CYBERSÉCURITÉ

Les bonnes pratiques informatiques

EXAUR
Cabinet d'Expertise Comptable

Que ce soit dans un cadre professionnel ou personnel, l'utilisation des outils numériques ne cesse de croître et de se diversifier. Cette intensification des usages représente pour les cybercriminels une opportunité de développer leurs attaques.

PRÉSENTATION PAR LE **CABINET EXAUR**

Comment se protéger au mieux face à ces risques ?

L'ESSENTIEL DES QUESTIONS À SE POSER

① Connaissez-vous votre parc informatique ?

Pour bien se protéger, il est important d'inventorier vos matériels et logiciels ainsi que les données et les traitements qui constituent votre patrimoine informationnel et contribuent à sa pérennité.

- **Inventorier tous les équipements et services** *(ordinateurs et leurs périphériques, mobile multifonction, tablette, serveur local, serveur distant (hébergement du site Web, service de messagerie, services logiciels en ligne, etc.), box, commutateurs, clés 4G, imprimantes etc.)*.
- **Inventorier les logiciels utilisés** *(nature, fonctions principales, versions, licences d'utilisation valides)*.
- **Inventorier les données et traitements de données** *(données & traitements susceptibles d'affecter ou d'interrompre l'activité en cas de perte ou d'altération ? Emplacement de stockage des données).*
- **Inventorier tous les accès** *(catégorie de l'accédant, moyen d'accès local ou à distance)*.
- **Inventorier les interconnexions avec l'extérieur** *(tout accès Internet vers un prestataire ou un partenaire doit être recensé)*.

② Effectuez-vous régulièrement des sauvegardes ?

Effectuer des sauvegardes régulières permet une restauration plus rapide des activités opérationnelles en cas d'incident, notamment en cas d'attaque par rançongiciel.

- **Identifier les données à sauvegarder** *(données "métier" et/ou "techniques" essentielles à la poursuite de votre activité)*.
- **Déterminer le rythme des sauvegardes** *(à définir en lien avec le volume de données numériques produites sur un temps donné)*.
- **Choisir le(s) support(s) à privilégier pour vos sauvegardes** *(physique ou cloud, attention toute sauvegarde doit faire l'objet d'un test pour vérifier son intégrité/viabilité lors d'une restauration)*.
- **Evaluer la pertinence du chiffrement de données** *(en cas d'accès illégitime au service cloud, les données restent protégées)*.
- **Respecter le cadre juridique** *(la RGPD s'applique quel que soit l'objectif du stockage de données : traitement ou sauvegarde)*.

EXAUR
Cabinet d'Expertise Comptable

CYBERSÉCURITÉ

Les bonnes pratiques informatiques

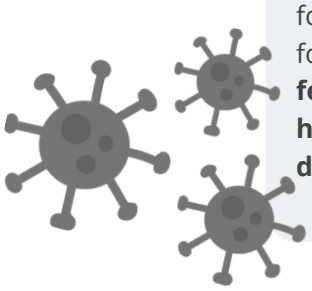
③ Appliquez-vous les mises à jour ?

Il est indispensable d'effectuer les mises à jour des systèmes d'exploitation et de tout logiciel dès la mise à disposition des correctifs de sécurité par leurs éditeurs.

- **Utiliser des solutions matérielles et logicielles maintenues** *(tout matériel ou logiciel qui ne peut plus être mis à jour doit être mis au rebut ou désinstallé)***.**
- **Activer la mise à jour automatique des logiciels et des matériels, et ceci dès la mise à disposition du correctif par les éditeurs.**
  - *Exiger cette pratique si vous faites appel à un prestataire extérieur !*

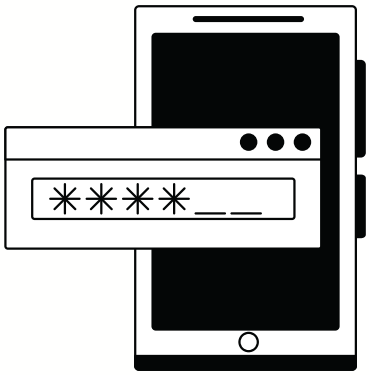
④ Utilisez-vous un antivirus ?

