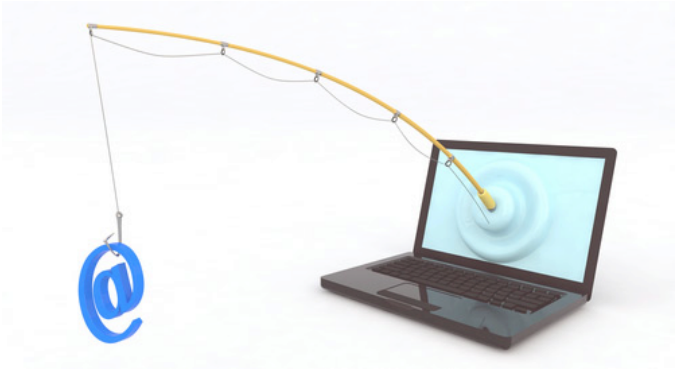
L'hameçonnage (ou phishing)

Comment le détecter et s'en protéger ?



Le but des malveillants :

Leur seul but est de récupérer vos coordonnées bancaires :

- N° de carte de crédit avec code de sécurité
- Codes d'accès à la gestion de vos comptes en ligne
- Codes d'accès aux organismes publics
- Adresses courriels à des fins publicitaires
- etc…

La forme :

- un courriel semblant venir de votre **FAI** (Fournisseur d'Accès Internet) type Orange, Free, SFR, etc. vous indiquant que votre banque a refusé le prélèvement automatique et que vous devez régulariser au plus vite, sous peine de supprimer votre compte.
- un courriel semblant venir de votre **banque** vous indiquant qu'un message important vous attend ou que le mode de connexion a changé pour améliorer la sécurité
- un **organisme officiel** (CAF, impôts…) vous indique que vous avez droit à un remboursement et qu'ils ont besoin de vos coordonnées bancaires.

Leur imagination est sans limite !

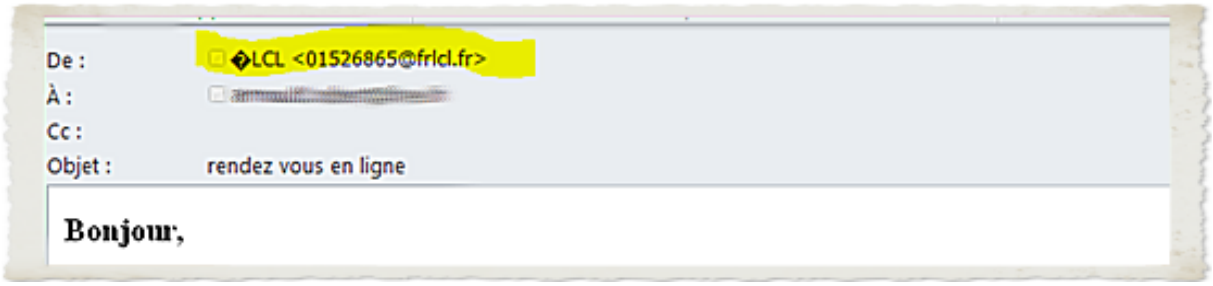
Tous ces courriels contiennent un lien sur lequel vous devez cliquer.
La règle d'or est de ne **JAMAIS CLIQUER DIRECTEMENT SUR LE LIEN !**
Tout au plus, recopiez-le dans votre navigateur internet (Firefox, Chrome, Internet explorer, Opera, Safari…).

Comment les repérer ?

