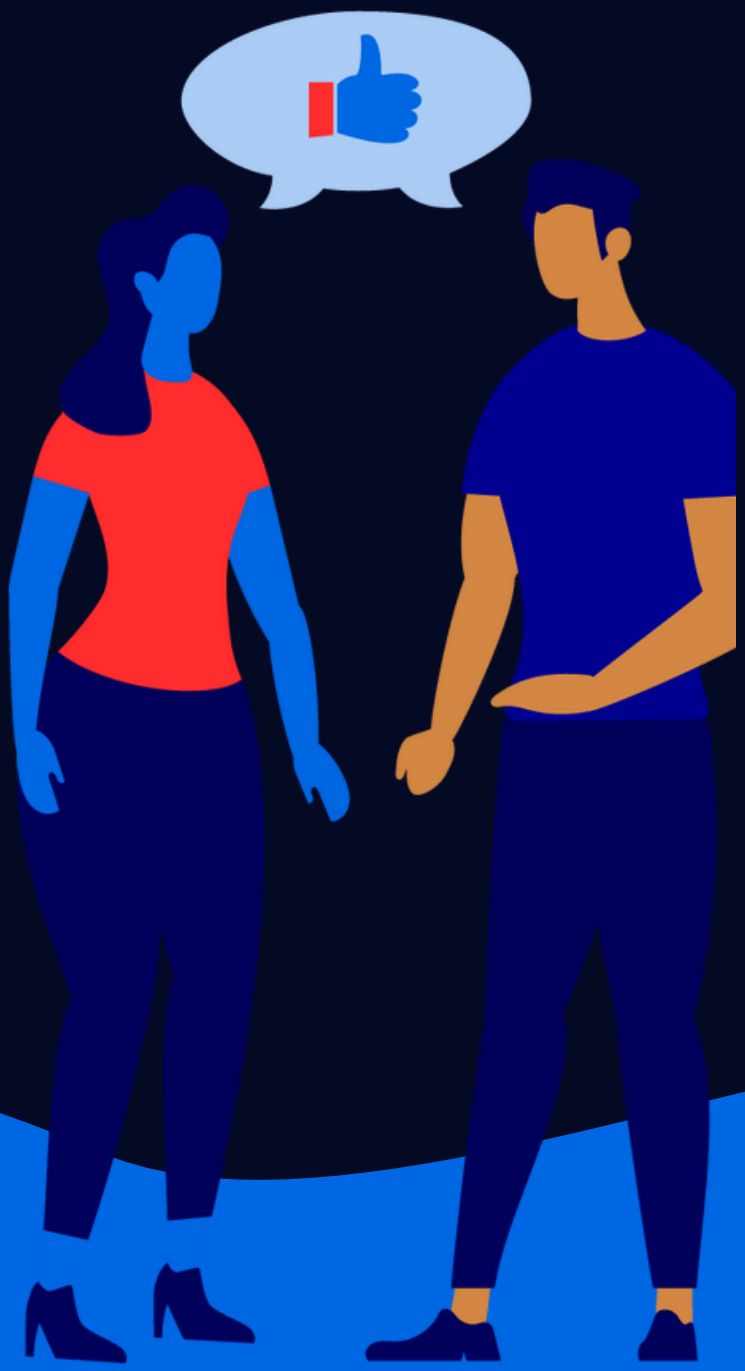
10 CONSEILS POUR RESTER EN CYBER-SÉCURITÉ



Crédit : Fabien Devilliers

43% DES FRANÇAIS ONT DÉJÀ ÉTÉ PIRATÉS OU TOUCHÉS PAR UNE ARNAQUE EN LIGNE

Sources : Odoxa 2020

Les **escroqueries** en ligne font parties des risques liés à l'usage du numérique. Elles sont utilisées par des **individus isolés ou en groupe** qui poursuivent **différents objectifs** : atteinte à la réputation, appât du gain, espionnage, sabotage, revendications politiques....

Afin de nous piéger, ils utilisent notre **manque de vigilance**, des **faux sites** web ou des **fausses identités**, mais également des **logiciels malveillants** (malware) : virus, vers, logiciels de rançon ou de publicité dissimulés dans des clés USB, des liens hypertextes, ou encore des pièces-jointes à un courriel.

Voici 10 conseils pour rester en "cyber-sécurité".

FAIRE PREUVE DE VIGILANCE

Tous les antivirus du monde ne serviront à rien si je ne prends pas le temps de lire avant de cliquer, de partager une publication ou si je me mets délibérément dans une situation à risque : streaming ou téléchargement illégal par exemple.

AVOIR DES "BONS" MOTS DE PASSE

Longs et complexes*, uniques et confidentiels.

*Pour ne pas oublier mes mots de passe, je peux utiliser un gestionnaire de mots de passe comme Bitwarden, Dashlane ou Keepass.

