EMARGENCE
Expertise Comptable

Cybercriminalité : que faut il faire ?

N°2.2 | mai 2017 **2ème Partie**

Quelques règles de sécurité informatique.
Ou comment réduire de manière significative les risques de piratage de mes données avec quelques gestes simples.

Utilisez des mots de passe de qualité

Cela peut faire sourire mais en 2015 le classement des 10 mots de passe les plus utilisés sur la planète était encore : 123456, password, 12345, 12345678, … *(source rapport 2015 – Splashdata.com)*

Le bon geste : un mot de passe doit être constitué de lettres minuscules, majuscules, de chiffres, de caractères spéciaux et faire 10 caractères environ. Surtout il ne doit pas correspondre à des éléments personnels pouvant vous identifier (date de naissance, prénom, nom).

Avoir un système d'exploitation et des logiciels à jour

Assurez-vous que vos antivirus soient bien activés et que vos logiciels (navigateurs, bureautique, pare-feu personnel, etc.) soient mis à jour régulièrement. Ces correctifs sont indispensables pour s'assurer que les agresseurs ne puissent utiliser les failles de l'ordinateur.

Effectuez des sauvegardes régulières

Pour s'assurer de la continuité de votre activité il est primordial d'effectuer des sauvegardes régulières (quotidiennes ou hebdomadaires). Que ce soit sur support physique (DVD, clé USB) ou via le Cloud, la sauvegarde vous permettra de faire face à des imprévus, qu'ils soient matériels (dysfonctionnement de votre ordinateur) ou malveillance externe (piratage informatique).

N'ayez pas une confiance aveugle dans le nom de l'expéditeur

Soyez donc attentif à tout indice mettant en doute l'origine réelle du courriel, notamment si le message comporte une pièce jointe ou des liens : incohérence de forme ou de fond entre le message reçu et ceux que votre interlocuteur légitime vous envoie d'habitude, par exemple. En cas de doute, contactez votre interlocuteur pour vérifier qu'il est à l'origine du message

Méfiez-vous des liens et pièces jointes

Soyez vigilant avant d'ouvrir des pièces jointes à un courriel, elles colportent souvent des codes malveillants. Pour se protéger, n'ouvrez jamais les pièces jointes dont les extensions sont les suivantes : .com ; .bat ; .exe ; .pif ; .vbs ; .lnk. De même, ne cliquez pas à l'aveuglette sur les liens d'un courriel. En passant la souris au-dessus du lien proposé, vous pouvez repérer s'il pointe bien vers l'adresse du site annoncée dans le message. Si l'adresse est différente, soyez méfiant, et évitez de cliquer sur le lien. Préférez inscrire l'adresse vous-même dans votre navigateur. Si votre poste a un comportement anormal (lenteur, écran blanc sporadique, etc.), faites-le contrôler.

Contrôlez la diffusion d'informations personnelles

Ne répondez jamais directement à une demande d'informations confidentielles. Les demandes d'informations confidentielles, lorsqu'elles sont légitimes, ne sont jamais faites par courriel (mots de passe, code PIN, coordonnées bancaires, etc.). Au moindre doute il vaut mieux s'abstenir.

Ne relayez pas de canulars

Quel que soit l'expéditeur il ne faut jamais rediffuser de messages types « chaînes de lettres, porte-bonheur, appel à solidarité, alertes virales, etc. ». Vous risquez une saturation du réseau et d'induire vos interlocuteurs en erreur.

Paramétrez correctement votre logiciel de messagerie

Pensez à activer la mise à jour automatique. Paramétrez également votre logiciel pour désactiver la prévisualisation automatique des courriels. S'il s'agit d'un email malveillant, l'ouverture automatique indiquerait à l'agresseur que votre adresse email est valide.
Dans les paramètres de sécurité de votre logiciel, interdisez l'exécution automatique des téléchargements, des plugins et d'ActiveX.

Pour aller plus loin :
Des mesures de prévention et un guide de paramétrage des logiciels de messagerie sont disponibles sur le site du CERT-FR (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques).

De nombreux conseils et fascicules sur la sécurité informatique personnelle et professionnelle sont disponibles sur le site de l'Agence Nationale de la Sécurité des Systèmes d'Information : www.ssi.gouv.fr