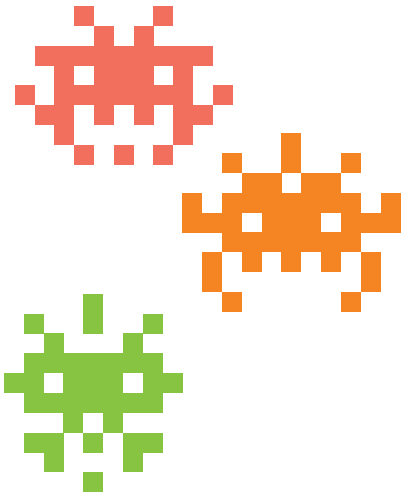
Le monde numérique offre plein d'avantages mais il comporte aussi des risques : entre les fraudes, les arnaques par e-mails, les faux profils qui se font passer pour des proches et les logiciels malveillants, il est légitime de s'inquiéter. Comment se protéger au mieux des pirates du web ?

1. Les logiciels malveillants ou malwares

Les logiciels malveillants sont des logiciels conçus à des fins de piratage informatique.
Il en existe de différentes sortes en fonction de l'objectif visé :



- **Le virus** est un logiciel qui se réplique de lui-même, comme un virus humain. Il se diffuse, entre autres, via les pièces jointes des mails.
- **Le ransomware/rançongiciel** prend les données en otage. Il bloque l'accès aux fichiers contenus sur l'appareil et le paiement d'une rançon est exigé pour y avoir à nouveau accès. Les grandes sociétés et les citoyens peuvent être visés par cette menace.
- **Le spyware** ou logiciel espion va s'immiscer dans la machine afin de récolter des informations, espionner. Il est très discret, restant généralement caché le temps de récolter les données recherchées.
- **Le Trojan ou cheval de Troie** est quant à lui un logiciel malveillant qui se présente comme légitime à l'utilisateur·trice : après téléchargement, il agira en arrière-plan afin de tirer profit des ressources et données de la machine.

Face à autant de menaces, il apparait qu'utiliser le numérique n'est pas sans danger. Vigilance et bons réflexes sont donc importants, tout comme un nettoyage régulier de vos appareils.
Et évitez les sites de téléchargement illégaux. Ils sont truffés de logiciels malveillants.

2. Les pratiques malveillantes

Aujourd'hui, il existe des logiciels très performants, qui peuvent bloquer la plupart des logiciels malveillants. Mais il y a toujours un point faible dans la sécurité informatique : **l'humain**.

Le social engineering, ou **l'ingénierie sociale**, consiste à manipuler une personne pour qu'elle télécharge un logiciel malveillant ou dévoile ses données. Les cybercriminels utilisent l'appât du gain, la peur ou la confiance des victimes pour parvenir à leurs fins. Ils utilisent différents canaux et exploitent les informations qu'ils trouvent en ligne, notamment sur les réseaux sociaux :

- En se faisant passer pour un proche malade/dans le besoin
- En créant un lien et en faisant preuve d'empathie avec la victime

- **Le hameçonnage/phishing** consiste à envoyer des e-mails dans le but de soutirer des informations personnelles comme le mot de passe ou les données bancaires.
  La variante **par SMS** s'appelle **le vishing**.
- **Le spoofing** est une technique de fraude qui consiste à se faire passer pour un organisme ou personne de confiance (comme la banque ou un proche) pour pousser à dévoiler ses données. Par exemple, avec un faux e-mail de la banque pour connaitre vos données bancaires.
- **Le piratage de compte** est l'accès non autorisé à un compte en ligne (boite mails, réseaux sociaux...) suite au vol des identifiants de connexion.
- Et toutes les autres formes d'arnaques qui visent à voler des données et/ou de l'argent.

Conseils sécurité avec les e-mails

- Supprimez les mails suspects sans les ouvrir
- Vérifiez l'adresse e-mail de l'expéditeur
- Ne cliquez pas sur le lien depuis un e-mail. Rendez-vous directement sur le site (voir fiche 3.2.)
- Vérifiez les pièces jointes

Vigilance avec les e-mails

Les spams, **pourriels**, ou **courriers indésirables** peuvent contenir une pièce jointe avec un virus ou un lien menant vers un faux site ressemblant à un site de confiance. Méfiez-vous aussi :

- des messages qui affirment que vous avez droit à un remboursement ou une prime avec une apparence officielle, encore plus selon l'actualité (crise énergétique etc).
- des demandes d'argent, des appels à l'aide larmoyants de personnes coincées à l'étranger ou de gains à des concours auxquels vous n'avez pas joué... (voir aussi fiche 3.4.et 4.4.).

Les techniques des cybercriminels pour tromper sont nombreuses et la vigilance est de mise.

3. Le net n'est pas sécurisé alors ?

Si l'idée de risquer de se faire arnaquer ou de cliquer sur le mauvais lien peut être inquiétante, rappelez-vous que le vol de données ou d'argent et les arnaques existaient avant le numérique.
Prudence, bon sens, protection de vos appareils et données sont vos meilleurs alliés pour limiter les risques.

Il existe différentes ressources pour s'entrainer à se protéger en ligne comme :

- Le site Cybersimple.be qui reprend de nombreux conseils pour se protéger en ligne
- Space Shelter, un jeu interactif sur la sécurité en ligne https://spaceshelter.withgoogle.com
- Le site https://safeonweb.be

CYBERSIMPLE.be

Safeonweb.be
Indice de Santé digitale

SPACE SHELTER

interface3 namur
www.interface3namur.be/box-numerique

Projet réalisé avec le soutien du Fonds "ING Fund for a more Digital Society", géré par la Fondation Roi Baudouin