi il offre un pourcentage sur la somme qui sera transférée, en général par la « voie

diplomatique ». Si la victime accepte, on lui demandera petit à petit d'avancer des sommes d'argent destinées à couvrir des frais imaginaires (notaires, entreprises de sécurité, pots-de-vin…) avant que le transfert ne soit effectif ; bien entendu, ce transfert n'aura jamais lieu.

Voici un exemple de spam typique de cette escroquerie 419 sur Internet :

> *Bonjour Monsieur /Madame,*
>
> *Je me nomme xxx ,j'ai 20 ans et je voudrais que vous m'aidiez a effectuer le transfert de mes fonds (2.500.000 €) que mon feu père m'a laisse avant sa mort, sur votre compte bancaire et vous serrez comme un guide pour moi pendant toute cette transaction.*
> *Je vous donnerai généreusement 20% de mes fonds qui seront transférés sur votre compte bancaire mais je veux aussi que vous soyez honnête envers moi et sincère. Si vous recevez mon message veuillez me contacter par mon mail : xxx@yahoo.fr. J'attends votre réponse favorable à mon message*

Commence alors un échange de mails faisant état de difficultés de l'administration locale, des banques, du notaire qui seront résolues moyennant le paiement d'avances… jusqu'à ce que l'arnaqueur disparaisse.

Arnaques aux "petites annonces"

Une grande partie des annonces (ebay, leboncoin…) est systématiquement exploitée par des escrocs qui utilisent le procédé décrit au dessus dans "l'arnaque nigériane".

C'est souvent le même cheminement : un acheteur d'un pays lointain, accepte d'acheter votre objet (souvent une voiture) sans la voir ni discuter du prix indiqué. Il propose de payer par Paypal et de prendre les frais d'expédition à sa charge. Exemple (vécu) :

> *Bonsoir,*
> *J'accuse bonne réception de votre message, je confirme l'achat de votre xxx vu les photos cela ma donner satisfaction mais étant donné que je suis française expatriée résidant en Afrique avec mon époux depuis cinq mois pour des raisons professionnelles là ou j'exerce a L'UNICEF. Alors j'aimerais savoir si vous avez un compte Paypal, me faire parvenir une demande de paiement avec frais de port inclus. Je vous informe que les frais de port seront à ma charge pour l'envoi du colis je préfère par Chronopost international qui est plus sécurisant.*
> *Je suis en attente de votre mail.*

Dans un prochain mail, l'acheteur assure que le paiement est parti est sera débloqué par Paypal dès que vous aurez envoyé le numéro de suivi de l'expédition…vers le Nigéria…

Si donc vous envoyez l'objet, le faux acheteur sera ravi et vous furieux de vous être fait escroquer sans avoir vérifié que l'argent n'était pas arrivé sur votre compte Paypal…

Voici un extrait des recommandations de Paypal sur son site :

> *Avant d'expédier un objet, assurez-vous toujours de voir les fonds associés à la transaction crédités sur le solde de votre compte PayPal.*
> *Si vous avez reçu un email vous demandant de fournir un numéro de suivi avant même d'avoir reçu les fonds, ou sans que la transaction ne figure sur votre compte,* ***transférez-le à spoof@paypal.fr*** *puis supprimez-le.*
> *Si vous avez déjà répondu à l'email et expédié l'objet, contactez immédiatement le transporteur afin de stopper la livraison du colis, et alertez les services de police pour signaler la fraude.*

"Scam" des jeux d'argent en ligne

Le **scam** de jeux d'argent en ligne concerne les casinos et le poker, entre autres. Ils cherchent à nous tromper, par exemple en proposant des bonus énormes mais assortis de conditions telles qu'on ne peut pas en profiter. Ou parfois une formule d'essai gratuit nous fait gagner trop souvent pour nous inciter à jouer notre argent.

Ils se manifestent par des spams promouvant des sites Web de jeux d'argent, dont la plupart sont fermés quelques semaines après leur ouverture.

Médicaments et poudres magiques

Le Net offre évidement le moyen d'importer légalement ou clandestinement toutes les sortes de produits. La mise en vente libre du Viagra n'a pas affecté le trafic de pilules magiques qui explose littéralement. Les pays asiatiques et africains sont d'immenses demandeurs (et producteurs) de ces pharmacopées exotiques et grigris.

Tout se trouve la DHEA, les pilules qui font maigrir, guérissent du cancer, allongent le pénis, rajeunissent de cinquante ans… Ce sont pour la plupart au mieux des placebos inoffensifs ou des produits que la médecine traditionnelle n'a pas validés et qu'un flou juridique n'interdit pas d'importer, mais il y a aussi de vrais toxiques.
La vente de rêves n'est pas une escroquerie et le paiement se passe très normalement par débit Visa. Il n'y a donc rien à redire, les clients reçoivent le rêve qu'ils ont librement choisi d'acheter.

