Garantissez la sécurité de vos postes de travail

Connecté en permanence à Internet, votre ordinateur peut être infecté à tout moment par un virus. Les risques ? Vol de données confidentielles, paralysie de toute l'activité, usurpation d'identité. Installer un antivirus et un pare-feu est indispensable.

Êtes-vous prêt à faire entrer chez vous un inconnu ? Tout le monde se pose cette question… sauf lorsqu'il s'agit d'Internet. En n'installant pas un **pare-feu** sur votre ordinateur, c'est comme si vous répondiez par « oui » à cette question.

Appelé aussi firewall en anglais, ce programme joue le même rôle que le physionomiste d'une discothèque interdisant l'accès aux personnes ayant un comportement agressif ou suspect.

Rapporté au réseau informatique, ce logiciel filtre les connexions entrantes (pour bloquer l'installation d'un programme malveillant) mais également sortantes (pour éviter des fuites de données par exemple).

Quant à l'antivirus, c'est la vigie de votre ordinateur. Il vérifie « l'identité » des logiciels et des fichiers que vous souhaitez installer ou ouvrir. Dès qu'il repère un code malveillant, il le met en quarantaine ou le supprime selon ses réglages.

Mais **« 90 % des PME n'ont aucun outil pour lutter contre la cybercriminalité »,** assure Michel Van Den Berghe, directeur général d'Orange Cyberdefense . Or, l'installation de ces deux outils de sécurité est indispensable. Sans eux, vous serez rapidement infectés par une pièce jointe cachant un virus comme les ransomware (ou rançongiciels) qui chiffrent toutes les données de votre réseau informatique. Selon une étude d'Avast, un éditeur d'antivirus, **20 000 ordinateurs sont infectés tous les mois en France par ce type de virus.**

Si aucune sauvegarde n'a été mise en place au préalable, la situation devient cauchemardesque : l'entreprise perd toutes ses données.

Autre menace : l'installation à votre insu d'un **keylogger.** Il s'agit d'un **logiciel espion enregistrant toutes les données que vous tapez** : mots de passe, identifiants, numéro de carte bancaire… Une fois récupérées, toutes ces informations sont revendues incognito sur le marché noir. D'où l'intérêt d'avoir un pare-feu filtrant ses flux sortants !

Des **symptômes pouvant indiquer la présence de codes malveillants** doivent vous alerter :

- ralentissement de l'ordinateur ou de la connexion ;
- ouvertures régulières de fenêtres de pop-up et de publicités ;
- surconsommation des ressources : réduction de l'espace libre sur le disque dur ou surcharge du processeur ;
- l'antivirus ou le pare-feu est désactivé sans votre intervention ;
- les mises à jour du système d'exploitation (Windows), de l'antivirus ou du pare-feu échouent constamment, etc.

La sécurité des postes de travail : les principales mesures à prendre

Le renforcement de ces droits accentue par conséquent les obligations de toutes les entreprises qui collectent, traitent et stockent des données personnelles.

Aujourd'hui, de nombreuses sociétés ne protègent pas assez leur réseau informatique, par manque de moyens ou de prise de conscience des risques numériques. Résultat, **onze incidents de cybersécurité seraient comptabilisés chaque jour en milieu professionnel en France,** d'après le cabinet de conseil PwC.

Face aux menaces numériques (phishing, infiltration sur le réseau informatique, virus…) pouvant entraîner une fuite de données - non seulement celles de vos clients, mais aussi celles de votre entreprise - vous devez renforcer votre niveau de sécurité.

Les mesures élémentaires à mettre en place

- **Première mesure : installer un antivirus et un pare-feu**
  L'installation de ces deux logiciels sur chacun de vos postes de travail renforce votre niveau de protection.
  Ne choisissez pas des solutions gratuites. Optez plutôt pour une suite payante regroupant notamment un antivirus, un pare-feu et un antispam. Proposés par le même éditeur, ces outils s'intègrent parfaitement et n'entraînent pas de bugs.

