

La gestion et la compréhension des outils numériques ne fait pas, ou peu, l'objet de formation au cours de notre éducation. Pourtant, en tant que parents, nous pouvons être pris de cours faces à l'univers des possibles avec un ordinateur ou un téléphone, et certains de nos choix numériques de parents sont suggérés (voire contraint) par les outils qui nous sont proposés. Devrions-nous plutôt être partisans d'une approche parentale reposant sur la confiance ou sur le contrôle ?

Ce guide pratique est à destination des parents ou personnes en charge de l'éducation d'enfants y compris dans l'adolescence.

Il a pour objectif d'aider son lectorat dans la mise en place d'un cadre clair et sain pour toutes les questions relatives à l'interaction des jeunes avec le numérique.

Parentalité



Numérique

**Petit guide à destination des parents
préoccupés par les usages
technologiques de leurs jeunes**

édition 2026

Hackstub x ARN

Ce guide pratique est à destination des parents ou personnes en charge de l'éducation d'enfants y compris dans l'adolescence.

Il a pour objectif d'aider son lectorat dans la mise en place d'un cadre clair et sain pour toutes les questions relatives à l'interaction des jeunes avec le numérique.

La gestion et la compréhension des outils numériques ne fait pas, ou peu, l'objet de formation au cours de notre éducation. Pourtant, en tant que parents, nous pouvons être pris de cours faces à l'univers des possibles avec un ordinateur ou un téléphone, et certains de nos choix numériques de parents sont suggérés (voire contraint) par les outils qui nous sont proposés.

Par ailleurs, en tant qu'outil technique relativement récent à l'échelle de l'humanité, l'électronique et ses applications numériques font muter nos sociétés et nos organisations tout

Il est sous licence libre CC BY-SA 4.0:
<https://creativecommons.org/licenses/by-sa/4.0/deed.fr>

Fontes de titres : VG5000 ; corps : Quebec

amoureuse ou sexuelle[1], état qu'ils décrivent comme célibat involontaire ou incel-dom.

Logiciel libre : un logiciel donnant le droit de l'utiliser et de lire, modifier et distribuer son code source

Minerais de sang : les minerais de conflit, parfois aussi nommés « minerais de sang », sont des minerais extraits dans des pays en conflit armé et suspectés d'alimenter, voire de susciter, des guerres civiles.

Sexting : Échanges de messages ou de photos sexuellement explicites

A propos de ce document

Ce document a été écrit initialement par Valentin Grimaud puis relu et complété par d'autres personnes bénévoles au sein d'Hackstub et d'Alsace Réseau Neutre, et mis en page par Ada LaNerd.

en renforçant déraisonnablement le sentiment de contrôle dans tous les domaines de la vie. La famille ou l'éducation n'échappent pas à cette tendance.

C'est pourquoi ce guide recommande en premier lieu de nous interroger sur notre posture. Outre les sujets de maîtrise des connaissances techniques, devrions-nous plutôt être partisans d'une **approche parentale reposant sur la confiance ou sur le contrôle** ?

Ce guide propose de tendre vers une perspective qui s'affranchit de ce dilemme de l'accompagnement de la jeunesse vers une maturité saine et épanouie, adaptée à notre contexte : co-construire la confiance et prendre soin d'offrir des garde-fous.

Sommaire

1. Faire confiance.....	5
Besoin d'expérimentation.....	5
Besoin d'autonomie.....	5
Besoin d'intimité et de vie privée.....	7
2. Évaluer les risques.....	8
Interfaces et contenus addictifs.....	8
Lumière bleue.....	10
Discussions nocturnes.....	11
Intelligences Artificielles génératives.....	11
Influences & image de soi.....	12
Cyber-criminalités.....	14
Contenus inadaptés ou dangereux.....	24
3. Penser aussi les bénéfiques.....	31
4. Conseils pour mieux éduquer avec le numérique	
.....	32
4.1. Protéger.....	33
4.2. Réguler.....	38
4.3. Encourager et accompagner les usages....	42
Glossaire.....	44
A propos de ce document.....	45

Glossaire

Allotage : pratique d'usurpation de la fonction d'un employé par téléphone. Par exemple : des personnes qui se font passer pour un conseiller bancaire et encourage la victime à mener des actions critiques sur une application bancaire.

