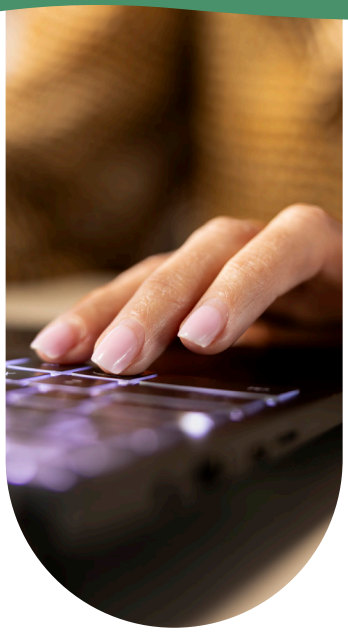
LIVRET D'INFORMATION

Numérique

Risques et bonnes pratiques



JEUNES-BFC.FR

MINISTÈRE DES SPORTS, DE LA JEUNESSE ET DE LA VIE ASSOCIATIVE
Liberté Égalité Fraternité

RÉGION BOURGOGNE FRANCHE COMTÉ

Label Information Jeunesse

info Jeunes BFC
EXPLORER LES POSSIBLES

Numérique : risques et bonnes partiques

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 3
> Piratage 5
> Fausses informations 7
> Agir face à la cybermalveillance 10
> Pour aller plus loin 11

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 **12 caractères** 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 certaines de 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 une photographie (ou film) est publiée 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…).

Attention au « **sharenting** » : qui consiste à publier des photos, vidéos ou des informations concernant son enfant sur les réseaux sociaux. Cette pratique courante des parents peut porter atteinte à la dignité ou à la réputation de son enfant, en effet ces photos, vidéos et informations peuvent être détournées (grâce à l'IA) par d'autres internautes dans le but de cyberharcèlement, création de faux profils, ou se retrouver sur des réseaux pédopornographiques. L'enfant à droit au respect de sa vie privée (qui inclut son image).

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.**

A noter : *avec l'essor de l'IA, il est illusoire de s'imaginer pouvoir protéger à 100% la confidentialité de ses contenus numérique. Nos données personnelles étant stockées sur divers sites et plateformes en ligne (banque, assurance maladie, impôts, sites de vente en ligne...) qui font l'objet de cyberattaques régulières.*

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 publications imprévues 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.

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.

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, sur le site *17cyber.gouv.fr* qui vous donnera les démarches à suivre en cas de piratage.

Pour les services suivants : Facebook, X, LinkedIn, Gmail, Hotmail, Yahoo, Tik Tok, Instagram, Snapchat, vous trouverez des informations utiles 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, tchat, 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, ils tiennent très rarement leur promesse en termes de contenus et incitent à générer un clic… ce sont les fameux **"Pièges à clics"** !

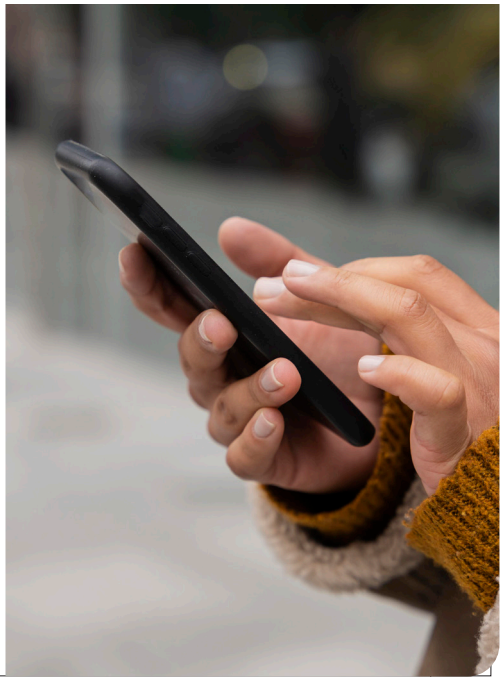
Attention donc aux titres avec superlatifs tels que « hallucinant ou incroyable », aux devinettes du type « Vous n'imaginerez jamais ce qui est arrivé à cet homme », et aux titres listes telles que « 10 trucs qui… ».

Avec l'utilisation massive de **l'IA (Intelligence artificielle) générative** on assiste à la multiplication de **faux contenus (Fake-news).** Par exemple, une photo de Donald Trump en train de planter le drapeau des Etats-Unis sur le sol du Groenland, ou des sites internet entièrement générés par l'IA diffusant de fausses informations.

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.



