Sécurité des données : les règles essentielles pour protéger les données et votre activité

19.6.2026 - | Commission Nationale de l'Informatique et des Libertés

Le numérique offre des opportunités pour développer votre entreprise, mais il s'accompagne aussi de risques concernant la sécurité des données que vous détenez, qu'elles soient personnelles (fichiers clients, employés…) ou non (informations financières, industrielles…). Il est donc impératif de sécuriser les outils que vous utilisez.

Les risques liés à l'usage du numérique concernent toutes les entreprises, indépendamment de leur taille et de leur secteur d'activité.

Quand on les interroge, les TPE/PME indiquent qu'elles manquent de moyens humains et matériels pour mettre en place des mesures de sécurité adéquates. La méconnaissance des obligations légales ou des interlocuteurs qu'il est possible de solliciter apparaît comme un obstacle supplémentaire.

Par ailleurs, si les attaquants sont très compétents et parfaitement équipés, ils privilégient souvent les attaques les plus faciles à réaliser.

C'est pourquoi la CNIL rappelle qu'il est important de commencer par **adopter les recommandations essentielles** ci-dessous : elles vont grandement réduire les risques, sans être onéreuses ou sans demander des connaissances techniques avancées.

Pour améliorer la cybersécurité de votre organisation, ces mesures peuvent ensuite être suivies d'un diagnostic adapté à votre activité qu'il est possible de demander, **gratuitement**, à partir du site MesServices.cyber.gouv.fr.

Recommandations essentielles de sécurité

1. Verrouillez vos accès avec des mots de passe solides

De nombreuses attaques réussissent grâce à des mots de passe trop simples, partagés ou réutilisés.

 Imposez à vos utilisateurs d'utiliser des mots de passe d'au moins 12 caractères mélangeant majuscules, minuscules, chiffres et caractères spéciaux. Testez-les sur le site de la CNIL ou vérifiez votre politique de mot de passe.

2. Adoptez un gestionnaire de mots de passe

Le gestionnaire de mots de passe est un outil qui permet de **générer et conserver de multiples mots de passe solides, uniques pour chaque compte** ou service.

 Utilisez un gestionnaire de mots de passe (par exemple KeePassXC, un outil gratuit et certifié par l'ANSSI) qui stockera vos codes d'accès de manière sécurisée.

3. Utilisez la double authentification

L’activation de la double authentification (également appelée « l'authentification multifacteur » ou « MFA ») permet de réduire le risque d'usurpation de compte dont l’identifiant et le mot de passe auraient été volés.

Dès que possible, activez-la, en particulier pour vos boîtes de courriels, vos comptes « administrateurs » et vos services en ligne. En plus de votre mot de passe solide, un code à usage unique reçu sur votre téléphone, par exemple, confirme que c'est bien vous qui vous connectez.

4. Soyez vigilant en utilisant la messagerie

Les **fraudes** passant par un courriel (via l’hameçonnage) sont **fréquentes et peuvent prendre des formes différentes**.

 Faites preuve de **prudence** vis-à-vis d’un message :

- qui invite à cliquer sur un lien ;
- qui invite à se reconnecter ;
- qui contient un caractère d’urgence inhabituel ;
- qui déroge aux procédures habituelles ;
- qui requiert un paiement ;
- qui demande un changement de coordonnées bancaires ;
- qui montre des incohérences lors du survol, avec la souris, sur les adresses courriels ou sur des liens hypertextes.

 En cas de doute, demandez **confirmation** à l’émetteur par un autre moyen (appel téléphonique sur le numéro habituel).

Cas typique : Le piratage de compte de messagerie

Le scénario : Camille reçoit un message avec un lien vers un document. À l’ouverture, une page l’invite à saisir son identifiant et son mot de passe.

L’objectif malveillant : le lien renvoie vers un site frauduleux, conçu pour voler les mots de passe.

Les bonnes pratiques : pour éviter cela, activez la double authentification. Ainsi, même avec votre mot de passe compromis, le pirate sera bloqué au moment de la 2nde vérification. Changez de mot de passe (désormais compromis) et ne l’utilisez plus jamais !

5. Installez des applications uniquement depuis les sites officiels

Des sites « non officiels » proposent **des versions gratuites d’applications payantes** qui sont conçues pour prendre le contrôle de vos outils, **à votre insu**.