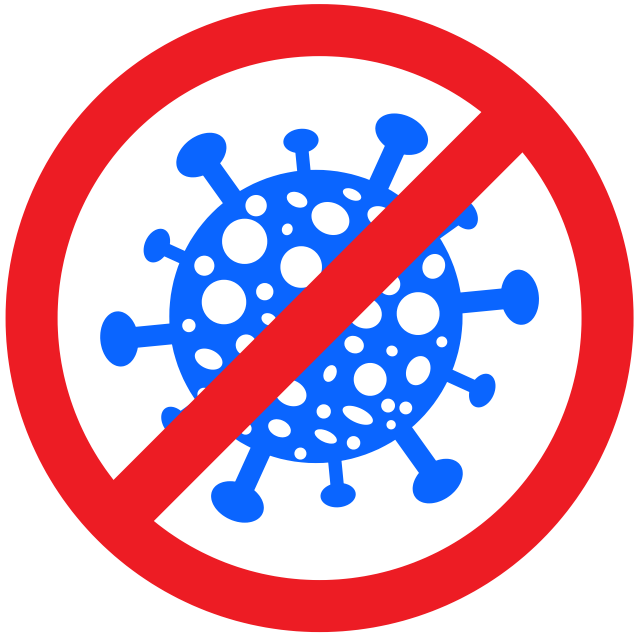
UTILISER LA DOUBLE AUTHENTIFICATION

Elle s'active depuis les paramètres de sécurité de mon compte utilisateur et permet de vérifier par deux systèmes d'authentification différents qu'il s'agit bien de moi.
Souvent : un mot de passe "classique" et un mot de passe temporaire envoyer sur mon smartphone.

*Free OTP est une application pour smartphone qui permet de générer des mots de passe temporaires.

ACTIVER L'ANTIVIRUS

L'antivirus permet d'être protégé contre les logiciels malveillants (malware), à condition d'être à jour.
Avoir plusieurs antivirus sur le même équipement ne me protège pas plus et peut entrainer des dysfonctionnements.



Gratuits ou payants ? Le mieux c'est de comparer les différents services et tarifs proposés dans les enquêtes de consommateurs et sites web spécialisés (UFC que choisir, 60 millions de consommateur, BDM, Numerama, Next INpact...).

FAIRE LES MISES À JOUR

En principe, elles sont automatiques* à condition que mon équipement soit allumé et connecté à Internet.
Attention aux vieux équipements sur lesquels les mises à jour ne sont plus disponibles.

*Certaines personnes préfèrent désactiver les mises à jour automatiques pour garder le contrôle. En effet, certaines mises à jour peuvent parfois entraîner des dysfonctionnements. Cela demande de prendre le temps de s'informer sur chaque mises à jour.

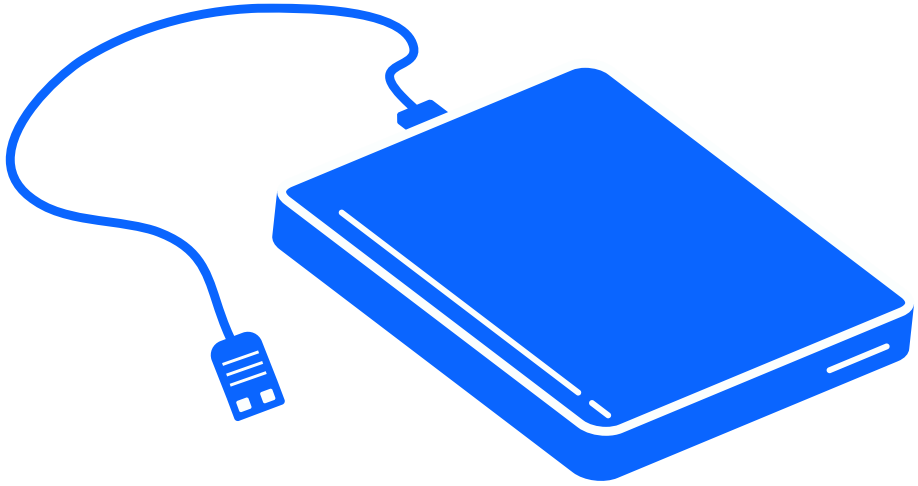
FAIRE ATTENTION AUX RÉSEAUX WIFI

En particulier les réseaux wifi publics ou portails captifs accessibles dans les hôtels, restaurants, trains... qui ne sont pas toujours très sécurisés.
Je peux privilégier les données mobiles pour mieux protéger ma vie privée.

*Dans la plupart des cas, mon contrat avec mon Fournisseur d'Accès à Internet (FAI) m'interdit de louer ma connexion internet à des personnes extérieures à mon "foyer" : locataires ou voisins par exemple.
Pour protéger ma box, je dois avoir une clé de sécurité très longue et je peux également masquer mon réseau.

