LIVRET D'INFORMATION

Numérique : risques et bonnes pratiques

2021 - 2022

jeunes-bfc.fr

info Jeunes Bourgogne-Franche-Comté

EXPLORER LES POSSIBLES

Numérique : risques et bonnes pratiques

Le numérique englobe l'informatique, le téléphone, l'ordinateur et Internet. Aujourd'hui les pratiques sont telles qu'il est difficile d'imaginer se passer, entre autres, de son smartphone ou des réseaux sociaux. Mais la pratique numérique n'est pas sans risque : arnaques, piratages, publications malveillantes, fausses informations… Il est donc essentiel de savoir comment faire pour protéger ses données, sa vie privée, son image.

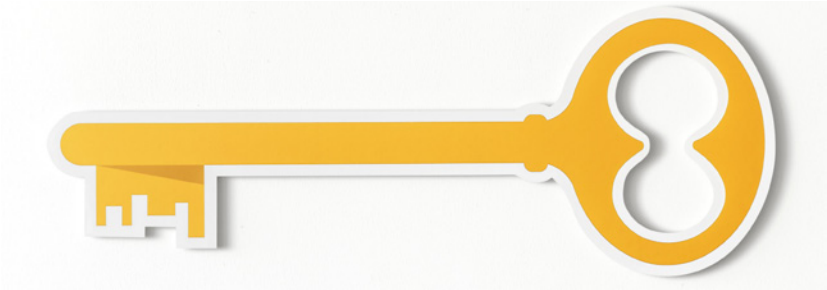
> Règles de base p3
> Piratage p5
> Fausses informations p7
> Agir face à la cybermalveillance p10
> Pour aller plus loin p12

Règles de base

Il est indispensable d'être attentif à quelques points de vigilance incontournables.

Les mots de passe

Veillez à ce que vos mots de passe soient composés d'au moins **10/12 signes** mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux, ne les communiquez jamais, changez-les régulièrement et utilisez un mot de passe différent pour chaque service.
Plus d'infos :
cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe



Les données personnelles

Toute **information** se rapportant à une **personne physique** est une donnée personnelle. **L'identification** d'une personne physique peut être **directe** (par exemple par ses nom et prénom) ou **indirecte** (par un numéro de téléphone, un numéro de sécurité sociale, une adresse postale ou mail…) et **réalisée** à partir d'une **seule donnée** ou à partir du **croisement d'un ensemble de données.**
Vos données vous appartiennent et vous définissent, il faut donc en conserver la **maîtrise**, être **vigilant** et ne pas les partager trop facilement afin de ne pas prendre le risque de donner accès à votre numéro de carte bancaire, à votre numéro de téléphone, aux messages échangés avec vos amis, etc.
Les outils numériques sont devenus incontournables, mais n'oubliez pas que lorsque vous vous connectez ou que vous créez un compte, et que vous acceptez des **conditions d'utilisation**, cela signifie que vous donnez accès à vos données personnelles ou même que vous les cédez.
Pour limiter le nombre d'informations personnelles que vous mettez en ligne, la **Cnil** propose des **tutoriels** permettant de bien configurer vos terminaux et comptes sociaux.
Plus d'infos :
cnil.fr/fr/configurer-ses-outils

Les photos ou vidéos

Le **droit à l'image** permet de faire respecter le **droit** à la **vie privée** ; il est donc nécessaire d'avoir un **accord écrit** d'une personne pour utiliser son image (photo ou vidéo) sur un site internet ou un réseau social... De fait si, **sans son accord**, une personne a été photographiée ou filmée dans un lieu privé, ou si cette photographie ou ce film est publié et que cela porte atteinte à sa vie privée, elle peut **porter plainte**.
Plus d'infos : service-public.fr/particuliers/vosdroits/F32103
Par ailleurs, n'oubliez pas que les photos ou vidéos que vous diffusez peuvent, dans certains cas, porter **préjudice** non seulement à vous-même mais également à vos proches (amis, famille...).