Un certain nombre d'indices permettent de repérer les courriels frauduleux à coup sûr :

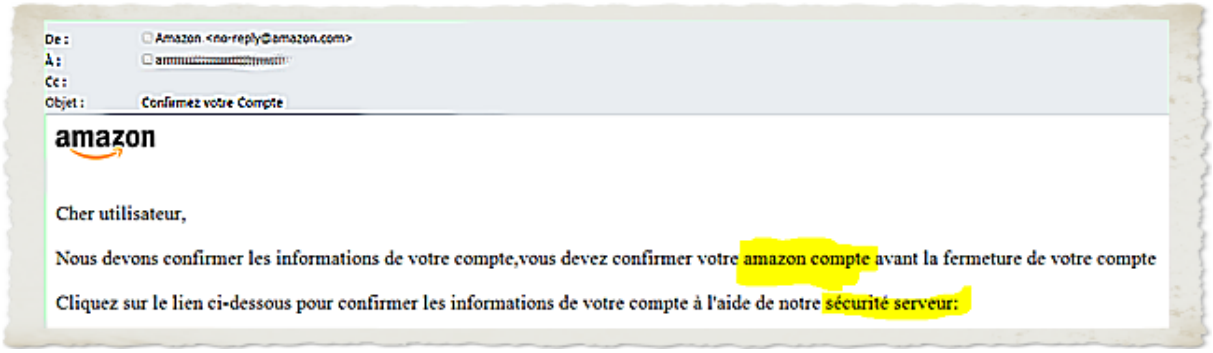
1. **Vous n'êtes pas client** de la banque ou du FAI ou usager de l'organisme. Il s'agit bien sûr d'un faux ! Il est inutile d'ouvrir le courriel car vous risqueriez de valider votre adresse. Et elle pourrait être réutilisée ou revendue à d'autres malveillants. Le supprimer simplement.

2. **Etudier l'adresse de l'émetteur**

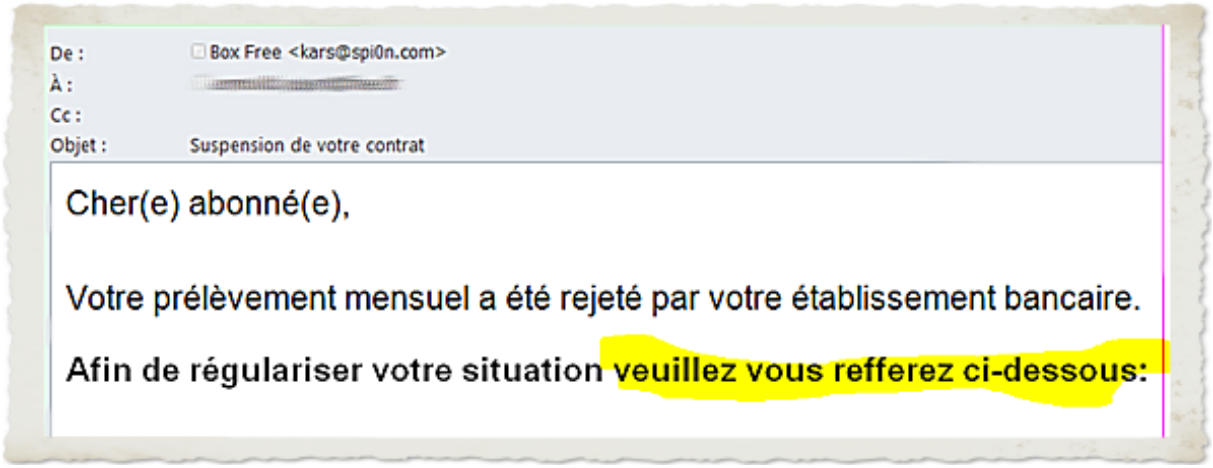


Dans ce cas, nous constatons que l'émetteur n'est pas la banque.
Il faut regarder attentivement le libellé de l'adresse : il ressemble souvent à l'adresse officielle.
Exemples : amazone.com ou **amason.com** à la place de **amazon.com**