Brouteur : Personne spécialiste des arnaques sur Internet (arnaque aux sentiments, chantage, etc.).

Dark pattern : une interface utilisateur qui a été volontairement conçue pour tromper ou manipuler un utilisateur.

DSA : Le règlement européen sur les services numériques (DSA) qui vise une responsabilisation des plateformes

Incels : Personnes qui se définissent comme étant incapables de trouver une partenaire

usages dans le cadre que l'on a mis en place.

Installer des logiciels dédiés à la création

Pour favoriser la création, il semble pertinent d'installer des logiciels de bureautique (LibreOffice ou OnlyOffice), de dessins (GIMP, Krita), de montage audio ou vidéo (audacity, kdenlive), de graphisme 3d (blender), de programmation (thonny), etc.

1. Faire confiance

Ce guide part de l'idée que la confiance est un des ingrédients clés pour répondre correctement aux besoins des jeunes et favoriser leur développement.

Besoin d'expérimentation

Pour grandir et apprendre, **les enfants ont besoin d'expérimenter et de faire des erreurs**, cela s'applique aussi à l'espace numérique. Face aux risques détaillés dans la partie 2, vous pourriez être tenté·e·s dans l'absolu de retirer complètement le numérique de la vie de vos jeunes, mais ce faisant, vous risquez d'entraver leur apprentissage et vous ferez probablement pire que mieux.

Besoin d'autonomie

Au fil des années, les ados acquièrent **une maturité et une autonomie qu'il est bon**

4.3. Encourager et accompagner les usages

Préférez l'ordinateur dans le salon plutôt que le smartphone

Les ordinateurs ont des environnements plus ouverts et explorables que les smartphones. Ils favorisent une meilleure compréhension du numérique.

Distinguer les usages récréatifs, passifs ou consommateurs des activités de création

La recherche s'accorde à dire que le temps d'écrans n'est pas une bonne métrique pour évaluer les effets positifs ou négatifs du numérique. Il convient de distinguer plus finement les choses, regarder un film n'est pas équivalent à jouer à un jeu ou à faire de la peinture numérique.

Il peut dès lors être pertinent de distinguer les

d'offrir à Noël ou lors d'anniversaire des équipements numériques (montres connectées, console de jeux, smartphone, abonnement steam, etc.). Si ce n'est pas votre souhait, faite le savoir, c'est plus facile que de refuser ou retirer un cadeau...

Du téléphone basique au smartphone avec internet et réseaux sociaux

De nombreux enfants se retrouvent directement avec des smartphones ayant accès à internet et aux réseaux sociaux. Si vous décidez d'équiper votre enfant et qu'il est assez jeune, il peut être pertinent de le faire de façon graduelle, plutôt que de lâcher votre enfant seul·e dans le Grand Internet. Commencez par un téléphone simple, puis éventuellement un smartphone mais sans internet, etc.

d'accompagner. Il faudra donc adapter votre cadre au fur et à mesure qu'ils grandissent. Toutefois, comme en escalade, même si vous donnez du mou pour leur permettre d'évoluer, vous devez rester attentif·ve pour assurer leur sécurité en cas de grosses gamelles. C'est pour cela que dans la section 4, nous suggérons également des mesures qui permettront à votre enfant d'évoluer avec quelques gardes fous. Besoin de se définir et d'appartenir au groupe

Les ados tentent de répondre aux grandes questions tels que « Qui suis-je ? », c'est en partie pour ça qu'ils ressentent le besoin d'appartenir à un groupe et commencent à se soucier de comment les autres les perçoivent.

Il est donc important de **s'assurer qu'ils puissent au mieux évoluer dans leur relation aux autres.** Les couper du monde numérique à cause des risques peut-être aussi dangereux que les risques que l'on cherche à éviter.