Un antivirus doit être déployé sur **tous les équipements, en priorité ceux connectés à Internet** *(postes de travail, serveurs de fichier, etc.)*.
Les antivirus commerciaux proposent une mise à jour automatique, et un scan automatique des espaces de stockage : **il est indispensable de procéder à l'activation de ces mécanismes dans les paramètres**.
Lors de l'achat d'un antivirus, il est intéressant, en fonction de vos usages, de souscrire aux fonctionnalités complémentaires tels qu'un **pare-feu**, un **filtrage Web**, un **VPN**, des outils **anti-hameçonnage** et de renforcement de la **sécurité des transactions bancaires**.



⑤ Avez-vous mis en place une politique de mots de passe robustes ?

De nombreuses attaques sur Internet sont facilitées par l'utilisation de mots de passe trop simples ou réutilisés d'un service à l'autre. Une attaque contre les mots de passe peut permettre une propagation de l'attaque au sein de l'entreprise ou à ses partenaires !
Découvrez toutes les bonnes pratiques liées aux mots de passe en **page 6** de ce document mais également sur le site web du cabinet Exaur :
https://www.exaur.fr/actualites/gestion-mots-de-passe

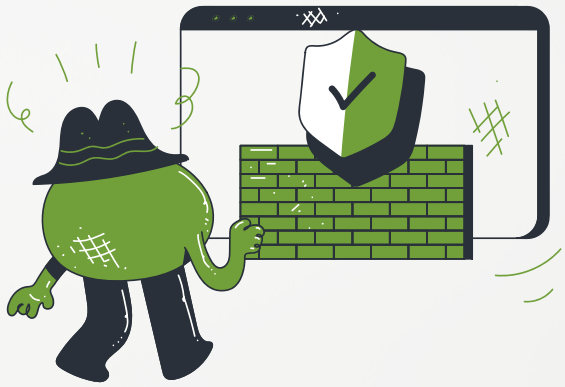


CYBERSÉCURITÉ

Les bonnes pratiques informatiques

⑥ Avez-vous activé un pare-feu ?

Un pare-feu protège principalement contre des attaques provenant d'Internet. Pour les entreprises disposant d'un système d'information, il permet aussi de **ralentir ou limiter l'action d'un acteur malveillant** ayant réussi à prendre le contrôle d'un des postes de travail.
Un pare-feu local *(intégré au système d'exploitation ou via une solution logicielle tierce)*, doit donc être installé sur tous les postes de travail. La configuration de l'ensemble du parc informatique et de sa politique de filtrage doit être homogène.
Des pare-feu physiques doivent être prioriser pour protéger l'interconnexion du SI à Internet, mais aussi pour **segmenter le réseau interne en zones ayant des niveaux différents de sensibilité et d'exposition aux menaces**.



⑦ Comment sécurisez-vous votre messagerie ?

La messagerie est **un des principaux vecteurs d'infection du poste de travail** *(ouverture de pièces jointes contenant un code malveillant, clic sur un lien frauduleux : phishing ou hameçonnage)*. En cas de doute, une vérification de l'authenticité du message par un autre canal est nécessaire. De plus, la redirection de messages professionnels vers une messagerie personnelle est à proscrire.
Que votre entité héberge ou fasse héberger son système de messagerie, vous devez vous assurer de :

- **Disposer d'un système d'analyse antivirus en amont des boîtes aux lettres des utilisateurs** *(pour prévenir la réception de fichiers infectés).*
- **L'activation du chiffrement TLS** des échanges entre serveurs de messagerie ainsi qu'entre les postes utilisateur et les serveurs hébergeant les boîtes de messagerie
- La mise en place de **mesures organisationnelles et structurelles** *(un serveur relai dédié à l'envoi et à la réception des messages doit être mis en place en coupure d'Internet et de ses possibles attaques).*

CYBERSÉCURITÉ

Les bonnes pratiques informatiques

⑧ Comment séparez-vous vos usages informatiques ?