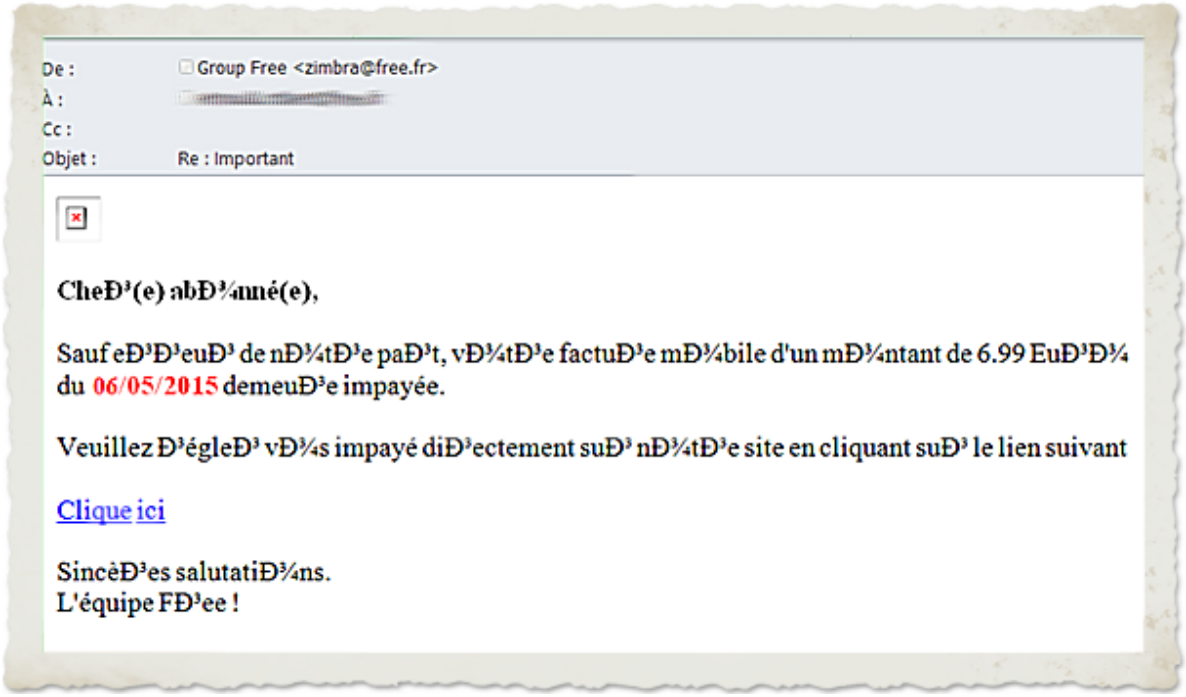
3. **Après ouverture du courriel, regarder la langue, les fautes d'orthographe et le style**



Un courriel dans une langue étrangère est à priori suspect.



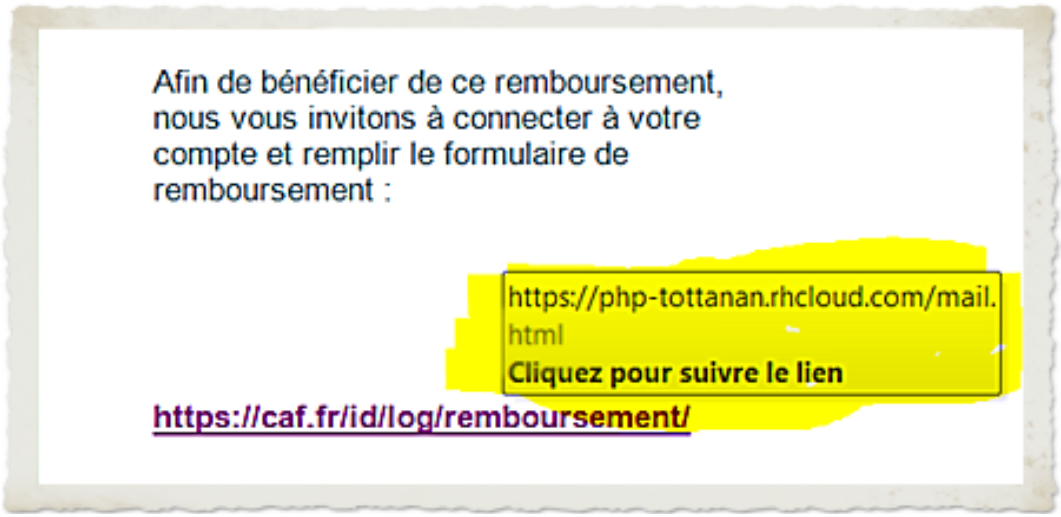
Repérez les fautes d'orthographe.



