La sécurité

en informatique

Les principaux dangers en informatique (à part les orages imprévus) sont les virus, les failles de sécurité, les logiciels espions qui détectent les mots de passe, le spam qui est un courrier non sollicité, etc. Ces cyber-attaques sont provoquées par l'appât du gain, la volonté de nuire, le vol d'informations confidentielles, l'usurpation d'identité.

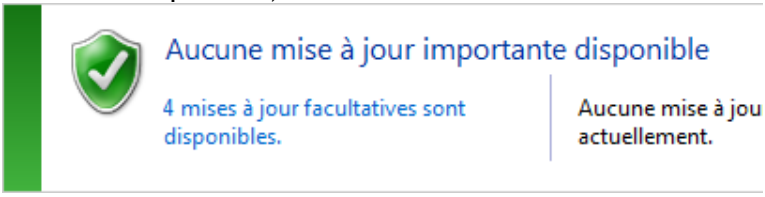
Les virus se servent de tous les moyens possibles pour rentrer dans l'ordinateur : Internet, les clés USB, les CD gravés, **mais surtout les erreurs de l'utilisateur** ! Il faut donc se protéger.

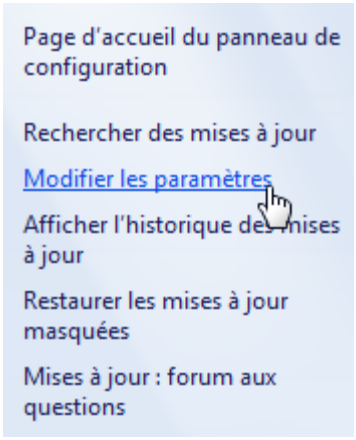
Les principales catégories de virus sont :

- **Les vers** : ils se répliquent sur un réseau informatique (dans une entreprise par exemple) et finissent par le saturer.
- **Les espions** (= *spywares*) : cachés au fond de l'ordinateur, ils ne font à priori pas de dégât mais ils envoient à leurs auteurs des informations personnelles, comme des numéros de carte de crédit.
- **Les chevaux de Troie** : sous l'apparence d'un programme valide, normal, il contient de quoi contourner les protections mises en place. Il permet donc des intrusions ou la propagation d'autres virus.
- **Les keyloggers :** ils enregistrent et transmettent à une personne extérieure ce qui est tapé au clavier, et permettent de récupérer les mots de passe, le numéro de comptes bancaires…

Pour se protéger, il faut essentiellement se préoccuper de l'anti-virus, des mises à jour, de ses mots de passe, et faire attention à ce que l'on installe et aux mails que l'on ouvre.

1. **Pour la sécurité logicielle, il faut :**
   - Un anti-virus à jour et des analyses régulières du disque dur (jamais 2 anti-virus !)
   - Des programmes à jour
   - Les mises à jour de Windows par Windows Update (passer par « Démarrer », « Tous les programmes », « Windows Update »)





Attention : s'assurer que les mises à jour sont automatiques. Pour cela, cliquez sur Modifier les paramètres, dans la partie gauche de Windows Update :

- Un pare feu pour se protéger contre les intrusions. Celui-ci est installé d'office avec Windows.
- Un anti-spyware à jour avec des analyses régulières

2. Les mots de passe :

Il est très important de savoir choisir plusieurs mots de passe dits forts, c'est-à-dire difficile à retrouver à l'aide d'outils automatisés, et difficile à deviner par une tierce personne. La force d'un mot de passe dépend de sa longueur et du mélange de minuscules, majuscules, chiffres et caractères spéciaux.

Ce type de mots de passe est très difficile à retenir. Il faut donc trouver des moyens mnémotechniques pour les fabriquer et s'en souvenir facilement. Un exemple de mot de passe phonétique :

ght3CD%E7am = « J'ai acheté 3 CD pour cent euros cet après-midi »

Règles générales :

- ✓ Avoir des mots de passe de 12 caractères minimum, si possible de 16 caractères.
- ✓ Utiliser des caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux).
- ✓ Ne pas utiliser de mot de passe ayant un lien avec soi (noms, dates de naissance).
- ✓ Le même mot de passe ne doit pas être utilisé pour des accès différents (banque, emails)
- ✓ Ne pas garder le mot de passe par défaut et changer de mot de passe régulièrement.
- ✓ En règle générale, ne pas configurer les logiciels pour qu'ils retiennent les mots de passe.
- ✓ Éviter de stocker ses mots de passe dans un fichier ou lieu proche de l'ordinateur si celui-ci est accessible par d'autres personnes.
- ✓ Si possible, limiter le nombre de tentatives d'accès.
- ✓ Ne jamais donner son mot de passe à quelqu'un.