 Installez des applications uniquement depuis les sites et magasins officiels des éditeurs (App Store, Google Play, etc.).

6. Automatisez les mises à jour de vos équipements (portables, tablettes, serveurs, logiciels, etc.)

Les pirates utilisent fréquemment des failles techniques (ou vulnérabilités) pour entrer dans vos applications informatiques. Lorsqu'elles sont connues, ces failles sont en général corrigées par des mises à jour des fournisseurs d'applications.

 Activez la mise à jour automatique sur tous vos appareils (ordinateurs, mobiles, tablettes, etc.) **pour bénéficier, sans tarder, des correctifs des éditeurs**.

7. Effectuez des sauvegardes, dont une « hors de la société », et faites des tests de restauration, régulièrement

En cas d'attaque par rançongiciel, de panne matérielle ou d'incendie, la **sauvegarde** est souvent le seul **moyen de récupérer vos données**.

 Appliquez la règle du **3-2-1** : **3** copies, sur **2** supports différents, dont **1** déconnectée du réseau (disque dur externe débranché du réseau, par exemple).

Cas typique : Le piratage du parcours de paiement d'un site marchand

Le scénario : Dominique a créé un site marchand, via un CMS (par exemple, PrestaShop, Magento, Wordpress, etc.). Un matin, l'accès au site n'est plus possible, ce qui ne permet plus de traiter correctement les commandes.

L'objectif malveillant : un tiers a changé le parcours de paiement afin d'obtenir les données de carte bancaires.

Les bonnes pratiques : activez la double authentification sur le compte administrateur. Privilégiez les modules des sites officiels. Veillez à effectuer la mise à jour des modules. Réalisez des sauvegardes régulièrement.

8. Installez des protections contre les intrusions (antivirus, pare-feu, etc.

Installées sur vos équipements (portables, tablettes, serveurs, logiciels, etc.), elles constituent une première ligne de défense efficace.

 Utilisez une solution antivirale professionnelle **pour détecter les programmes malveillants** (ou maliciels) et un pare-feu **pour bloquer des connexions potentiellement malveillantes**.

9. Protégez vos matériels mobiles (portables, disques externes, tablettes, etc.)

Les équipements mobiles peuvent être perdus ou volés. S'ils ne sont pas protégés, une personne tierce peut accéder à leur contenu.

 Utilisez un **code de verrouillage complexe** (évitez une date de naissance, le code par défaut, 0000, 1234, etc.)

 Assurez-vous de l'activation du chiffrement des données, dans les paramètres, pour les rendre illisibles en cas de vol ou de perte.

- Sur Windows :
  - Menu démarrer / Touche Windows
  - > Paramètres
  - > Chiffrement
  - > Sécurité des appareils
  - > Chiffrement BitLocker
- MacOS :
  - Menu Apple
  - > Réglages systèmes
  - > Confidentialité et sécurité
  - > FileVault
- Sur téléphone iOS ou Android, le chiffrement par défaut est activé dès que vous configurez un code d'accès, reconnaissance faciale ou d'empreinte digitale. Vous pouvez également chiffrer vos données sauvegardées ou synchronisées dans le nuage (cloud).

10. Séparez vos usages personnels des usages professionnels

Cette séparation réduit le **risque qu'un incident privé** (par exemple un proche qui installerait un jeu contenant un malware) **n'impacte la sécurité de votre entreprise**, et inversement !

 N'utilisez pas vos matériels ou vos comptes professionnels pour des besoins personnels ou familiaux.

Cas typique : La demande de rançon

Le scénario : Sam constate que le serveur de son entreprise ne contient plus aucun fichier, hormis un « lisez-moi.txt » qui demande le paiement d'une rançon pour récupérer les données.

L'objectif malveillant : Un attaquant monnaye le code qui permettra de récupérer les fichiers.

Les investigations concluront qu'un maliciel a été installé quand l'enfant de Sam a téléchargé un logiciel gratuit sur l'ordinateur de la société. L'attaquant a ainsi obtenu les mots de passe de l'entreprise, s'est connecté au serveur puis a chiffré son contenu.

