CIRCULAIRE – entrepreneurs

Protégez les données de votre entreprise

2021-02-26

Quelles règles de cybersécurité appliquer ?

Utilisez un équipement informatique efficace

La première étape pour vous protéger de cyberattaques est de vous doter d'un équipement informatique efficace et régulièrement mis à jour.

Nos conseils :

• Procédez aux mises à jour suggérées par les logiciels en respectant les conditions d'utilisation qui accompagnent la plupart des appareils.

• Utilisez le filtre contre l'hameçonnage du navigateur internet : la plupart des navigateurs existants proposent une fonctionnalité d'avertissement contre l'hameçonnage. Ces fonctions aident à maintenir votre vigilance.

• Utilisez un logiciel de filtre anti-pourriel ou les fonctionnalités de classement automatique en tant que spam de votre boite de réception même si ces filtrages ne sont pas exhaustifs, ils permettent de réduire le nombre de pourriels.

Dotez-vous d'une identité numérique fiable

Créez un nom de domaine fiable

Le nom de domaine constitue la base de l'identité numérique d'une entreprise. Il s'agit de la partie qui se trouve après le « @ » dans les courriels et celle située après « www. » dans les adresses de sites.

Notre conseil :

Si vous choisissez d'utiliser un domaine se terminant par « .fr » vous pourrez bénéficier des services de l'Association française pour le nommage Internet en coopération (AFNIC).

Choisissez une messagerie sécurisée

Le courriel est dans une entreprise l'un des moyens de communication les plus utilisés. Il fait aussi régulièrement l'objet de cyberattaques, notamment en matière d'usurpation d'identité ou de fraude.

Pour vous en prémunir, assurez-vous que le fournisseur d'accès choisi soit à jour sur les standards de sécurité actuels.

Luttez contre les spams

Le spam, courriel indésirable ou pourriel, est une communication électronique non sollicitée. Cela va de l'abus marketing à l'hameçonnage, qui consiste à travestir un courriel en message d'une banque, d'un site marchand déjà fréquenté ou de tout autre service, afin de récupérer les données personnelles du destinataire. Les spams peuvent donc représenter un réel danger pour votre entreprise.

«Si vous pensez avoir été victime d'une escroquerie ou d'une tentative d'escroquerie par phishing signalez-le sur signal-spam.fr.

Sécurisez votre site web

• Il est vivement recommandé de créer un site web disposant d'une sécurité « https ».

• Par ailleurs, pour assurer une sécurité la plus optimale possible, il est nécessaire de faire une revue régulière des paramètres de sécurité de votre site web et de procéder aux mises à jour nécessaires.

Protégez les informations sensibles de votre entreprise

Les mesures de protection prises pour vos documents doivent être proportionnelles à la confidentialité et à la sensibilité des données contenues.

• **Marquez l'information selon son niveau de sensibilité** : pour évaluer les solutions nécessaires à la bonne protection de vos données, il est important de leur imposer un marquage. Ce marquage découle d'une analyse de risque qui doit permettre de protéger vos documents les plus importants.

• **Verrouillez l'accès à des documents confidentiels** : plusieurs logiciels de traitement de texte offrent une possibilité de sécurisation par code. La création de ce code permet de limiter l'accès aux documents sensibles aux personnes habilitées dans votre entreprise et vous donnera un premier niveau de protection face aux attaques extérieures. Si vous souhaitez mettre en place des solutions plus sûres pour vos données stratégiques, il est également possible d'avoir recours à des solutions de chiffrement ou à des accès via une carte à puce dotée d'un certificat numérique. De manière générale, nous vous conseillons d'établir un système de sécurité clair et régulièrement évalué.

• **Effectuez des sauvegardes régulières** : pour vous protéger d'incidents matériels, d'erreurs de manipulation de données ou d'attaques, il est vivement recommandé de mettre en place un plan de sauvegarde de vos informations.

Sensibilisez vos salariés à la cybersécurité

Rappelez à vos salariés les précautions d'usage contre les différentes méthodes de piratage

De nombreuses méthodes de piratage des données existent et représentent une menace pour votre entreprise. Au-delà des outils à mettre en place, en tant que chef d'entreprise vous pouvez vous prémunir gratuitement contre beaucoup de ces menaces en ayant les bons réflexes, ainsi qu'en sensibilisant vos salariés.

• Rappelez à vos salariés de ne pas ouvrir les messages dont la provenance ou la forme est douteuse, il pourrait s'agir d'un rançongiciel

• Rappelez à vos salariés de se méfier des extensions de pièces jointes qui paraissent douteuses (exemples : .pif ; .com ; .bat ; .exe ; .vbs ; .lnk…), et qui peuvent contenir des codes malveillants.

• Rappelez la vigilance nécessaire concernant les liens URL sur lesquels chaque internaute est susceptible de cliquer. Une lettre ou un caractère en trop ou en moins peut conduire vers un tout autre site web. Il faut privilégier la saisie des URL directement sur la barre d'adresses ainsi que les liens commençant par « https ».

• Insistez sur l'importance de ne pas connecter une clé USB trouvée par hasard, elle est peut être piégée !

• Pour le chef d'entreprise ou les salariés ayant accès à des comptes administrateur, il est conseillé d'utiliser en priorité un compte utilisateur plutôt qu'administrateur. L'administrateur d'un ordinateur dispose d'un certain nombre de privilèges sur celui-ci, comme réaliser certaines actions ou accéder à certains fichiers cachés un ordinateur. Préférez donc - dans la mesure du possible - l'utilisation d'un compte utilisateur, notamment pour les tâches quotidiennes.

(Source : BERCY ENTREPRISE - Février 2021)