FAIRE DES SAUVEGARDES

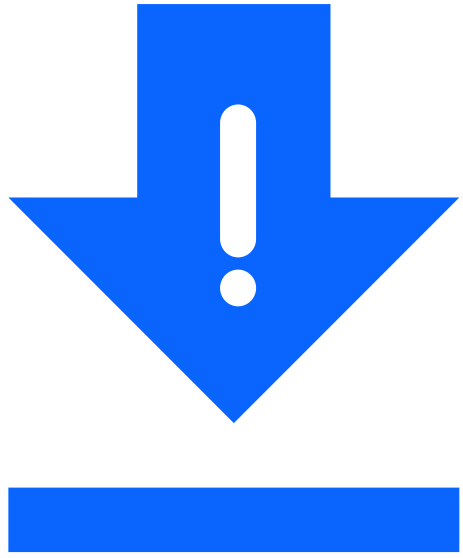
Pour éviter de me faire voler mes dossiers et fichiers ou de les perdre à cause d'une panne, je peux les stocker et faire des copies sur des supports de stockage externes, notamment un disque dur, une clé USB, un CD*.



*Chaque supports de stockage a des avantages et des inconvénients. Je peux également faire des sauvegardes sur un service de stockage en ligne : cloud pour avoir accès à mes données depuis n'importe quel équipement connecté à Internet. Mais cela augmente les émissions de GES et je perds en partie le contrôle de mes données.

TÉLÉCHARGER AVEC VIGILANCE

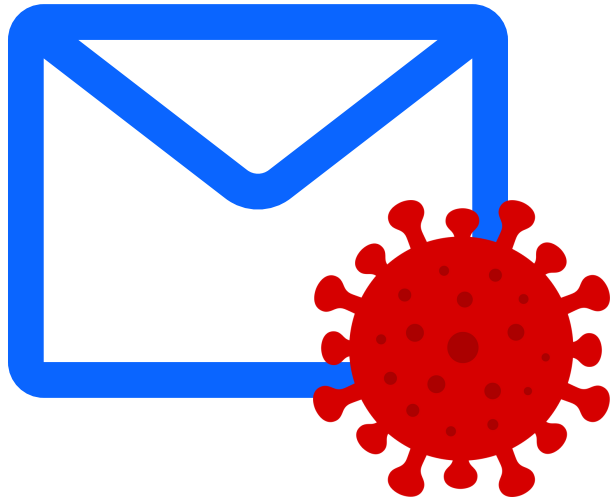
Pour télécharger un logiciel ou une application il est préférable de passer par des magasins d'applications (store) : play store ou App store par exemple et des sites spécialisés : O1net, Clubic, framalibre...



*Avant de d'installer un logiciel ou une application, je peux regarder qui est l'éditeur, la note, les avis ou encore le nombre de téléchargement pour limiter le risque d'arnaque.
Egalement, je dois me méfier des applications qui demandent de nombreuses autorisations : contact, galerie, journal d'appel, appareil photo, localisation...
Enfin, décocher ou cocher les petites cases qui autorisent l'installation de programmes complémentaires.

FAIRE ATTENTION AUX COURRIELS

Ils peuvent contenir : des liens qui me redirigent vers des faux sites web, des messages rédigés pour me faire paniquer ou m'émouvoir ou encore des pièces-jointes contenant des virus.
Si j'ai le moindre doute sur l'identité de mon interlocuteur, la corbeille est la solution.



Le courrier postal est toujours utilisé pour les documents les plus importants. Si je dois envoyer des documents importants, d'identités par exemple, par courriel, je privilégie une photocopie portant la mention : "usage réservé à XXXXX" et la date.

SURVEILLER SON E-RÉPUTATION

Afin de contrôler mon e-réputation je peux demander à mon FAI d'être en liste rouge. Je peux régler les paramètres de confidentialité, utiliser un pseudonyme, supprimer les identifications sur les photos et surtout vérifier régulièrement les "traces" de mon identité sur le web*.

*Grâce à une recherche de mon nom et prénom avec un moteur de recherche ou en utilisant un site web comme "webmii" ou "haveIbeenpwned".

ET SI JE SUIS PIRATÉ ?

- Rester calme
- Rassembler les preuves
- Prévenir ma banque et mes proches
- Bloquer mes données à distance
- Contacter un.e expert.e cybersécurité
- Déposer plainte

PRÊT.E À VOUS DÉFENDRE?

POUR ALLER PLUS LOIN :

- @cybergend
- www.cybermalveillance.gouv.fr
- www.numerama.com/cyberguerre/
- Sébastien Dupont, Vous êtes fous d'aller sur Internet ! Flammarion, 2019.
- Olivier Bogaert, Internet – évitez les arnaques et le harcèlement, Racine, 2021.

@NUMERIQUE_ET_MOI