Besoin d'intimité et de vie privée

Certaines formes de contrôle visant à nous rassurer en tant que parent peuvent avoir des impacts négatifs imprévus. En l'occurrence, ce n'est pas parce qu'une application vous propose une option de suivis qu'elle est légitime ou sans risque pour vos relations à venir avec vos jeunes. La géolocalisation, la lecture de l'historique de navigation ou des conversations, toutes ces pratiques sont assez similaires à la lecture d'un journal intime. Vous devez donc bien réfléchir pour respecter du mieux possible l'intimité et la vie privée de votre jeune.

Rappel: espionner les actions d'un proche à son insu par le biais d'outils technologiques est illégal, même si iel est mineure.

Il peut être judicieux de distinguer les types de pratiques (créatives, récréatives, etc.).

Boite à smartphone

L'idée est simple, une boîte dans lequel on dépose le smartphone pendant les repas et les moments de repos (ou sans écrans).

Extinction automatique de l'équipement

Il peut être possible d'éteindre automatiquement un équipement, ce qui évite parfois de houleuses négociations.

Extinction automatique du wifi

Il est possible également d'opter pour une coupure du wifi, par exemple la nuit. Dans ce cas, il faut penser à mettre un mot de passe correct sur la box.

Donner des consignes pour les cadeaux

Les proches ou parents séparés sont susceptibles

d'écrans si l'on est soi-même très scotché à son écran, au point que ses enfants ressentent une frustration ou une absence. Il s'agit donc de donner autant que possible l'exemple.

Proposer d'autres activités

Proposer d'autres activités est une façon douce d'aider à réguler la sur-consommation d'écrans. Ce n'est pas toujours facile ou possible, mais c'est parfois une alternative possible pour éviter des disputes ou des sermons sur le sujet.

Quota de temps d'écrans

Il peut être utile de définir un temps d'écrans par semaine à adapter en fonction de l'âge et des capacités du ou de la jeune. Pour le mettre en place des applications de contrôle parentale peuvent être utilisés, mais également des mots de passe, une extinction automatique et/ou une boîte à smartphone.

2. Évaluer les risques

Même si les géants de la tech n'en font pas publicité, les risques liés à l'usage du numérique sont nombreux: troubles de l'apprentissage, perte de relation sociale, perte d'autonomie, troubles du sommeil, mauvaises images de soi, influences, addictions, traumatismes, perte d'argent, non respect du consentement, mise en danger, esclavage moderne, etc.

Pour la plupart, ces risques apparaissent dans des situations ou des usages précis. C'est pourquoi, ci-dessous, sont détaillés ces risques en fonction des situations. Néanmoins, plus un ou une jeune utilise le numérique plus il ou elle est susceptible d'être confronté·e à ces risques.

Interfaces et contenus addictifs

Les géants de la tech créent volontairement

des interfaces et contenus addictifs. Ces entreprises embauchent leurs personnels et développent des méthodes dans le but de rendre leurs utilisateur·ices ou leur audimat captif en récoltant le plus d'informations possibles pour leur faire adopter de nouvelles habitudes. Elles sont d'ailleurs régulièrement condamnées pour certains des procédés utilisés.

Ces contenus entrent en symbiose avec les besoins des parents qui ont besoin d'occuper leurs enfants lorsqu'ils sont occupés ou qu'ils ont besoin de souffler.

Malheureusement, la conséquence de ces conceptions addictives est souvent une surconsommation numérique récréative qui peut remplacer d'autres activités (sommeil, discussions orales, jeux, activités physiques, etc.) qui sont bénéfiques au développement des jeunes (et des adultes). Les impacts semblent être plus ou moins graves selon l'âge, le temps passé et le type d'activité numérique.

pas, quelles apps sont installées, que font-elles ?

4.2. Réguler

Sacraliser au moins un temps sans smartphone / écrans

Que ce soit le repas ou à un autre moment, il est important que chaque jour, vous et vos enfants, puissiez être ensemble sans écrans interposés.

Pas d'écran ou smartphone 1 h avant le coucher

La lumière bleue maintient le cerveau éveillé et peut nuire au sommeil. Pour que vos enfants ne soient pas fatigués dès 8h, pensez à interdire les smartphones dans les chambres et les écrans avant de se coucher. Couper le wifi après une certaine heure et cachez vos vieux appareils.