Ici le style montre clairement un mail frauduleux.

4. **Vérifier l'adresse effective du lien proposé**

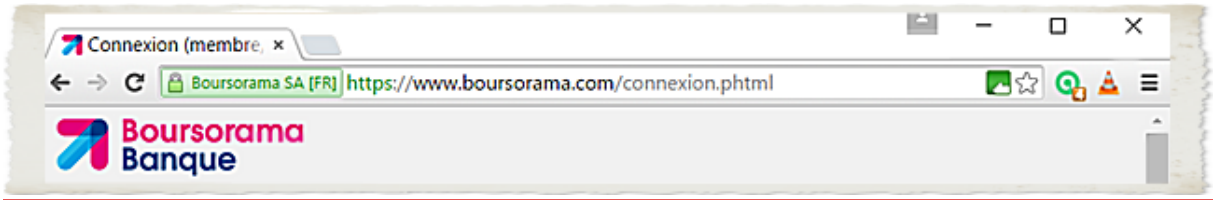
Le passage de la souris sur un lien fait apparaitre sa véritable valeur. Le plus souvent, une fenêtre « pop-up » apparaît, comme ci-dessous, mais le lien peut également apparaître dans une ligne en bas de l'écran selon votre navigateur internet.



Et si vous avez cliqué ?

Vous arrivez en général sur un site qui ressemble à s'y méprendre au site officiel.
Tout n'est pas encore perdu car il y a encore des choses faciles à vérifier !

1. **La barre d'adresse**



Vérifiez s'il s'agit bien du site censé vous adresser le courriel (voir ci-dessus un exemple tout à fait valide).

Il doit commencer par **HTTPS:// et/ou afficher un petit cadenas (🔒)** s'il vous demande des coordonnées confidentielles (n° de compte, mot de passe etc.).
Le cadenas est situé soit au début de la barre d'adresse (en haut) soit dans la barre d'état en bas selon le navigateur et sa version.
Si ce n'est pas le cas, fermez immédiatement la session

2. **Le contenu**

Vérifiez les fautes de français et d'orthographe. Dans l'exemple ci-dessous, aucun des liens en bas de page n'est actif et il manque le bouton d'aide vocale présent sur le site d'origine.

La conduite à tenir

- **Vous avez déjoué le piège**

Bravo, tout va bien !
Vous pouvez transférer le courriel à l'expéditeur officiel qui a, en général, une boîte aux lettres spécifique réservée à ce signalement.
Le site http://phishing-initiative.com/ permet également de signaler le problème à des spécialistes qui agiront en conséquence auprès des éditeurs des navigateurs internet.
Détruisez le courriel puis mettez l'expéditeur dans la liste des courriels indésirables.

- **Vous vous êtes fait piéger**

Il est impératif de **MODIFIER IMMEDIATEMENT vos identifiants d'accès** (mot de passe) et/ou de contacter votre banque pour **faire opposition sur votre carte de crédit** (**N° interbancaire : 08 92 705 705 (0,34€/min)).**
Surveillez également attentivement vos relevés bancaires dans les semaines qui suivent. En cas d'anomalie, le signaler à votre banque qui doit vous rembourser (*Article L133-18 du code monétaire et financier*).
Vous trouverez de plus amples informations sur les sites :
http://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/Phishing-hameconnage-ou-filoutage,
http://arnaqueinternet.com/arnaque-internet-que-faire/
https://fr.wikipedia.org/wiki/Hameçonnage .

NB : Tous ces exemples ont été effectivement reçus par l'auteur.

Robert Arnould-Laurent