L'hameçonnage ou phishing est une technique destinée à leurrer l'internaute en se faisant passer pour un tiers de confiance afin de l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe, coordonnées bancaires...). Il peut s'agir d'un faux message, SMS ou appel téléphonique que l'on pense émaner d'une administration, d'un site de commerce en ligne, d'une banque, d'un réseau social, d'un opérateur de téléphonie, etc.

Les sauvegardes

En cas notamment de **vol**, de **piratage** ou de **détérioration** de vos appareils numériques (téléphone, ordinateur, tablette) vous perdez vos **données** qui, pour certaines, peuvent être **importantes** ou **essentielles** dans le cadre de vos activités **personnelles** ou **professionnelles** (photos, vidéos, fichiers). Il est donc important d'avoir le réflexe de réaliser régulièrement une **sauvegarde** de vos **données**.
Plus d'infos :
cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes

Piratage

Le piratage de compte désigne la prise de contrôle par un individu malveillant d'un compte au détriment de son propriétaire légitime.
L'objectif est de **dérober** des **informations** personnelles ou professionnelles pour en faire un **usage illégal** (usurpation d'identité, transactions frauduleuses, spam, revente des données, etc.).
Comme vos **comptes sociaux** abritent une somme considérable de données personnelles, il est indispensable de les sécuriser.

Pour prévenir un piratage

Choisissez des mots de passe complexes, ne les communiquez pas.
Activez un dispositif d'alerte en cas d'intrusion.
Déconnectez à distance les terminaux encore liés à votre compte.
Désactivez les applications tierces connectées à votre compte.
Réglez vos paramètres de confidentialité.

Pour repérer un piratage

Votre mot de passe est invalide.
Des tweets/posts imprévus sont envoyés depuis votre compte.
Des messages privés sont envoyés de façon non volontaire.
Des comportements inhabituels ont lieu sur votre compte sans votre consentement.
Une notification vous informe que vous avez changé l'adresse électronique associée à votre compte.

Comment réagir en cas de piratage

Signalez le compte piraté auprès du réseau social.
Demandez une réinitialisation de votre mot de passe.
Une fois votre compte sécurisé, n'oubliez pas de parcourir les rubriques sécurité proposées par les réseaux sociaux.

Plus d'infos, et toutes les démarches à suivre pour Facebook, Twitter, LinkedIn, Hotmail, Yahoo, Tik Tok, Instagram, Snapchat, sur le site de la Cnil : cnil.fr/fr/prevenir-reperer-et-reagir-face-au-piratage-de-ses-comptes-sociaux

L'arnaque au faux support technique consiste à effrayer la victime, par SMS, téléphone, chat, courriel ou par diffusion d'un message bloquant son ordinateur, afin, dans un premier temps de l'informer qu'un problème technique grave risque d'entraîner la perte de ses données ou de l'usage de son équipement, puis dans un deuxième temps de la convaincre de payer un pseudo-dépannage informatique et/ou d'acheter des logiciels inutiles, voire nuisibles.

Fausses informations

Certains éléments sont à prendre en compte face à une actualité, une photo ou une vidéo afin de juger de leur pertinence.

Face à une actualité

Méfiez-vous des titres sensationnels et accrocheurs qui cachent souvent de fausses actualités, tiennent très rarement leur promesse en termes de contenus et incitent à générer un clic… ce sont les fameux *putaclics* !
Attention donc aux titres avec superlatifs tels que « hallucinant ou incroyable », aux devinettes du type « Vous n'imaginerez jamais ce qui est arrivé à cet homme », et aux titres listes telles que « 10 trucs qui… ».

Vérifiez l'origine de l'information, si celle-ci émane d'un média ou d'un site internet dont vous n'avez jamais entendu parler, soyez méfiant et consultez les mentions légales pour en savoir plus.
Faites également attention à l'URL (adresse de la page, du site internet), êtes-vous bien à l'endroit auquel vous pensiez aller en cliquant sur un lien raccourci notamment.