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 photo générée via l'Intelligence artificielle (IA), une retouche Photoshop, un montage grossier, une incohérence entre la photo et sa légende…

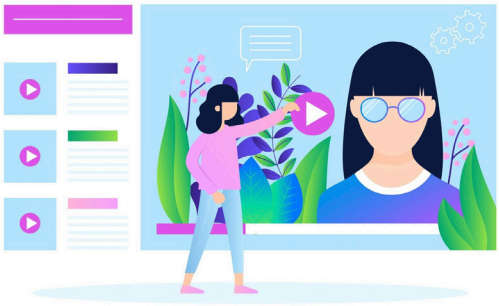
Effectuez une recherche inversée de la photo. Si vous avez des doutes sur l'authenticité d'une photo ou si vous voulez vérifier qu'elle n'est pas utilisée hors de son contexte, vous pouvez effectuer une recherche en utilisant, entre autres, Google Image ou le site *tineye.com*

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).

Les **deepfakes**, ces montages vidéo hyperréalistes **générés par l'IA**, se multiplient et deviennent de plus en plus difficiles à détecter. Le site *internetsanscrainte.fr* donne des conseils pour les repérer et plus généralement il sensibilise les jeunes aux risques de désinformation.



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.

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*

- **Vera (AskVera)** est une IA française gratuite de vérification de l'information, créée par l'ONG LaReponse.tech pour aider à lutter contre la désinformation. On lui pose une question par téléphone, WhatsApp ou Instagram ; elle recherche en temps réel dans des médias et sites de fact-checking fiables, puis renvoie une réponse sourcée.
Elle est connectée à plus de 500 sources fiables :
askvera.org - 09 74 99 12 95 *(par tél ou WhatsApp).*

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, un service proposé par la Police Nationale, la Gendarmerie Nationale et Cybermalveillance.gouv.fr intitulé **17Cyber : *17cyber.gouv.fr* vous permet de faire le diagnostic de votre situation.**

Ce guichet unique d'assistance Cyber propose aux victimes de cybermalveillances de les assister, il permet :

- d'établir rapidement un diagnostic du problème rencontré,
- de bénéficier de recommandations personnalisées selon la situation rencontrée,
- de se voir proposer une assistance technique par un prestataire informatique et un accompagnement par tchat 24/7 avec un gendarme ou un policier lorsque la menace le nécessite.

Si vous souhaitez **signaler une escroquerie en ligne** (virus, hameçonnage, arnaque bancaire…) **ou un contenu illicite** sur Internet (incitation à la haine, trafics illégaux, pédophilie, …), la plateforme 17Cyber vous orientera vers les services concernés et vous guidera dans vos démarches. Vous pouvez également vous connecter directement 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 : *francevictimes.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.

Pour aller plus loin

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

17 CYBER
Mon assistance en ligne

• cybermalveillance.gouv.fr et 17cyber.gouv.fr

Ces deux plateformes ont 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.

• info.gouv.fr/risques/cyber-conseils-aux-usagers

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.

• cyber.gouv.fr

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

• promeneursdunet.fr

Site du dispositif des **Promeneurs du Net**, un réseau de professionnels de la jeunesse qui poursuivent leurs actions éducatives sur Internet.

Les Promeneurs du Net assurent, en prolongement de leur travail, une présence bienveillante sur les réseaux sociaux qui permet à tous les jeunes de venir échanger avec eux, même s'ils ne fréquentent pas leurs structures.

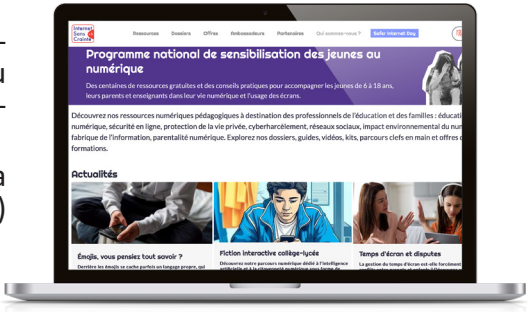
Ils ne jugent pas, ne sanctionnent pas, ils sont disponibles pour écouter, conseiller et soutenir, en toute confidentialité, en ligne ou en face-à-face.

Ils peuvent notamment vous accompagner sur les questions du numérique, du cyber-harcèlement, des fakes news …

Cette initiative est portée par la Caf (Caisse d'allocations familiales) de chaque département.

• internetsanscrainte.fr

Ce site propose des centaines de ressources gratuites (vidéos, serious games, activités interactives, guides, fiches…) pour accompagner les jeunes dans leur vie numérique et **les sensibiliser aux bons usages du numérique**. Destiné aux professionnels, aux parents et enseignants, il traite de différentes thématiques : éducation au numérique, sécurité en ligne, protection de la vie privée, cyberharcèlement, réseaux sociaux, impact environnemental du numérique, fabrique de l'information, parentalité numérique…



Parution : octobre 2026