Faux antivirus et anti-spyware : les "Rogues"

Cette arnaque sur Internet plus récente se manifeste d'abord par une page Web infectée par un programme malveillant, qui ouvre des fenêtres intempestives en rafale pour signaler la présence de programmes malveillants sur le PC, virus, spywares ou autres. Ces alertes sont très souvent fausses, le but étant de faire payer la victime pour régler les soi-disant problèmes, en téléchargeant un soi-disant antivirus ou anti-spyware.

Le scan effectué ensuite par ce faux antivirus ou anti-spyware, appelé rogue, est très rapide : c'est en fait un simulacre d'examen. Il annonce que les soi-disant programmes malveillants sont éradiqués alors qu'il n'a rien fait sur le PC.

Loterie gagnante gratuite (ou voyage gratuit…)

"Congratulations, you are the lucky winner of Email Lottery Promotion …" Suivent des numéros personnels bidons et une somme en millions d'euros ou de dollars.

Si vous répondez, vous aurez après diverses ruses l'inévitable page à remplir avec vos numéros de carte « pour vous virer vos millions de dollars »…

Ces mails sont envoyés par dizaines de millions au hasard et comme toujours des milliers de gogos se font avoir chaque jour. Ils semblent venir des US mais sont gérés industriellement par les mafias de l'Est.

Toute l'astuce est de vous demander comment cette somme fabuleuse vous sera virée. Vous devrez par la suite impérativement fournir toutes vos coordonnées bancaires et ils vous videront astucieusement votre compte…

Petits abus de confiance

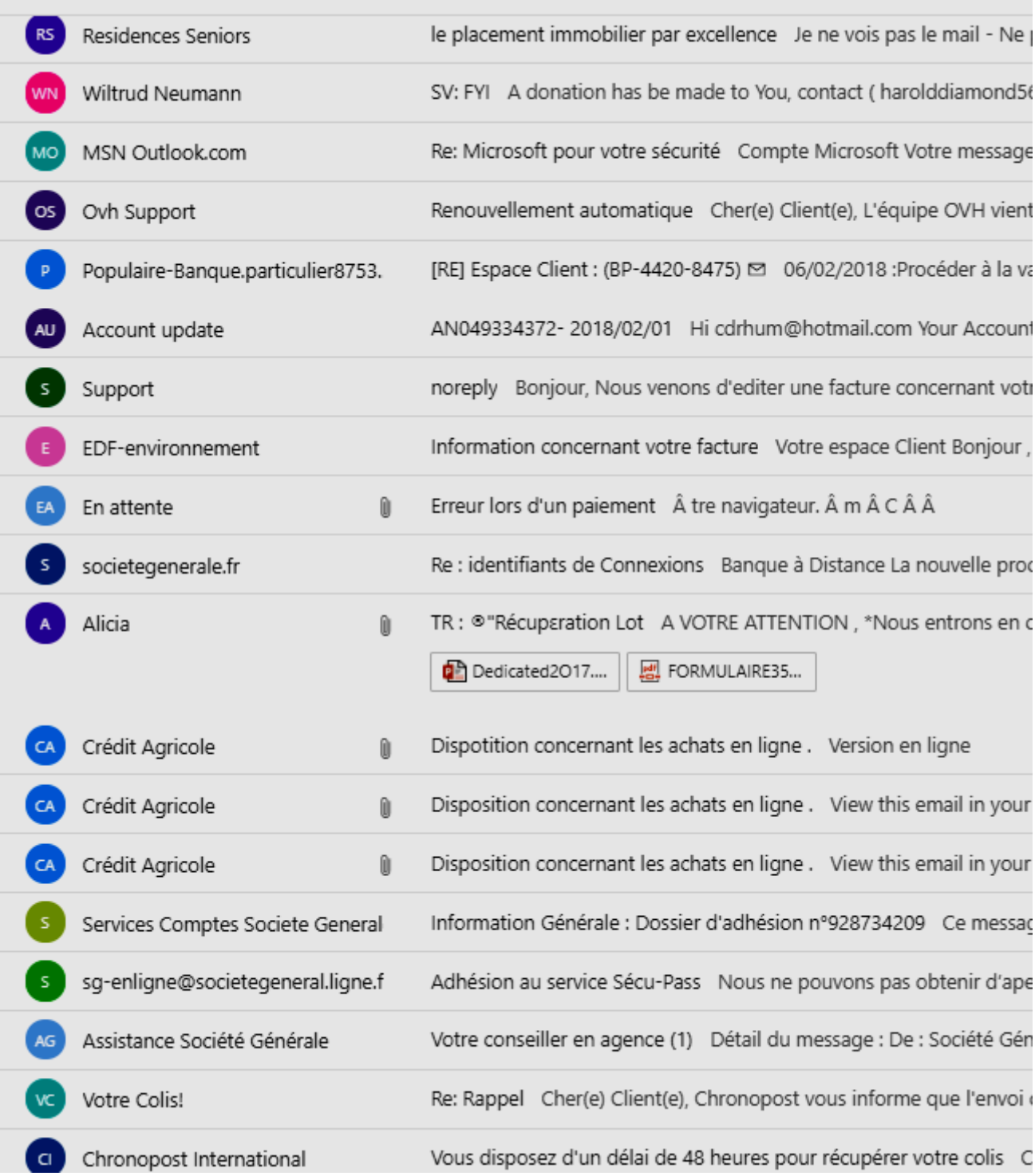
Une petite arnaque minable consiste à demander une petite somme en échange d'une méthode promise comme infaillible. Toute l'astuce tient à l'ambiguïté du contenu de l'annonce, suffisamment astucieuse pour ne pas être attaquable en justice.

