A+ A-

Entreprises : quelles règles de cybersécurité appliquer ?

Par **Bercy Infos < https://economie.gouv.fr/entreprises/bercy-infos-qui-sommes-nous>** , le 17/10/2022 - **Sécurité numérique**

Vous souhaitez protéger au mieux les données de votre entreprise ? Vos documents confidentiels ? Vous protéger des cyberattaques ? Découvrez nos conseils.

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) < https://www.afnic.fr/fr/>** .

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.

Notre conseil :

Pour vous en prémunir, assurez-vous que le fournisseur d'accès choisi est 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.

Nos conseils :

- Afin de vous prémunir efficacement contre cette menace potentielle, consultez notre article « **Comment lutter contre les spams ?** ».
- Si vous pensez avoir été victime d'une escroquerie ou d'une tentative d'escroquerie par **phishing** signalez-le sur **signal-spam.fr. < https://www.signal-spam.fr>**

Sécurisez votre site web

Notre conseil :

- 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.

Évaluez votre niveau de cybersécurité

Les services du **Haut fonctionnaire de défense et de sécurité du ministère de l'Économie et des finances** vous permettent de réaliser - gratuitement et en ligne - votre auto-diagnostics de cybersécurité afin de vérifier que vos protections ou celles de vos partenaires et fournisseurs sont bien en place.

Réalisez votre auto-diagnostic de cybersécurité < https://ssi.economie.gouv.fr/>

Protégez les informations sensibles de votre entreprise

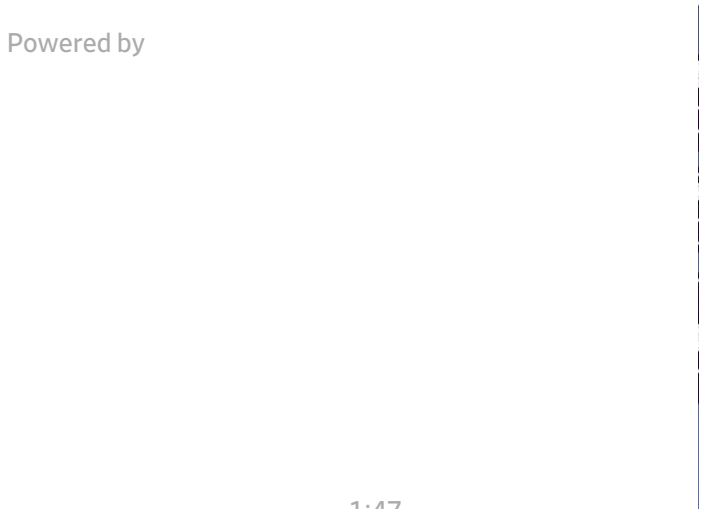
Les mesures de protection prises pour vos documents doivent être proportionnelles à la confidentialité et à la sensibilité des données contenues.

Nos conseils :

- **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 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.

Entreprises : suivez les conseils du HFDS !

Profitez des conseils du **Haut fonctionnaire de défense et de sécurité (HFDS) du ministère de l'Économie et des finances**.
Visionnez en vidéo les conseils concernant la sauvegarde de vos données : **< https://www.economie.gouv.fr/hfds>**



Visionnez également en vidéo les conseils relatifs à la **sécurité de votre**

navigateur < https://www.dailymotion.com/video/x7kvk9i> et à la sécurisation des mots de passe < https://www.dailymotion.com/video/x7lqui2> .

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.

Nos conseils (liste non exhaustive) :

- 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 peuvent 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 sur un ordinateur. Préférez donc - dans la mesure du possible - l'utilisation d'un compte utilisateur, notamment pour les tâches quotidiennes.

Prévoyez des formations pour vous et vos salariés

Si vous souhaitez aller plus loin, il peut être utile de vous former ainsi que vos salariés sur la cybersécurité.

Nos conseils :

- Consultez le kit de sensibilisation élaboré par le site cybermalveillance.gouv.fr < https://www.cybermalveillance.gouv.fr/> , afin de sensibiliser vos équipes aux questions de sécurité numérique tout en développant la formation personnelle de vos collaborateurs : téléchargez le kit de sensibilisation < https://www.cybermalveillance.gouv.fr/contenus-de-sensibilisation/> .
- Pour comprendre les enjeux de la sécurité numérique et se former à la protection des données, l'agence nationale de de la sécurité des systèmes d'information (ANSSI) < https://www.ssi.gouv.fr/> propose en ligne et gratuitement, un MOOC < https://secnumacademie.gouv.fr/> à destination à la fois des chefs d'entreprises, des salariés et des citoyens.

Désignez un RSSI

Afin d'organiser au mieux votre cybersécurité et dans la mesure de vos ressources, il peut être utile de désigner un responsable de la sécurité des systèmes d'information (RSSI).

Notre conseil :

En fonction de la taille de votre entreprise et du niveau de sensibilité des données traitées, il pourra également être pertinent de créer une équipe dédiée à la sécurité des systèmes d'information (SSI).

Sachez comment réagir en cas de cyberattaque

Si vous subissez un accident de cybersécurité, plusieurs solutions existent afin de réagir rapidement et efficacement.

Nos conseils :

- En cas d'acte ou de suspicion de cybermalveillance à votre encontre, contactez la plateforme cybermalveillance.gouv.fr < https://www.cybermalveillance.gouv.fr/> pour bénéficier d'un accompagnement spécialisé.
- Vous pouvez aussi signaler des contenus illicites sur le site du ministère de l'Intérieur : Pharos < https://www.internet-signalement.gouv.fr/PharosS1/> .

Ces contenus peuvent aussi vous intéresser

Cinq conseils pour se prémunir contre les « rançongiciels » (ransomware)

Sécurité de vos données : qu'est-ce que l'attaque par hameçonnage ciblé (spearphishing) ?

Sécurité de vos données : les méthodes de piratage les plus courantes

Cybersécurité : bénéficiez d'un accompagnement sur-mesure avec cybermalveillance.gouv.fr

En savoir plus sur la cybersécurité

Sur le portail du HFDS Bercy

Sur le site de l'AFNIC < https://www.afnic.fr/>

Sur le site de la CNIL < https://www.cnil.fr/>

Sur le portail gouvernemental contre la cybermalvaillance < https://www.cybermalveillance.gouv.fr/>

Fiches pratiques cybersécurité

Mémento cybersécurité pour le dirigeant d'entreprise (pdf -)

Mémento cybersécurité pour le créateur d'entreprise (pdf -)

Thématiques : **Sécurité numérique**

Ce sujet vous intéresse ? Chaque jeudi avec la lettre Bercy infos Entreprises, recevez les toutes les dernières actus fiscales, comptables RH et financières… utiles à la gestion de votre activité.

exemple : nom.prenom@domaine.com Je m'al

Je consens à ce que mon adresse email soit utilisée afin de recev
de Bercy infos. Consulter notre politique de confidentiali

Partager la page