Attention hackers !

(Hacker = Pirate et escroc informatique)

Dès que vous utilisez l'informatique (ce qui devient quasi obligatoire de nos jours) vous pouvez faire de mauvaises rencontres … Notre objectif n'est pas de déclencher chez vous des crises de paranoïa, mais de vous mettre en garde contre quelques techniques les plus répandues utilisant les messages électroniques (mails) et les Pop-up (fenêtres internet intempestives).

1 - Le faux mail :

Vous recevez d'un de vos contacts (amis, relations, …) un mail un peu bizarre. Ce message dit que votre contact est en détresse à l'étranger, que vous ne pouvez pas lui téléphoner, mais que vous pouvez lui répondre par mail ; si vous répondez au mail votre contact expliquera avoir besoin d'un peu d'argent pour s'en sortir...

Règle n°1 : Ce n'est pas parce que le mail est expédié par un de vos amis qu'il est obligatoirement vrai ! Un hacker a pu pirater sa boite aux lettres électroniques et envoyer à tous ses contacts un faux message.

Le mieux est de téléphoner à cet ami pour vérification.

Le plus souvent votre ami est tranquille chez lui !

2 - Pièce jointe et lien inséré dans un mail :

Soyez vigilant avant d'ouvrir des pièces jointes à un courriel :

Elles peuvent colporter des codes malveillants. **Une des méthodes les plus efficaces pour diffuser des codes malveillants est d'utiliser des fichiers joints aux courriels**. Pour se protéger, ne jamais ouvrir les pièces jointes dont les extensions sont les suivantes : .com; .bat; .exe; .vbs; .lnk; .pif; (Comme par exemple une pièce jointe appelée photos.pif)
À l'inverse, quand vous envoyez des fichiers en pièces jointes à des courriels privilégiez l'envoi de pièces jointes au format le plus « inerte » possible, comme RTF ou PDF par exemple.

Vous recevez un mail d'une personne ou d'un organisme : Banque, Sécurité Sociale, Mutuelle, … qui vous demandent de cliquer sur un lien pour actualiser vos coordonnées et références : **n'en faites rien sauf si vous-même êtes à l'origine du message**.
Autre exemple, La Mutuelle Générale avertit ses adhérents par mail de l'existence d'un nouveau décompte, et invite à cliquer sur le lien contenu dans le mail pour en prendre connaissance. **Il vaut mieux procéder autrement :** vous fermez votre messagerie, vous allez sur Internet et accédez au site de la Mutuelle Générale, (vous êtes sûr d'aller sur le site authentique). En entrant sur votre espace personnel vous serez en sécurité.

Règle n°2 : Soyez vigilant ! Ouvrir une pièce jointe ou cliquer sur un lien n'est pas anodin ! Vous risquez de téléchargez de petits programmes qui peuvent voler vos données et/ou perturber votre système !

3 - Le phishing (hameçonnage ou filoutage)

Cette arnaque est liée à la précédente. Un lien vous fait entrer sur un site avec l'intitulé, le logo, l'identité graphique de votre banque, des Impôts, de la Sécurité Sociale, ou d'une grande société du commerce… Vous ne vous méfiez donc pas ! Souvent, un message vous invite à confirmer vos coordonnées, votre code d'accès, …. Il arrive par exemple que les Impôts (sic !) vous informent que vous avez un trop-perçu et qu'il faut cliquer sur le lien joint pour valider la procédure de remboursement. **Surtout n'en faites rien !** Car vous risquez de fournir des données sensibles ou de télécharger des programmes plus ou moins toxiques ou malveillants ! Dans d'autre cas, un logo du Gouvernement peut apparaitre, en indiquant que vous êtes soupçonné d'être un pirate ou un terroriste informatique ! Vous devez répondre au questionnaire dans le fichier joint pour justifier que vous êtes un honnête citoyen ! **Là encore, il s'agit d'un piège ne cliquez pas sur le lien proposé**. Vous pourriez fournir des informations sensibles et/ou de télécharger un programme malveillant !

Règle n°3 : Tout message que vous n'avez pas sollicité doit vous inciter à la prudence ! Des spécialistes en design (infographistes) peuvent copier à s'y méprendre la chartre graphique d'une entreprise (publique ou privée) pour vous mettre en confiance !

4 - Le message d'annonce de virus et/ou le message menaçant et autoritaire :

Vous êtes tranquillement sur Internet et, soudain, un message s'affiche sur votre écran indiquant qu'un virus terrible vous menace !
Vous avez moins de 2 minutes pour cliquer afin de protéger votre ordinateur, sinon toutes vos données et photos seront effacées ! !

