



## SÉCURITÉ - 8 RÈGLES DE BASE

Installer une suite de sécurité (Norton, Bitdefender, Kaspersky, Gdata, F.Secure...) reste le meilleur moyen pour protéger son ordinateur. Elles comprennent en général un antivirus, un antispam (spam = courrier non sollicité), un antispyware (spyware = logiciel espion), un antiphishing (phishing ou hameçonnage = duper l'utilisateur pour lui subtiliser certaines données personnelles), un pare-feu (firewall) et un contrôle parental.

Il existe de très bons antivirus gratuits (Avast, AVG, Antivir...) mais il faut les compléter avec un antispyware (Spybot S&D...) et un antispam (Spamihilator, K9...)

### 1. Supprimer les e-mails d'expéditeurs inconnus

Envoyés au hasard et en masse, ces messages peuvent véhiculer des virus : ne pas ouvrir les pièces jointes qui y sont parfois attachées, ne pas répondre ou cliquer sur les liens qu'ils peuvent contenir. Supprimer ces messages.

### 2. Installer les mises à jour de Windows

Cette opération permet d'installer les derniers correctifs de sécurité ; elle peut être automatisée (panneau de configuration puis « mises à jour Windows » ou « Windows update »)

### 3. Ne pas surfer depuis la session « administrateur »

La session administrateur (par défaut dans Windows) permet d'installer des programmes et autorise les paramétrages et modifications avancées du système. Pour ne pas exposer l'ordinateur, créer un compte utilisateur ou invité (accès restreint) et l'utiliser pour surfer.

### 4. Sauvegarder ses données sur des supports externes

Si l'ordinateur est gravement infecté et ne fonctionne plus, il faudra formater le disque dur (tout effacer). On pourra récupérer le système d'exploitation et les principaux logiciels, mais les données personnelles (textes, photos, musiques et vidéos) seront perdues : copier régulièrement ces données sur clé USB ou disque dur externe.

### 5. Bien choisir ses mots de passe

Changer de mot de passe pour chaque site sécurisé où l'on s'inscrit, les renouveler de temps en temps et ne pas hésiter à mélanger majuscules, minuscules, chiffres et caractères spéciaux (% , \$ , ? , § , ! , # , & ...)

### 6. Prudence lors des achats en ligne

Avant de taper le code de la carte bancaire, vérifier que l'adresse du site (barre d'adresse) a changé : « <http://www.nomdusite.fr> » se transforme en « <https://www.nomdusite.fr> » et un cadenas fermé doit apparaître.

### 7. Ne télécharger que des logiciels vraiment utiles

Il est très facile de télécharger des quantités de logiciels gratuits ; biens que généralement sains, certains peuvent contenir des programmes malveillants. Se méfier notamment des noms de fichier à double extension (ex: « superjeu.doc.exe »)

### 8. Sécuriser votre accès wi-fi

Si on utilise une connexion wi-fi, il faut absolument la sécuriser (autrement un utilisateur mal intentionné pourrait utiliser la connexion pour commettre des actes illicites). On préférera un cryptage WPA, plus sûr que le cryptage WEP.