Sécuriser sa messagerie (mail)

Quelques conseils pour sécuriser sa messagerie internet.

Des sites à visiter :

- https://www.ssi.gouv.fr/entreprise/precautions-elementaires/5-reflexes-a-avoir-lors-de-la-reception-dun-courriel/

- https://o.nouvelobs.com/high-tech/20140507.OBS6330/victimes-du-piratage-d-orange-5-conseils-pour-ne-pas-se-faire-pieger.html

- https://communaute.orange.fr/t5/prot%C3%A9ger-mes-donn%C3%A9es-et-mon/s%C3%A9curiser-l-acc%C3%A8s-%C3%A0-ma-bo%C3%AEte-mails/td-p/524296

- https://coreight.com/content/10-conseils-pour-securiser-son-compte-google

1 Ne pas répondre à n'importe qui !!

N'importe qui peut vous envoyer un courriel (mèle ou mail) en se faisant passer pour un autre ! Cela n'est pas beaucoup plus compliqué que de mettre un faux nom d'expéditeur au verso d'une enveloppe.

Se méfier si :

- on a un mèle de quelqu'un que l'on ne connaît pas
- on vous demande de l'argent, même si c'est votre ami
- quelqu'un que vous connaissez, vous demande de ne répondre qu'à ce mail et pas au téléphone
- un organisme officiel, ou votre banque vous demande votre mot de passe, ou votre numéro de carte bleue.
- Se méfier si on vous demande de diffuser une information sur des virus à tous vos contacts. Le virus c'est la multiplication des mails..

2 Bien choisir un mot de passe

Un mot de passe idéal est celui que vous fournit Orange au départ. Mais ce n'est pas facile de le retenir. Normalement, un mot de passe contient entre 8 et 12 caractères, avec des majuscules, des chiffres et des caractères spéciaux. Exemple : aiRvD1h20*M-

Il faut éviter de mettre son nom ou son prénom.

Pour retenir un mot de passe, on peut l'extraire d'une phrase.

Exemple : le petit chaperon rouge et deux loups étoilés, donne = Lpcre2l*

Ou bien : les violons de l'automne bercent mon cœur = lvdlabmC

3 Se déconnecter après chaque utilisation

Remarque : vérifier avant, que vous avez le bon mot de passe de connexion.

Fermer la fenêtre du navigateur internet ne déconnecte pas sa messagerie. Il faut se déconnecter, si la session reste ouverte, on peut avoir accès à votre messagerie sans mot de passe.

Pour Orange :

Pour se déconnecter, passer la souris sur votre nom en haut à droite, une fenêtre s'ouvre :

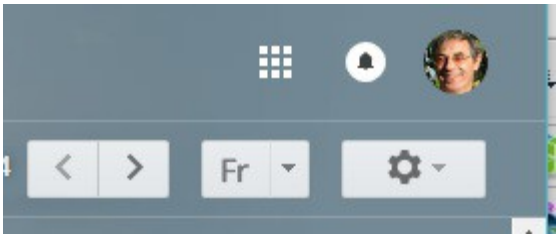
Cliquer sur Se déconnecter.

Si vous avez en haut à droite de votre cran

C'est que vous n'êtes pas connecté.

Pour Google

Pour se déconnecter, cliquer sur votre image en haut à droite



Une fenêtre apparaît :