3. La sécurité bancaire

- Pensez à vérifier le site (conditions générales de vente, garanties, frais de port)
- L'adresse de page doit commencer par « https » et un cadenas fermé doit apparaître (en bas de l'écran)
- Contacter sa banque pour avoir un numéro virtuel de carte ou un boîtier lecteur de carte : un numéro virtuel de carte bancaire à usage unique est communiqué en temps réel. Ce numéro change à chaque nouvel achat sur Internet.

4. Un peu de logique :

- Attention aux « hoax » ou fausses rumeurs (ex. : fichier à supprimer)
- Pas de mises à jour de l'anti-virus par email
- Attention aux alertes de sécurité et proposition d'installation (fenêtre qui s'ouvre)
- Attention aux demandes d'aide pour transferts de fonds

- Attention au blanchiment de capitaux sous couvert d'offre de travail
- Attention au phishing (= hameçonnage) : (ex. : humanitaire, banque)

En se présentant comme un tiers de confiance, le fraudeur peut obtenir des renseignements personnels (mot de passe, numéro de carte) dans le but de perpétrer une usurpation d'identité.

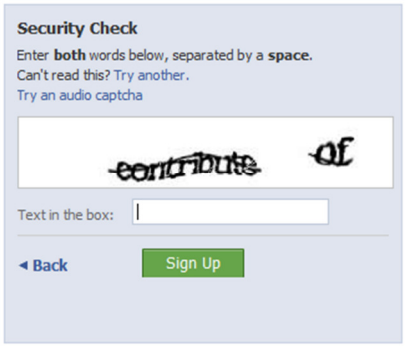
- Attention au vishing (équivalent du phishing, mais par téléphone)
- Ne pas installer tous les programmes possibles, juste ceux qui sont nécessaires
- Eviter les logiciels de peer to peer (= échange de fichiers de poste à poste)

5. Savoir utiliser l'Email

- Avoir plusieurs adresses, ne pas donner son l'adresse personnelle, changer l'adresse publique dès qu'elle est spammée
- Filtrer les adresses et / ou les contenus
- Ne pas répondre aux spams
- Refusez les « bons plans » des amis (adhésion sans votre accord)
- Si vous envoyez un message à plusieurs personnes, mettre les adresses en « Cci » pour que les adresses ne soient pas visibles (Cci = copie carbone invisible)
- Attention aux pièces jointes, surtout si le nom du document est machin-chose**.exe**
- Ne pas cliquer sur un lien dans un email, mais copier/coller l'adresse sur Internet, dans la barre d'adresse du navigateur.
- Conserver les messages d'enregistrement pour pouvoir se désabonner

Un bon email, c'est : UN OBJET, UN MESSAGE ET UNE SIGNATURE (pas juste une pièce jointe)

Remarque : Un **captcha** est une image (ou un son s'il s'agit d'un captcha audio) qui permet de différencier de manière automatisée un utilisateur humain d'un ordinateur. L'image contient des caractères déformés, théoriquement seul un humain est capable d'en extraire le contenu et de saisir les lettres sur son clavier, et donc seul un humain peut remplir les champs lors d'une inscription.



Pour aller plus loin : **www.droitdunet.fr** / **www.internetsanscrainte.fr/**

Pour plus d'informations :

Le planning des sessions de cours est en ligne à l'adresse :

http://mediatheque.capdegascogne.fr/Mediatheque/Informatique/Initiations

Pour plus de renseignements, contacter l'animatrice à la Médiathèque :

- par téléphone : **05 58 76 09 69**
- par mail : atelier.informatique@capdegascogne.fr

en vous présentant à l'atelier informatique durant les heures d'ouverture au public.