Donner l'exemple

Il est évidemment difficile de réguler le temps

contenus non adaptés aux mineurs. Ils ont également des accès qui permettent l'installation de nouvelles apps. Il convient de sécuriser ses accès pour éviter que les jeunes soient exposés à divers menaces, contenus ou suppriment accidentellement des données importantes.

Il est donc déconseillé de prêter son smartphone ou de donner ses mots de passe.

Mettre en place une session enfant

Vous pouvez combiner tout ou partie des conseils de cette section pour créer une session enfant (ou ados) adaptées sur les équipements de vos choix.

Configurer aux mieux l'équipement et les comptes de réseaux sociaux

Il est important de paramétrer avec vos jeunes les équipements et les apps installées. Notamment, est-ce que un profil est public ou

Quoi qu'il en soit, **ne soyez pas trop rudes sur ce sujet avec vos jeunes (ou avec vous-même)**, dirigez plutôt votre colère vers les concepteur·ices de ces contenus, et piochez dans la boîte à outils de ce guide (partie 4) pour vous aider à revenir à un usage raisonnable.

Lumière bleue

La lumière bleue est un autre élément qui peut déclencher des troubles ou du manque de sommeil. De plus, une exposition aiguë, peut être phototoxique pour la rétine. La technologie de la plupart des écrans diffusent une lumière bleue qui maintient éveillée. C'est l'une des raisons pour lesquelles il est conseillé qu'il y ait une activité tampon sans écran avant de dormir.

Rappelons qu'un ou une jeune fatiguée est plus susceptible d'être irritable ou d'avoir des difficultés en cours.

Discussions nocturnes

Les chats qu'ils soient intégrés à une application ou un jeu vidéo, ont les défauts de leurs qualités puisqu'ils permettent de rester en contact. Chez les ados, il n'est pas rare que ces derniers réclament leur smartphone après 21h, car c'est à partir de cette heure que tout ce passe. Gardez donc bien en tête que si vous autorisez vos ados à chatter à ces heures tardives, vous faites à la fois le choix pour vos jeunes mais aussi pour leurs ami·es. Une parade pour les parentés qui se connaissent et de se mettre d'accord sur une heure de fin des conversations, malheureusement ce n'est pas toujours possible.

Intelligences Artificielles génératives

Depuis 2023, les IA génératives sont de plus en plus utilisées dans la société. Ces nouveaux usages se retrouvent également chez les jeunes

Utiliser si possible des outils libres

Les logiciels libres sont souvent moins malveillants et certaines attaques y sont inopérantes. Par contre, rien n'est parfait, ils sont parfois utilisés par le cybercrime, comme d'autres petites plateformes, car ils sont moins surveillés.

Créer un portail de ressource

Afin de baliser le chemin de vos enfants et pré-ados, il peut être pertinent de créer un portail de ressources (jeu vidéo, film, etc.) que l'on aura pré-validé. Ce portail peut ainsi permettre au jeune d'utiliser efficacement son temps d'écrans tout en restant dans une zone bornée et adaptée à son âge.

Protéger les équipements et données des adultes du foyer

Les adultes d'un foyer sont susceptibles de gérer des données importantes ou de consulter des

intrusifs. Demandez-vous ce dont vous avez besoin pour votre cadre éducatif plutôt que d'activer des fonctionnalités qu'une entreprise propose et présente comme la norme au travers de ses interfaces (souvent avec un intérêt commercial).

Rappel: espionner les actions d'un proche à son insu par le biais d'outils technologiques est illégal, même si iel est mineure. Les ados doivent savoir si on les géolocalise ou si on lit leurs conversations.

Pensez aux anciens smartphones

Certains jeunes ayant un smartphone avec contrôle parental, le contourne en utilisant un ancien smartphone de la famille (en général celui des parents). Mettez-les dans un endroit sûr à l'abri des tentations ou simplement donnez-les pour qu'ils soient reconditionnés.

générations qui les utilisent aussi, notamment pour chercher une information ou faire leur devoir.