Les bonnes pratiques : Ne payez pas ! Séparez les usages personnels des usages professionnels. Installez des protections contre les intrusions. Réalisez des sauvegardes régulièrement pour faire redémarrer votre activité.

11. Protégez les données, lors des déplacements

En déplacement, les **réseaux Wi-Fi publics** peuvent être **insuffisamment sécurisés** ou contrôlés par des tiers malveillants.

 Évitez de vous connecter à des réseaux Wi-Fi publics ou, une fois connecté, passez par votre réseau privé virtuel d’entreprise pour sécuriser l’accès à vos outils, par exemples.

12. Formez les collaborateurs et les dirigeants, à intervalles réguliers

L’humain est clé pour protéger votre organisme.

 Appuyez-vous sur les contenus gratuits tels que l’e-sensibilisation SensCyber ou le MOOC SecNumAcadémie, par exemple, pour les initier aux bonnes pratiques. Donnez des consignes claires sur la manière de signaler un doute ou une situation anormale.

Cas typique : Le cas du faux support technique

Le scénario : Morgan, responsable d’une agence, reçoit un appel pressant d'une personne se présentant comme un technicien informatique. L’expert affirme qu'une intervention immédiate sur son ordinateur est nécessaire et qu’il suffit de cliquer sur un lien pour corriger la situation.

L’objectif malveillant : L'escroc cherche à prendre le contrôle de votre machine à distance pour voler des données.

Les bonnes pratiques : Raccrochez ! Aucune société de maintenance sérieuse ne vous demandera votre mot de passe par téléphone ou ne vous incitera à installer un logiciel sous la pression. En cas de doute, rappelez vous-même votre interlocuteur habituel en utilisant son numéro de téléphone officiel.

Le réflexe RGPD

Le RGPD vous aide à réduire l'impact d'une éventuelle attaque grâce à deux principes clés :

- la minimisation par laquelle vous **ne collectez que les informations strictement nécessaires à votre objectif** (contrat, facturation, etc.). **Si une donnée n'est pas indispensable, ne la demandez pas**. Les données que vous ne possédez pas ne peuvent pas être volées.
- la limitation de la durée de conservation pour ne pas conserver les données indéfiniment. Elles ne doivent être gardées que le temps utile au service ou à la durée légale du contrat. **Une fois ce délai passé, supprimez-les ou anonymisez-les**. Des fichiers anciens ou oubliés sont des cibles inutiles et risquées en cas de vol ou d'intrusion.

De façon régulière (par exemple, une fois par semestre), faites le point sur ces deux principes.

Se faire accompagner

Réaliser un diagnostic sur le niveau de sécurisation de votre entreprise

Ces bonnes pratiques sont une première barrière et correspondent à des conseils généraux. **Elles doivent être complétées par des mesures additionnelles**, adaptées à chaque structure, qu’un professionnel peut vous aider à prioriser.

Demandez un diagnostic pour évaluer votre niveau sécurité, par exemple en déposant votre demande sur le site MesServices.cyber.gouv.fr. Il s'agit d'un premier état des lieux, **gratuit**, qui s'appuie sur l'état de la menace : 6 mois après ce diagnostic, un point est proposé pour suivre votre évolution.

Contacter un prestataire

Cybermalveillance.gouv.fr propose une mise en relation avec des prestataires informatiques de confiance labellisés « ExpertCyber » en capacité d'accompagner la sécurisation des systèmes informatiques des entreprises et collectivités : securisation.cybermalveillance.gouv.fr.

Réagir en cas de violation de données

Comment se préparer ?

Évaluez et anticipez au mieux les conséquences potentielles d'une violation de données, d'une attaque, par exemple en consultant les ressources SenCy-crise ou en rédigeant une procédure.

Comment réagir ?

Contactez votre support informatique ou **demandez de l'assistance** via le 17cyber.

Si des **données de personnes physiques** (employés, clients, etc.) sont concernées, informez la CNIL.

Dans le cas spécifique d'une d'attaque : isolez, préservez, déclarez !

Ne payez pas de rançon !

Débranchez le câble réseau ou coupez le Wi-Fi de la machine touchée.

N'éteignez pas l'appareil pour garder les preuves.

https://www.cnil.fr/fr/securite-des-donnees-les-regles-essentielles