Croisez vos sources, en vérifiant que l'information est relayée par différentes sources fiables ; une information relayée uniquement par une seule source doit être prise avec du recul.
Pour vos recherches dans un moteur de recherche, essayez de ne pas dépasser plus de 3 mots et de sélec-

tionner les termes les plus significatifs. Effectuez une recherche neutre sur le sujet (par exemple effectuez une recherche avec « vaccin » et non pas « danger vaccin »).

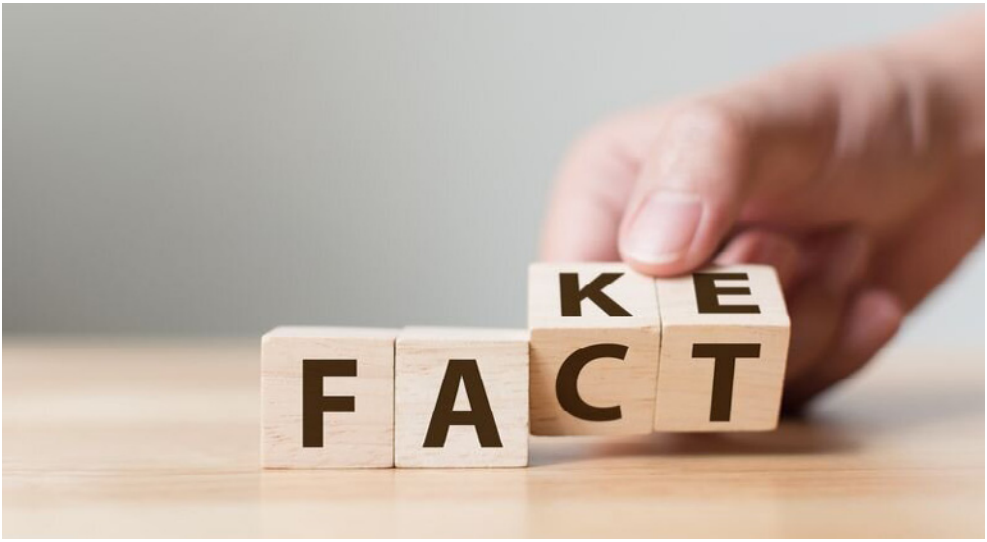
Soyez vigilant à l'orthographe… gare aux posts, articles, publications multipliant les fautes d'orthographe ou de français ; elles sont souvent le reflet du peu de sérieux de l'auteur et synonymes de fausses informations.

Assurez-vous que l'information n'est ni un canular, ni une blague. Certains sites parodiques (ex : Gorafi, NordPresse…) se sont fait une spécialité dans la création de fausses informations humoristiques. Pensez à vérifier que vous n'êtes pas sur l'un de ces sites avant de partager un contenu.

Face à une photo

Prenez le temps de détailler la photo. En faisant appel à votre esprit critique, certains détails peuvent vous interpeller : une retouche Photoshop, un montage grossier, une incohérence entre la photo et sa légende…

Effectuez une recherche inversée de la photo. Si vous avez des doutes sur l'authenticité d'une photo ou si vous voulez vérifier qu'elle n'est pas utilisée hors de son contexte, vous pouvez effectuer une recherche en utilisant, entre autres, Google Image ou le site tineye.com



Face à une vidéo

Le nombre de vues n'est pas un signe de crédibilité, mais seulement un critère de popularité de la vidéo. Une vidéo véhiculant de fausses informations peut ainsi être extrêmement vue.

Une vidéo n'est pas une preuve en soi, il faut être conscient qu'elle peut être source de manipulation ou de désinformation (montage volontairement erroné), ou chercher à véhiculer de fausses interprétations (enchaînement d'images sans lien afin de créer artificiellement du sens).

S'interroger sur le contexte de diffusion et consulter les commentaires. Qui est l'auteur de la vidéo ? Qui a effectué la mise en ligne ? Quelle en est la date ?

Vous n'êtes pas le seul à visionner le contenu, il est possible que d'autres internautes aient laissé des commentaires ou des remarques pertinentes sur la vidéo qui peuvent s'avérer de bonnes sources d'information.

