# Phishing, kekseksa ? De la cybercriminalité bien sûr !

05/03/2020

## Bonjour le Monde !

**Le phishing (anglais) ou hameçonnage (français)**, est une tentative de vol d'information personnelle pour perpétrer une usurpation d'identité le plus souvent dans le but de voler de l'argent bien entendu…

Cela peut se faire de multiples façons mais les messages (instantanés, SMS et mails) sont le vecteur le plus courant de ces tentatives et je vais me concentrer là-dessus dans ce qui suit…

En 2016 et 2017, j'ai écrit une **série d'articles sur la cybercriminalité** qui mettait en lumière le manque total de concertation et d'efficacité dans la lutte contre les Ransomware et le phishing et puis les frémissements d'amélioration …

Nous sommes en 2020 et la lecture d'un petit encart dans Test-Achats me fait

revenir sur ce sujet toujours brûlant !

Comme déjà mentionné au rayon Geek dans Les News de Mars 2020, les signalements de phishing explosent en 2019 et ont déjà permis à la **Computer Crime Unit** de bloquer 4000 faux sites faisant du phishing !

La tendance actuelle des pirates est de vous envoyer un mail ressemblant à s'y méprendre à un mail provenant d'une grande enseigne (Colruyt, Lidl, votre banque, etc) et soit piquant votre curiosité soit essayant de vous faire peur pour que vous cliquiez sur des liens qui vous enverront évidemment sur un site pirate et qui vous soutirera un maximum d'information et/ou d'argent ! C'est ce genre de site que peut fermer la Computer Crime Unit grâce aux signalements !

Dans Les News de Mai 2019, je vous suggérais de vous entraîner à détecter un mail de phishing sur le site **https://www.cybersimple.be/fr/quiz/phishing** qui est toujours d'actualité, essayez ou ré-essayez donc !

**Prenons quelques exemples complètement fictifs:**

- **Promotion Colruyt**

1. vous recevez un message de Colruyt vantant une « promotion que vous ne pouvez pas rater »
2. **ne cliquez sur aucun des liens contenus dans ce message**
3. fermez ce message
4. visitez manuellement le site colruyt.be en entrant l'adresse du site vous-même dans votre navigateur Internet ou en faisant une recherche du site
5. vérifiez que cette promotion existe vraiment
6. si la promotion est soi-disant uniquement pour vous, prenez contact par un autre moyen avec Colruyt pour vérifier

- **Bon d'achat chez Lidl**

1. vous recevez un mail de Lidl vous offrant un bon d'achat de 500 €
2. **ne cliquez sur aucun des liens contenus dans ce message**
3. fermez ce message
4. visitez manuellement le site lidl.be en entrant l'adresse du site vous-même dans votre navigateur Internet ou en faisant une recherche du site
5. vérifiez que cette promotion existe vraiment
6. si la promotion est soi-disant uniquement pour vous, prenez contact par

un autre moyen avec Lidl pour vérifier

- **Solde impayé chez Carrefour**

1. vous recevez un mail de Carrefour vous enjoignant de payer le solde d'une facture en souffrance (ce qui peut arriver si vous avez acheté un article payable en plusieurs fois)
2. **ne cliquez sur aucun des liens contenus dans ce message**
3. fermez ce message
4. prenez contact par un autre moyen avec Carrefour pour vérifier

**Si vos doutes sont confirmés, c'est une bonne idée de signaler cette tentative de phishing, voici comment faire:**

En gros, il faut envoyer le message de phishing reçu à **suspect@safeonweb.be** mais de préférence sous forme de pièce jointe, ce qui fournira beaucoup plus d'informations utiles sur ce message frauduleux qui si vous le transférez simplement !

Si vous ne savez pas comment faire pour envoyer un message en pièce jointe, vous pouvez soit le transférer quand même soit suivre mes instructions ci-dessous…

**Comment envoyer un mail reçu en pièce jointe d'un autre message ?**

1. il faut sauver le mail reçu en tant que fichier (explications plus bas) – c'est l'étape inhabituelle et un peu difficile…
2. il faut ensuite créer un nouveau mail et lui joindre celui que vous venez de sauver (comme joindre un document ou une photo)
3. et enfin envoyer le tout à suspect@safeonweb.be

C'est le même principe que d'envoyer un document ou une photo en pièce jointe mais la difficulté est la première étape: sauver un mail en tant que fichier car la procédure est différente pour chaque client de messagerie !

**Allons-y pour les explications plus complètes:**

Certains clients de messageries permettent de sauver un mail en tant que fichier en utilisant « enregistrer sous » ou « exporter », d'autres ne permettent même pas de faire cela…

Dis donc Li P'ti Fouineu, **c'est quoi un client de messagerie ?**

Il faut d'abord savoir que vos mails sont conservés sur les disques durs d'un serveur mail (gros PC) localisé quelque part sur l'Internet et qui permet à un client de messagerie de se connecter pour gérer ces mails.

