Cybercriminalité : sécurisez vos équipements numériques !

En à peine 20 ans nous sommes passés de l'ère du papier à celle du tout informatique. Corollaire de cette évolution, la cybercriminalité est apparue.
Vol de données, escroqueries financières, sabotages de sites, chantage... sont autant de nouveaux risques qui ont émergé de manière exponentielle.

Ainsi, début 2016 a vu l'émergence des rançonlogiciels, logiciels malveillants qui cryptent les données des ordinateurs infectés et les rendent donc inaccessibles pour les utilisateurs. L'objectif est pour les pirates d'obtenir une rançon, généralement payée en bitcoin (monnaie électronique) contre le déchiffrage des données. Toutes les entreprises sont concernées, la cybercriminalité n'est pas l'apanage des grandes entreprises. Les TPE PME sont même une cible de choix étant bien souvent moins sécurisées. A l'heure du virtuel, le risque est lui en revanche bien réel et à prendre très au sérieux. La prévention est essentielle et relève souvent de réflexes simples.
Vous trouverez ci-dessous quelques conseils extraits du « guide des bonnes pratiques de l'informatique » de la CGPME-ANSSI disponible sur le site du SEDIMA.

Mettez des mots de passe (complexe) sur vos équipements numériques

✔ Choisissez des mots de passe composés si possible de 12 caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux) n'ayant aucun lien avec vous (nom, date de naissance...) et ne figurant pas dans le dictionnaire ;

✔ 2 méthodes simples pour choisir vos mots de passe :

✔ La méthode phonétique :
« J'ai acheté 5 CDs pour cent euros cet après-midi » : ght5CDs%E7am ;

✔ La méthode des premières lettres :
« Allons enfants de la patrie, le jour de gloire est arrivé » : aE2lP,lJ2Géa!

Mettez à jour régulièrement vos logiciels

✔ Définissez et faites appliquer une politique de mises à jour régulières.

✔ Configurez vos logiciels pour que les mises à jour de sécurité s'installent automatiquement chaque fois que cela est possible. Sinon, téléchargez les correctifs de sécurité disponibles.

✔ Utilisez exclusivement les sites Internet officiels des éditeurs...

Effectuez des sauvegardes régulières

Pour sauvegarder vos données, vous pouvez utiliser des supports externes tels qu'un disque dur externe réservé exclusivement à cet usage. Vous le rangerez ensuite dans un lieu éloigné de votre ordinateur, de préférence à l'extérieur de l'entreprise pour éviter que la destruction des données d'origine ne s'accompagne de la destruction de la copie de sauvegarde en cas d'incendie ou d'inondation...
Avant d'effectuer des sauvegardes sur des plateformes sur Internet (souvent appelées « cloud » ou « informatique en nuage »), soyez conscient que ces sites de stockage peuvent être la cible d'attaques informatiques et que ces solutions impliquent des risques spécifiques.

Soyez prudent avec votre smartphone ou tablette

✔ N'installez que les applications nécessaires et vérifiez à quelles données elles peuvent avoir accès avant de les télécharger (informations géographiques, contacts, appels téléphoniques...). Certaines applications demandent l'accès à des données qui ne sont pas nécessaires à leur fonctionnement, il faut éviter de les installer.

✔ En plus du code PIN qui protège votre carte téléphonique, utilisez un schéma ou un mot de passe pour sécuriser l'accès à votre terminal et le configurer pour qu'il se verrouille automatiquement.

✔ Effectuez des sauvegardes régulières de vos contenus sur un support externe pour pouvoir les conserver en cas de restauration de votre appareil dans son état initial.

✔ Ne préenregistrez pas vos mots de passe.

Soyez prudent lors de l'utilisation de votre messagerie

Lorsque vous recevez des courriels, prenez les précautions suivantes :

✔ L'identité d'un expéditeur n'étant en rien garantie : vérifiez la cohérence entre l'expéditeur présumé et le contenu du message et vérifier son identité. En cas de doute, ne pas hésiter à contacter directement l'émetteur du mail.

✔ N'ouvrez pas les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoient habituellement vos contacts.

✔ Ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles (ex : code confidentiel et numéro de votre carte bancaire). En effet, des courriels circulent aux couleurs d'institutions comme les Impôts pour récupérer vos données. Il s'agit d'attaques par hameçonnage ou « phishing ».

✔ N'ouvrez pas et ne relayez pas de messages de types chaînes de lettre, appels à la solidarité, alertes virales, etc.

✔ Désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus avant de les ouvrir afin de vérifier qu'ils ne contiennent aucune charge virale connue.

Soyez vigilant lors d'un paiement sur Internet

Avant d'effectuer un paiement en ligne, il est nécessaire de procéder à des vérifications sur le site Internet :

✔ Contrôlez la présence d'un cadenas dans la barre d'adresse ou en bas à droite de la fenêtre de votre navigateur Internet (ce cadenas n'est pas visible sur tous les navigateurs).

✔ Assurez-vous que la mention « https:// » apparait au début de l'adresse du site Internet.

✔ Vérifiez l'exactitude de l'adresse du site Internet en prenant garde aux fautes d'orthographe par exemple.

68 %

des entreprises françaises ont été victimes de fraudes au cours des 24 derniers mois du fait de l'explosion de la cybercriminalité

Source : 8ème édition de l'étude PWC sur la fraude en entreprise, 7 mars 2016