- **Seconde mesure : bien configurer vos antivirus, anti spam et pare-feu**
  Activez leur mise à jour automatique afin qu'ils intègrent les dernières variantes des programmes malveillants ou des adresses URL suspectes. Réglez également l'antivirus de façon à ce qu'il scanne tout le contenu d'une clé USB ou d'un disque dur externe dès qu'il est inséré dans un poste de travail. Ce logiciel doit aussi analyser toutes les pièces jointes avant leur ouverture.

- **Troisième mesure : faites des analyses complètes**
  Beaucoup plus longues qu'un scan rapide, les analyses complètes doivent être réalisées régulièrement, car elles traquent les virus dans les moindres recoins de vos disques durs. Cette analyse pouvant durer plusieurs heures, lancez-la le soir en laissant allumé votre PC (mais en verrouillant la session par un mot de passe !) pour éviter qu'une personne n'accède à vos fichiers.

- **Quatrième mesure : sécuriser votre PC**
  Utilisez un mot de passe « fort » comprenant au moins 8 caractères mêlant majuscules, minuscules et caractères spéciaux (évitez les noms, dates de naissance, et tout terme du dictionnaire) pour ouvrir votre session. Changez-le tous les six mois. Enfin, configurez Windows pour qu'il télécharge automatiquement ses mises à jour. Faites de même avec tous les logiciels installés sur chacun des postes de travail.

- **Cinquième mesure : faites référence à votre charte informatique**
  Précisez dans ce document les devoirs de vos salariés en matière de sécurité informatique : ne pas ouvrir d'email suspect, ne pas installer de version pirate de logiciels, ne communiquer ses identifiants à quiconque… Ces règles de base doivent être rappelées lors de sessions de sensibilisation.

Ce qu'il ne faut pas faire

- **Pré-enregistrer ses mots de passe dans les navigateurs**
  La facilité d'usage n'a jamais fait bon ménage avec la sécurité informatique. Configurer son navigateur Web pour qu'il enregistre tous vos identifiants et mots de passe est pratique pour ouvrir plus rapidement son compte sur un réseau social ou sa messagerie en ligne. Mais si un pirate accède à votre ordinateur, il peut récupérer toutes vos précieuses données.

- **Ne pas verrouiller sa session**
  Vous devez régler votre système d'exploitation de façon à ce que votre session soit verrouillée au bout de quelques minutes. Pour accéder de nouveau à vos fichiers, vous devrez retaper votre mot de passe. Cela évitera qu'une personne mal intentionnée puisse consulter vos documents en votre absence.

- **Utiliser un compte « administrateur »**
  Ce type de compte permet de tout faire sur un poste de travail et notamment d'installer ou de supprimer un programme. Seul le responsable informatique doit en posséder un. Tous les autres salariés doivent avoir un compte « utilisateur ».

Pour aller plus loin

Pour repérer les virus, ce logiciel applique deux principales méthodes :

- **il vérifie la « signature »** (en quelque sorte l'ADN) des programmes et des fichiers fonctionnant sur le PC. Si une signature correspond à celle d'un code malveillant, celui-ci est mis en quarantaine ou supprimé selon la configuration préalablement établie. La mise en quarantaine est conseillée, car les antivirus peuvent parfois afficher de fausses alertes en pointant du doigt un programme légitime ;

- **il étudie le comportement** des logiciels pour repérer des actions douteuses (tentatives d'ouverture en lecture/écriture de fichiers exécutables, écriture sur une partition...). Là aussi, il les bloque ou les supprime.

ANNEXE

Deux techniques simples pour choisir vos mots de passe :

- la méthode phonétique : « J'ai acheté 5 CD pour cent euros cet après-midi » : ght5CD%E7am ;
- la méthode des premières lettres : « 1 Chef d'Entreprise averti en vaut 2 » : 1Cd'Eaev2.

Pour vous accompagner dans la protection de vos postes de travail, découvrez l'offre Generali Protection Numérique

https://www.generali.fr/professionnel/assurance-cyber-risques/

SG2685MARK-25 - Décembre 2025 - Studio graphique