**Un client de messagerie est le programme avec lequel vous consultez vos mails en vous connectant au serveur mail !**

Il peut s'agir de votre navigateur Internet (**Firefox**, **Chrome**, **Safari** ou autres) qui accède au site web de votre messagerie (gmail.com, gmx.com, outlook.com, skynet.be ou autres) => on parle alors d'un **webmail** ou client web pour le mail !
Le webmail communique avec le serveur de mail via le protocole **HTTP**. Un protocole est une convention de langage qui permet à plusieurs appareils de communiquer entre eux, chaque protocole possède ses qualités et limitations propres.

Il peut aussi s'agir d'un programme installé sur Linux, Windows, macOS, Android, IOS ou autres comme par exemple **Thunderbird, Courrier, Mail** et **Outlook**.
Dans ce cas, le client de messagerie communique avec le serveur via le protocole **IMAP** pour la gestion de vos messages (lecture, effacement, etc) et via le protocole **SMTP** pour envoyer un nouveau mail à vos correspondants

**Note:** il ne faut pas confondre outlook.com qui est un webmail et Outlook 2010/2013/2016/2019 qui est un client de messagerie installé sur votre PC Windows avec Microsoft Office…

La communication entre les différents serveurs de mail se fait aussi via le protocole **SMTP**.
À chaque étape du trajet d'un mail, SMTP ajoute des informations dites de routage à votre message. Ces informations sont attachées au message mais ne sont pas visibles dans ce que vous présente votre client de messagerie.
Ce sont ces informations de routage qui sont perdues si vous transférez un mail plutôt que de le sauver en tant que fichier et de l'envoyer comme pièce jointe.

**Comment sauver un mail reçu en tant que fichier sur votre disque dur ou SSD ?**

- **Depuis Thunderbird** (Linux, Windows et macOS)

- Ouvrir le mail à sauver
- Menu « **Fichiers**«
- Option « **Enregistrer comme**«
- Option « **Fichier** Ctrl-S »
- Sélectionner où sauver le fichier
- Bouton « **Enregistrer**«
- Le mail est sauvé en tant que fichier au format EML

- **Depuis Courrier** (Windows 10)
  - Ouvrir le mail à sauver
  - Cliquez sur **les trois point horizontaux** du menu Autre dans le coin supérieur droit
  - Dans le menu, cliquez sur « **Enregistrer sous**«
  - Sélectionner où sauver le fichier
  - Bouton « **Enregistrer**«
  - Le mail est sauvé en tant que fichier au format EML

- **Depuis Outlook** 2010/2013/2016/2019 (Windows) ou Outlook 2011/2016/2019 (macOS)
  - Ouvrir le mail à sauver
  - Menu « **Fichiers**«
  - Option « **Enregistrer sous ...**«
  - Sélectionner où sauver le fichier
  - Sélectionner le format Texte (TXT) ou HTML (EML n'existe pas)
  - Bouton « **Enregistrer**«
  - Le mail est sauvé en tant que fichier au format TXT ou HTML

- **Depuis Mail** (macOS)
  - Ouvrir le mail à sauver
  - Menu « **Fichiers**«
  - Option « **Enregistrer sous ...**«
  - Sélectionner l'emplacement où sauver le ficher
  - Sélectionner le format « **Source du message brut**«
  - Le mail est sauvé en tant que fichier au format EML à l'emplacement sélectionné

- **Depuis Gmail** (webmail)
  - Ouvrir le mail à sauver

        - Cliquer sur les 3 points verticaux à droite de la date du message
        - Choisir « **Télécharger le message**«
        - Le mail est sauvé en tant que fichier au format EML dans votre dossier de téléchargement

- **Depuis Outlook.com** ou Hotmail.com ou MSN.com (webmail)
    - **il est impossible de sauver un mail en tant que fichier !**

- **Depuis GMX.com** (webmail)
    - Ouvrir le mail à sauver
    - Cliquer sur le bouton « **Sauvegarder** » en haut à droite (icône disquette)
    - Le mail est sauvé en tant que fichier au format EML dans votre dossier de téléchargement

Il faut noter que le fichier ainsi sauvé peut être ouvert/consulté avec un éditeur de texte et inclut toutes les informations de routage.
Ouvrez donc le fichier sauvé avec Notepad (Windows) ou TextEdit (macOS) ou Gedit (Linux) pour voir à quoi ça ressemble…

Il ne vous reste plus qu'à créer un nouveau message, taper une petite explication avec vos mots à vous, attacher le fichier juste sauvé et envoyer ce message à **suspect@safeonweb.be**

**Safe**on**web** est une initiative du **Centre for Cyber Security Belgium**

# Li P'ti Fouineu vous salue bien !