A noter : pour vérifier les différentes utilisations d'une vidéo sur Youtube, vous pouvez utiliser l'outil d'Amnesty International Youtube Data Viewer : citizenevidence.amnestyusa.org

Plus d'infos grâce aux sites suivants :
- **Les Décodeurs**, site du Monde dédié au décodage de l'actu : lemonde.fr/les-decodeurs
- **Les Observateurs**, site de vérification de l'actualité de France 24 : observers.france24.com/fr
- **HoaxBuster**, plateforme collaborative contre la désinformation : hoaxbuster.com

Le cryptovirus ou rançongiciel est un logiciel malveillant qui vise à extorquer de l'argent. Une fois ouvert sur votre poste de travail, il crypte tout ou partie de vos fichiers. On vous demande ensuite une somme d'argent en contrepartie d'une clé de décryptage. Ces virus s'attrapent souvent via le téléchargement de pièces jointes depuis une boite mail ou de fichiers sur internet.

Agir face à la cybermalveillance

Les **actes** de cybermalveillance sont strictement **interdits** par la **loi pénale**, ce sont donc des **infractions** sanctionnées par des peines d'**emprisonnement** et des **amendes**.

Si vous pensez être **victime** d'un acte de cybermalveillance la **plateforme cybermalveillance.gouv.fr** met à disposition un **service en ligne gratuit :** cybermalveillance.gouv.fr/diagnostic/accueil

Si vous souhaitez **signaler** une **escroquerie** en ligne ou un **contenu** illicite sur Internet (incitation à la haine, trafics illégaux, pédophilie, ...), connectez-vous sur la **plateforme** du **ministère de l'Intérieur :** internet-signalement.gouv.fr

Si vous voulez **déposer plainte**, vous pouvez être accompagné gratuitement par les associations du **réseau France Victimes :** france-victimes.fr - 116 006 (appel gratuit 7 jours sur 7 de 9h à 19h). Vous pouvez également vous rendre au **commissariat** ou à la **gendarmerie** dont vous dépendez, ou adresser votre plainte par écrit au **procureur de la République** du tribunal judiciaire de votre lieu de domicile.

Quel risque pour quel usage ?

Cybermenaces \ Supports	Données	Mails	Ordinateurs	Sites web	Tablettes	Téléphone
Chantage à l'ordinateur/la webcam prétendus piratés		×	×			
Fausses offres d'emploi	×	×		×		
Arnaques au faux support technique	×	×	×		×	×
Fraude à la carte bancaire	×	×	×	×	×	×
Hameçonnage (phishing)	×	×		×		
Piratage de compte	×	×		×		
Rançongiciels (ransomwares)	×	×	×	×		
Spams électroniques	×	×				
Spams téléphoniques						×
Virus informatique	×	×	×		×	×

Plus d'infos : cybermalveillance.gouv.fr/cybermenaces

Pour aller plus loin

cybermalveillance.gouv.fr
Cette plateforme a pour missions d'assister les particuliers, les entreprises, les associations, les collectivités et les administrations victimes de cybermalveillance, de les informer sur les menaces numériques et les moyens de s'en protéger.

gouvernement.fr/risques/risques-cyber
Site officiel qui aborde, notamment, les thématiques de la cybercriminalité, de l'atteinte à l'image, de l'espionnage, du sabotage et qui apporte de précieux conseils aux usagers.

cnil.fr
Site de la Commission nationale de l'informatique et des libertés - CNIL - qui est le régulateur des données personnelles ; elle accompagne les professionnels dans leur mise en conformité et aide les particuliers à maîtriser leurs données personnelles et à exercer leurs droits.

ssi.gouv.fr
Site de l'Agence nationale de la sécurité des systèmes d'information - ANSII - dont la volonté est de répondre aux questions de cybersécurité et de partager une information ciblée et accessible.

Info Jeunes Bourgogne-Franche-Comté (Crij)
27 rue de la République
25000 BESANÇON
03 81 21 16 16

2 rue des Corroyeurs
21000 DIJON
03 80 44 18 29

jeunes-bfc.fr

Informations susceptibles d'évoluer :
*version mise à jour en ligne sur **jeunes-bfc.fr/livrets-dinfos***