Exemple: Envoyez-moi 100 Euros pour recevoir une méthode infaillible pour gagner beaucoup d'argent. En retour vous aurez une feuille disent "*Faites comme moi, vendez des méthodes pour s'enrichir facilement*", avec quelques conseils et lieux communs sur le travail qui enrichit.

Etc… etc… la liste n'est pas exhaustive, alors : **méfiance !**

Ne jamais faire sur le web ce qu'on ne ferait jamais dans la vie courante…

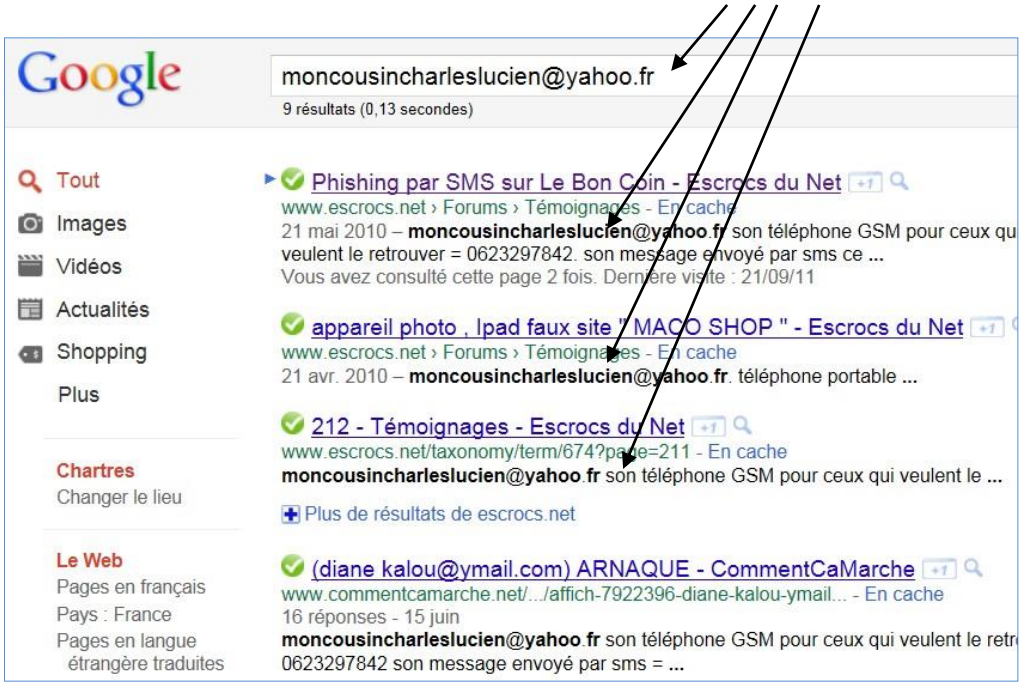
- **Quelques exemples de mails frauduleux que tout le monde reçoit ;**



- **Quelques sites de lutte contre les escroqueries du net :**
    - https://www.internet-signalement.gouv.fr
    - https://www.signal-spam.fr
    - http://www.escrocs.net

En cas de doute sur un mail suspect, ne pas hésiter à copier l'adresse et la coller dans la barre de recherche Google !

Ci-dessous, le résultat de la recherche de l'adresse du "cousin Charles"…



- **Quelques vidéos suggérant des conseils pour éviter les pièges des arnaques sur internet :**