Les risques liés à l'interconnexion de vos outils informatiques sont nombreux : exfiltration de données, usurpation d'identité, détournement du système informatique pour des usages frauduleux, etc. Pour diminuer ces risques, plusieurs principes doivent être appliqués :

- **Création de comptes utilisateurs dédiés à chaque employé** et ne disposant pas de privilège d'administration *(seuls ces comptes doivent être utilisés pour la navigation sur Internet).* **Ces comptes et droits doivent être tenus à jour** *(lors d'un départ : faire l'inventaire des accès du salarié et tous les révoquer, de telle sorte que lui-même ou un tiers ne puisse plus y accéder).*

L'idéal est de posséder un ordinateur uniquement dédié à sa pratique professionnelle *(en cas d'usages multiples, il est impératif de créer des comptes utilisateur pour chaque usage)*. De plus :

- **Les connexions entre les postes des utilisateurs doivent être interdites par défaut** *(ce cloisonnement évite la propagation)*.
- Les postes et comptes d'administration doivent être dédiés uniquement à cet usage.

⑨ Comment sensibiliser vos collaborateurs ?

Vous pouvez prendre connaissance de recommandations concernant les bonnes pratiques, d'alertes sur les menaces en cours et d'informations sur les mises à jour logicielles disponibles en suivant les actualités publiées par le dispositif **Cybermalveillance.gouv.fr**.

Une veille technique relative aux campagnes d'attaques et aux vulnérabilités est également effectuée par le **CERT-FR**.

Il est recommandé de mettre en place les bases d'une culture de l'hygiène informatique par une **information régulière de votre personnel aux bonnes pratiques de sécurité et aux principales menaces** *(notamment par le biais d'une charte informatique remise à chaque nouvel arrivant et détaillant les usages numériques à respecter et la procédure de déclaration d'un incident).*

CYBERSÉCURITÉ

Les bonnes pratiques informatiques

100 Comment réagir en cas de cyberattaque ?

En cas d'incident avéré concernant votre système d'information, **le premier réflexe est de déconnecter votre équipement ou SI d'entreprise d'Internet** (*action menée sur l'équipement réseau ou le pare-feu d'entreprise pour empêcher l'attaquant de piloter son attaque telle qu'un rançongiciel, et éviter une exfiltration éventuelle de vos données).*

N'éteignez pas ni ne modifiez les ordinateurs et matériels affectés par l'attaque : ils seront utiles aux enquêteurs.

En cas de rançongiciel, **ne payez jamais la rançon demandée** : **des solutions de déchiffrement existent** : vous serez assisté par les gardiens de la paix et vos sauvegardes vous permettront un retour "à la normale".

Les entreprises traitant des informations personnelles, relevant du RGPD son**t soumises au respect des exigences de ce texte. En cas d'incident, elles tenues d'informer la CNIL et leurs clients. Il est essentiel de porter plainte**.

CYBERSÉCURITÉ

Les bonnes pratiques informatiques

EXAUR
Cabinet d'Expertise Comptable

LES BONNES PRATIQUES À METTRE EN PLACE

① Mots de passe

Un **mot de passe robuste** :

- Sa **longueur est corrélée avec la criticité du service auquel il donne accès** *(un minimum de 9 caractères pour les services "peu critiques", dont la compromission ne donnerait accès à aucune information personnelle, financière)*.
- Comporte des capitales et des minuscules, des chiffres et des caractères spéciaux.
- Ne comporte aucun élément personnel.
- Il est possible d'avoir recours à une phrase de passe *(consiste à choisir aléatoirement un certain nombre de mots parmi un corpus déterminé)*.

