Se protéger des cyberattaques (virus, vol de données, chantages….)

Avoir un système avec des défenses à jour

- Tenir à jour son ordinateur :
  - Le système d'exploitation (autoriser les mises à jour automatiques)
  - Tous vos logiciels et en particulier les logiciels de navigation sur Internet ou de consultation de courrier électronique
  - Les logiciels additionnels ou plugins et en particulier ceux qui permettent d'afficher des animations Java, Flash ou encore des fichiers PDF
- Installer un logiciel antivirus et le tenir à jour. Payant ou gratuit, l'antivirus doit permettre de contrôler : les activités en temps réel sur l'ordinateur, le système de messagerie et les activités autorisées par les navigateurs.

Prendre un minimum de précautions

Ne jamais insérer dans votre ordinateur **de supports extérieurs (**inconnus ou provenant d'un autre ordinateur) **sans contrôle antivirus**. Le contrôle doit devenir un acte naturel !

- Avoir des mots de passe et en changer régulièrement.
- Ne pas cliquer sur les liens provenant de sources inconnues (notamment des courriers électroniques non sollicités ou des messages sur les réseaux sociaux provenant de contacts inconnus ou ne correspondant à leur façon habituelle de s'adresser à vous). Il est de façon générale préférable, lorsque vous recevez un mail comportant un lien à cliquer, d'aller via votre navigateur sur le site directement. Les mails qui vous sont envoyés peuvent l'être par des hacker qui ont constitué à l'identique un faux sites (dans l'intention de récupérer des mots de passe, des numéros d'adhérents, des numéros de carte bleue…).
  Réaliser des sauvegardes de vos fichiers les plus importants (système, données, carnet d'adresses, favoris) : sur un disque dur amovible, sur des cédéroms ou à défaut sur des disques de partage sur Internet. Ce dernier moyen est peu recommandé dans le cas de service gratuit non sécurisé.
- Désactiver les fonctions de démarrage automatique (USB ou réseau) si elles ne sont pas indispensables dans votre environnement.

Ne pas « laisser les clefs sur la porte » et ne pas introduire d'intrus (cheval de Troie, spyware)

- Ne pas laisser les applications se souvenir de vos mots de passe (notamment les navigateurs) et utiliser un mot de passe un peu compliqué pour ce qui vous paraît important.
- Vider le cache du navigateur en fin de session (ce peut être automatisé).
- Il faut **éviter** à tout prix les **sources alternatives de diffusion** des systèmes d'exploitation ou des logiciels, plate-formes de téléchargement, logiciels commerciaux ou ceux qui sont diffusés sous des licences libres (dans le premier cas on ne travaille qu'avec les sites officiels, dans le dernier cas on recherchera des sites miroirs officiels ou de confiance).

Ne pas exposer sa porte aux attaques en permanence

- Arrêter son ordinateur régulièrement (une fois par jour – avez-vous vraiment besoin de maintenir votre ordinateur allumé la nuit ?) et relancer (ou arrêter quand c'est possible) la boite de raccordement à Internet (une fois par semaine).

Ne pas devenir une cible intéressante

- Ne pas laisser de fichiers sensibles sur l'ordinateur (numéros de compte, listes d'adresses, compilation de données, photos que vous ne souhaitez pas retrouver sur Internet…), préferez stocker ces fichiers sur un support amovible qui ne sera connecté qu'en cas de besoin.