Règle n°4 : Réfléchissez : C'est un piège ! L'objectif est de vous paniquer, vous empêcher de réfléchir. C'est en cliquant intempestivement que vous risquez de téléchargez un virus ! !

5 - Le Ransomware (Logiciel rançonneur) :

Le Ransomware prend en otage vos données personnelles !
En effet, si vous n'avez pas été assez vigilant, notamment lors d'un téléchargement intempestif, votre système se bloque ! Un message vous demande de payer une rançon pour débloquer votre ordinateur. Le paiement se fait souvent en monnaie virtuelle (bitcoins) ou autres, difficilement traçables par la police.

Règle n°5 : Les spécialistes recommandent de ne pas payer la rançon. Rien ne garantit que votre système soit débloqué par les pirates après l'encaissement de la rançon.

Essayez plutôt de fermer la session (Ctrl + Alt + Suppr), puis (comme ça ne marchera pas si le rançonneur est bien fait) **éteignez votre ordinateur avec le bouton de mise en marche (pour forcer l'arrêt il faut maintenir le bouton « marche / arrêt » appuyé pendant 5 secondes).**
Votre système n'aura pas été éteint selon la procédure et vous aurez droit à un test de Windows ; c'est un moindre mal !

Ce ne sont que quelques exemples d'arnaques et de piratages informatiques, tant l'imagination et les compétences techniques des hackers sont sans limites !
Donc, pas de paranoïa mais une vigilance de bon aloi ! Pensez à faire très régulièrement, une (ou mieux deux) sauvegardes (« back up ») de vos données personnelles (bureautique, photos, vidéos, musiques …) sur un support amovible : Au cas où il faudrait réinitialiser votre ordinateur, vous pourrez ensuite réinstaller vos données sauvegardées.
Un homme averti en vaut deux (proverbe qui vaut aussi pour les dames) ! ! !

De façon générale il vaut mieux éviter d'ouvrir un mail de provenance suspecte et, surtout, avant de faire ce qu'on vous demande, par pitié, prenez le temps de réfléchir aux conséquences néfastes pour vous !

Et n'oubliez pas : le lundi après-midi de 15h15 à 17h30 l'atelier informatique de l'ANR peut vous recevoir pour vous conseiller et, si possible, vous tirer d'un mauvais pas.

PIRATAGE DE BOITE MAIL

Un ami vous demande de cesser de lui envoyer des courriers bizarres ? C’est que votre boîte mail a été piratée.

Mode d’emploi pour ne plus vous faire piéger.

Et si ça n’arrivait pas qu’aux autres… Avides de soutirer des infos personnelles, les pirates s’attaquent aux webmails (Outlook, Gmail, etc.). Dans le meilleur des cas, ils utiliseront votre adresse pour inonder vos contacts de publicités plus ou moins agressives.

Mais le détournement peut aussi déboucher sur de véritables arnaques: tentative de phishing, ingérence dans un échange commercial (une location de vacances, par exemple) afin d’amener votre correspondant à verser de l’argent sur un compte hébergé dans un pays lointain. **Si vous êtes victime d’une telle attaque, vous devez avant tout reprendre le contrôle de votre messagerie**. Il sera temps ensuite de renforcer la sécurité de votre boîte mail pour éviter une récidive.

Testez votre adresse électronique pour savoir si elle est détournée

Comment savoir si un intrus a pris le contrôle de votre compte de messagerie ?
Les symptômes dépendent de la méthode employée pour détourner votre adresse. Les plaintes émanant de vos amis constituent un premier indicateur. Vous pouvez également surveiller périodiquement le contenu du dossier **Messages envoyés** de la version Web de votre webmail.

En revanche, si vous utilisez un logiciel de messagerie installé sur votre ordinateur, **Outlook 2013** ou **Thunderbird**, seuls les courriers expédiés depuis l’ordinateur sont stockés dans le dossier d’envoi local, vous n’y découvrirez pas de traces d’intrusion. **Autre moyen de contrôle : le tableau de bord ou la page de suivi d’activité de votre webmail**. Avec Hotmail (ou Outlook.com), cliquez sur **Vérifier l’activité récente** dans la section **Sécurité et confidentialité**.

