Sécurité informatique

• Le phishing

Le phishing (hameçonnage ou filoutage en français) est une technique utilisée par des personnes malveillantes. Celles-ci envoient des mails frauduleux **en se faisant passer pour des sociétés ou organismes connus.** Elles vous demandent en général de mettre à jour votre compte sous peine de le supprimer, et vous proposent pour cela de vous connecter en cliquant sur un lien où vous devrez entrer vos coordonnées bancaires, parfois même votre code bancaire, vos identifiants et mot de passe.

La solution : reconnaître les mails frauduleux

Les mails menaçants sont toujours suspects. Si vous recevez un mail de votre opérateur, de votre banque, d'un magasin en ligne ou tout autre organisme qui vous menace de supprimer votre compte, soyez vigilants. Jamais l'un de vos fournisseurs ne vous demandera de vérifier votre compte de cette façon. **Ne cliquez pas sur le lien, même si le site paraît officiel !**

Ne remplissez jamais une demande de données personnelles et en particulier celles concernant votre carte bancaire.

Allez sur le site du fournisseur directement sans toucher aux liens dans le mail. **Une banque n'envoie jamais de lien dans un mail.**

Autres indices récurrents : l'orthographe et la tournure des phrases sont d'un niveau moyen et les accents mal retranscrits. Si vous avez un doute, contactez l'organisme ou tapez vous-même son adresse dans votre navigateur afin de vous connecter à votre compte.

• Les virus et Le pirate informatique

Un virus ou un ver informatique est un programme malveillant capable de contaminer les ordinateurs via les réseaux. Les plus dangereux peuvent infecter un ordinateur en exploitant une faille dans le système d'exploitation, d'où l'importance de faire les mises à jour des logiciels (Windows, Flash…). **Ils peuvent également être dissimulés dans des pièces jointes à des mails ou dans des URL**. C'est pourquoi il ne faut jamais cliquer sur une pièce jointe ou un lien suspect.

Les pirates informatiques créent des virus informatiques et des "chevaux de Troie", des logiciels capables de dérober des codes d'accès de comptes bancaires, ou de promouvoir des produits ou services sur les ordinateurs de leurs victimes. **Ils peuvent utiliser illégalement les ressources des ordinateurs infectés** afin de développer et de lancer des campagnes de spams, des attaques contre des réseaux pour les empêcher de fonctionner…

La solution : opter pour une solution complète

Nous vous recommandons d'installer un logiciel de protection sur tous vos appareils connectés à internet et de le mettre régulièrement à jour afin de vous protéger des menaces les plus récentes. **Il existe des antivirus complets et gratuits** (https://www.avira.com , www.avast.com) sont parmi les principaux pour une protection de base souvent suffisante.

Il existe des solutions payantes. Elles s'achètent sur les sites internet des éditeurs de sécurité (Norton, Bitdefender, Kaspersky, Secure, McAfee…).

• Piratage ou usurpation d'adresse mail

Si vous recevez un mail étrange et a priori inquiétant je suis à l'étranger et j'ai un gros problème…..

Ne répondez pas, ne vous inquiétez pas, supprimez-le. Si vous connaissez la personne appelez là et dites-lui qu'il est victime d'un piratage. *(Nous reviendrons sur la procédure dans un prochain bulletin).*

Hubert Suret