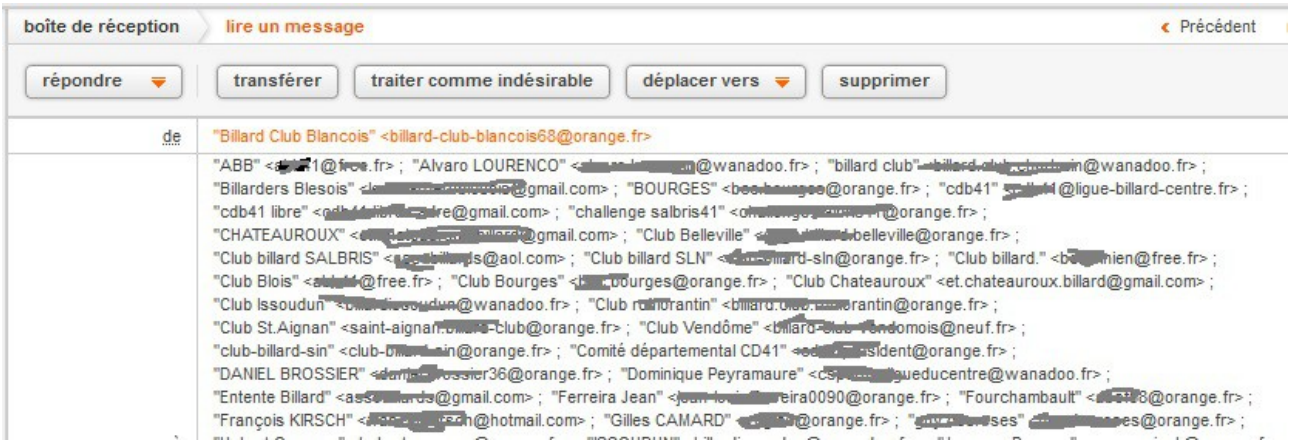
Cliquer sur Déconnexion.

4 Envoyer en copie cachée les mails pour plusieurs personnes

Il se peut que vous ayez des mails à envoyer à plusieurs personnes en même temps, par exemple pour un club, ou une association. En général on crée des groupes dans les contacts pour sélectionner un ensemble de contacts.

Ne pas mettre ce groupe dans le cadre de l'expéditeur. Si quelqu'un intercepte ce mail, il a l'adresse de tous ces contacts.

SURTOUT A EVITER :



Mettre ce groupe en copie cachée : CCI

Pour Orange :

pour Gmail :

5 Vérifier l'adresse de l'expéditeur

Pour déterminer s'il s'agit d'un courrier électronique frauduleux ou non, il est aussi possible de vérifier l'adresse mail qui accompagne le message. Si c'est un faux e-mail, l'adresse de l'expéditeur ne correspond pas à celle utilisée couramment par l'opérateur.

Par exemple :

pour la sécurité sociale, Ameli l'adresse est :

https://assure.ameli.fr/PortailAS/appmanager/PortailAS/

méfiez-vous de

http://user.assure.ameli.fr/portail

le *'user'* en plus est un site qui imite *assure.ameli* , c'est un détournement, en plus c'est *http* et non *https*

6 Vérifier les informations que l'on vous demande de diffuser

Il y a un site qui recense toutes les mauvaises informations (canular) qui sont diffusées sur internet.

Le site : http://www.hoaxkiller.fr/ (hoax en anglais = canular, killer = tueur)

Si on vous dit de diffuser qu'il y a un virus dans tel programme, vérifier avant dans le site Hoax.

Pour rechercher :

Ouvrir le site hoaxhiller.fr et remplir la case centrale avec le texte ou le sujet que l'on vous envoie.

Cliquer sur *Recherche Hoaxkiller.fr*

7 Ajouter des 'faux' contacts

En général, ceux qui piratent votre messagerie s'intéressent à vos contacts pour leur envoyer un message 'Fishing'. Si vos contacts répondent à ce message, ils seront aussi piratés. Souvent ce message demande de l'aide, une somme d'argent et de ne répondre que par mail et non par téléphone.

Pour bloquer en partie les robots (programmes) qui piratent, créer un contact du genre : aa.11@orange.fr : un contact qui n'existe pas et qui apparaît en tête des contacts. Ainsi les robots sont bloqués à cause de l'erreur d'envoi, ou au moins vous serez averti par le WebMaster qu'un envoi vers une adresse inexistante a été tenté, ce qui vous mettra la puce à l'oreille.