Si vous y notez des informations concernant les protocoles POP3, SMTP ou Imap, vérifiez que vous en êtes bien à l’origine. Il pourrait aussi s’agir de dispositifs de redirection mis en place par un pirate. **Si vous utilisez** Gmail, accédez au **Tableau de bord** (https://accounts.google.com/ServiceLogin?) de votre compte Google et cliquez sur **Gmail**. Observez le nombre de courriers signalés dans la section **Messages envoyés** et l’heure du dernier envoi. Si ces données sont anormales, l’hypothèse du détournement de la messagerie doit être envisagée.

Tracez l’e-mail du spammeur

Demandez à un ami ayant reçu un courrier douteux de votre part de vous le transmettre. Pour afficher les infos de suivi de l’e-mail avec **Outlook.com**, faites un clic

droit sur le message et choisissez **Afficher la source du message**. Avec **Gmail**, cliquez sur la flèche **Autres**, à droite du bouton **Répondre**, puis sur **Afficher l'original**. Si vous utilisez un client de messagerie type **Thunderbird** ou **Outlook**, affichez le message et déroulez le menu **Affichage**, **Code source du message**. Dans la section **Received From**, copiez l'adresse IP, généralement indiquée entre crochets [212.180.xx.x]. Accédez au site http://ip-lookup.net/, collez l'adresse IP dans la zone de saisie, cliquez sur la loupe, puis sur **IP owner info** (Whois) pour connaître le propriétaire de l'e-mail. Vérifiez l'adresse physique dans la partie **OrgName** et **Address**. Sollicitez les services de Google Maps pour géolocaliser le pays d'origine du spammeur. Sachez néanmoins que si les pirates sont expérimentés, ils auront pris soin d'effacer leurs traces.

Changez le mot de passe

La première chose à faire pour mettre un terme au détournement consiste à modifier et consolider le sésame de votre compte e-mail. Il est conseillé d'inventer une phrase mêlant lettres majuscules, minuscules, symboles et chiffres pour obtenir un code inviolable du genre: 69_JeN-mPas@Ma#BElleMere, par exemple. Surtout, évitez d'utiliser le même pour vos différents comptes de messagerie et **pensez à en changer régulièrement** (tous les trois mois). Vous pouvez également recourir à un gestionnaire spécifique comme Dashlane (www.dashlane.com/fr), qui générera des mots de passe sécurisés.

Scannez votre ordinateur à la recherche de malwares

Le détournement de votre compte mail peut reposer sur un logiciel espion installé sur votre ordinateur. Pour éradiquer d'éventuels malwares, servez-vous d'un utilitaire spécialisé tel qu'**AdwCleaner**, gratuit, léger, il s'installe et se désinstalle rapidement et se montre particulièrement efficace. Pour faire bonne mesure, téléchargez et installez **ZHP Cleaner**. Cet outil ne nécessite pas d'installation. Il rétablit les paramètres des proxys, supprime les redirections mises en place dans votre navigateur, élimine les barres d'outils et les pages d'accueil parasites.

Analysez les e-mails et les fichiers téléchargés

On ne le dira jamais assez : vous devez manipuler avec une extrême prudence les e-mails dont vous ne connaissez pas l'expéditeur. Prenez garde de ne pas ouvrir les pièces jointes d'origine douteuse et ne cliquez pas sur les liens contenus dans les messages potentiellement dangereux. Il suffit généralement d'un clic pour inoculer un logiciel malveillant !

Qu'il s'agisse de pièces jointes, d'applications ou d'un document téléchargé sur Internet, avant de les décompresser, de les ouvrir ou de les installer, faites un clic droit sur le fichier depuis l'Explorateur de Windows et choisissez la commande **Analyser** ajoutée au menu contextuel lors de l'installation de votre antivirus. Vous serez ainsi prévenu à temps d'une éventuelle menace.

Actualisez les infos de sécurité

Si vous êtes un adepte d'Outlook ou de Gmail, sachez que Microsoft et Google conservent des informations de sécurité vous concernant et peuvent ainsi vous prévenir en cas d'utilisation frauduleuse de votre compte. Tenez ces infos à jour en remplaçant une

vieille adresse mail ou un numéro de portable obsolète. **Pour Outlook**, allez dans la partie **Sécurité** de votre compte Microsoft et cliquez sur **Gérez vos informations de sécurité** (partie 02). **Pour Gmail**, accédez au **Tableau de bord Google**, cliquez sur **Gérer mon compte** (partie Compte), puis **Ajouter un numéro de téléphone pour sécuriser votre compte**.

SOURCE : MonPcPro
(c’est un site gratuit proposant des Tutoriels Informatique, de l’actualité sur le Web et les Nouvelles Technologies.

Pour Android, iOS, Mac, Windows et Linux)