La "bonne politique" à avoir :

- **Mots de passe différents pour chaque service nécessitant une authentification.**
- **Utilisation d'un coffre-fort de mots de passe** *(certifié par l'ANSSI)* peut vous aider à générer des mots de passe robustes et ne pas avoir à les mémoriser *(ou les conserver sur des fichiers trop facilement accessibles)*. Attention, ne préenregistrez pas vos mots de passe dans les navigateurs, notamment lors de l'utilisation ou de la connexion à un ordinateur public ou partagé.
- **Authentification multi-facteurs** à activer dès lors qu'elle est proposée par le fournisseur de service (+ *authentification par jeton physique pour simplifier l'accès aux terminaux de l'entreprise).*

② WIFI

- **N'utilisez jamais des réseaux de wifi publics** *(offerts dans les gares, aéroports ou hôtels)* pour des raisons de sécurité et de confidentialité.
- Privilégiez le partage de connexion avec votre smartphone professionnel ou attendez d'avoir un accès sécurisé à internet.

EXAUR
Cabinet d'Expertise Comptable

CYBERSÉCURITÉ

Les bonnes pratiques informatiques

③ En déplacement

- N'utilisez que du matériel fournis et/ou encadrés par le service informatique de votre entreprise.
- Travail pendant le trajet ? **Installez un filtre de confidentialité écran** !
- Apposez un signe distinctif sur vos appareils pour vous assurer qu'il n'y a pas eu d'échange pendant le transport.
- Gardez vos appareils, supports et fichiers avec vous, pendant votre voyage et séjour.
- Désactivez les fonctions Wi-Fi et Bluetooth de vos appareils.
- Retirez la carte SIM et la batterie si vous êtes contraint de vous séparer de votre téléphone.
- Informez votre entreprise en cas d'inspection ou de saisie de votre matériel par des autorités étrangères.
- Evitez de connecter vos équipements à des postes qui ne sont pas de confiance.
- Refusez la connexion d'équipements appartenant à des tiers à vos propres équipements.

Après le déplacement :

- Effacez l'historique des appels et de navigation.
- Changez les mots de passe utilisés.
- Faites analyser vos équipements.
- N'utilisez jamais les clés USB offertes lors de vos déplacements, susceptibles de contenir des programmes malveillants.

Mais aussi...

④ Antivirus

- **Ne désactivez en aucun cas logiciel de protection mis en place par votre entreprise.**
- **Ne bloquez pas les mises à jours planifiées poussées par votre service informatique.**

⑤ Smartphones et tablettes

- En plus du code PIN, u**tilisez un schéma ou un mot de passe pour sécuriser l'accès à votre terminal et configurez-le pour qu'il se verrouille automatiquement**.
- Ne préenregistrez pas vos mots de passe.

⑥ Téléchargements de logiciels

- **Téléchargez vos programmes sur les sites de leurs éditeurs.** Demandez l'autorisation préalable.
- Décocher ou désactiver toutes les cases proposant d'installer des logiciels complémentaires.

www.exaur.fr
Suivez-nous également sur :

EXAUR
Cabinet d'Expertise Comptable

CYBERSÉCURITÉ

Les bonnes pratiques informatiques

7 La messagerie

Les précautions suivantes sont essentielles lors de la réception d'emails :

- **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.
- Si des liens figurent dans un email, passez votre souris dessus avant de cliquer. L'adresse complète du site s'affichera dans la barre d'état du navigateur située en bas à gauche de la fenêtre. Vous pourrez ainsi en vérifier la cohérence.
- Ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles.
- N'ouvrez pas et ne relayez pas de messages de types chaînes de lettre, appels à la solidarité, alertes virales, etc.

8 Paiements en ligne

- Contrôlez la **présence d'un cadenas** dans la barre d'adresse ou en bas à droite de la fenêtre de votre navigateur Internet, et assurez-vous que la mention **« https:// »** apparait au début de l'adresse.
- Privilégiez la méthode impliquant l'envoi d'un code de confirmation par SMS.
- Rapprochez votre banque pour connaître et utiliser les moyens sécurisés qu'elle propose.

9 Identité numérique

Pour les formulaires : ne transmettez que les informations nécessaires, décochez les cases qui autorisent le site à conserver/partager vos données.

Sur les réseaux : Ne donnez accès qu'à un minimum d'informations perso/pro.

Enfin, **utilisez plusieurs adresses électroni**ques dédiées à vos différentes activités sur Internet *(une pro/une perso)*.