Il faut dès à présent sensibiliser les jeunes sur :

- la perte d'autonomie et le frein à l'apprentissage si iels prennent l'habitude de faire générer des réponses complètes à leurs devoirs
- la manière de vérifier si une information est vraie ou fausse (les IA génératives « hallucinant » des réponses qui peuvent sembler vraies mais ne le sont pas)

Influences & image de soi

Des documents internes de l'entreprise Meta qui gèrent Instagram, un des réseaux sociaux les plus utilisés par les jeunes, montrent au travers d'une étude interne que **30% des adolescentes utilisatrices d'Instagram développent une**

moins bonne image d'elles-mêmes du fait de l'utilisation du réseau social.

Plus globalement, nombreux et nombreuses sont les jeunes à regarder les contenus viraux ou produits par des "influenceurs", à rêver de le devenir elleux même, sans se rendre compte que **les vrais influenceurs restent les entreprises qui décident et orientent les algorithmes de mise en avant des contenus.**

Certains sites comme jeuxvideo.com ont aussi fait l'objet de **propagande et d'embrigadement politique ou haineuse par différents groupes et partis politiques (par exemple des groupes d'incels)**. Il existe même des logiciels et des organisations utilisant des milliers de faux comptes. Leur but est d'influencer les algorithmes pour propulser en avant des contenus, mais aussi de commenter massivement certains types de profils cibles sur les réseaux sociaux pour manipuler l'opinion ou harceler une

régulièrement autres que leurs parents pour augmenter leurs chances de réussir à demander de l'aide en cas de besoin.

Pas de réseaux sociaux avant 13 ans

Les États Unis empêche les géants de la tech de créer un compte à un enfant de moins de 13 ans. L'Australie empêche les moins de 16 ans d'avoir un compte. En France, il est interdit aux plateformes de créer un compte à un mineur de moins de 15 ans sans l'accord des parents. Mais la loi est en conflit avec le DSA et le décret n'est pas publié.

Nous vous conseillons de n'autoriser Instagram, TikTok ou Snapchat qu'à partir de la 3ème ou de la seconde. A vous de prendre en compte les risques et d'évaluer si vos jeunes sont prêts à les utiliser (cf partie 2).

Configurer un logiciel de contrôle parental

En évitant autant que possible, les logiciels trop

4.1. Protéger

Faire avec et sensibiliser (au moins au début)

Même si vous ne vous sentez pas à l'aise avec le numérique, il est important d'être au côté de vos enfants et ados lors de leur découverte du numérique. En tant qu'adulte, vous pouvez avoir un regard sur ce qu'il se passe même si votre ados va plus vite que vous pour manipuler.

Par ailleurs, de nombreux points de la partie 2 de ce guide mérite que vous sensibilisiez vos jeunes à différents moments de leurs enfances et adolescences.

Vous devriez notamment les sensibiliser à ce qui est un bon secret et ce qui est un mauvais secret (celui qui est lourd à porter et nous fait mal).

Favoriser la position d'un tiers de confiance

Certaines questions ou situations sont difficiles à évoquer avec un parent. Assurez-vous qu'ils ont au moins un tiers de confiance qu'ils voient

catégorie de population (femmes, opposants politiques, etc.).

De façon générale, ces personnes et entités qui influencent le font majoritairement pour leurs **intérêts qui coïncident ou non avec ceux de vos jeunes.**

Pour finir, si votre ado acquiert une notoriété en ligne, vous devriez l'accompagner dans sa gestion de son image publique. Il est facile de faire un faux pas, les critiques et commentaires négatifs sont légions et parfois la chute est douloureuse.

Cyber-criminalités

Si les géants de la tech sont régulièrement condamnés pour leurs procédés illégaux vis-à-vis des utilisateur·ices, ces mastodontes sont loin d'être les seules, et il existe de nombreux autres **tiers malveillants** sur le net.

La cyber-criminalité est très diverses, ci-dessous, vous trouverez un ensemble d'activités crapuleuses qui n'arrivent pas qu'aux autres.

Cyberharcèlement

Avec ou sans écran, **votre jeune peut harceler ou être harcelé·e**. Dans les cas les plus graves, les victimes sont susceptibles de développer une dépression, d'être en danger ou de tenter de mettre fin à leurs jours. Les jeunes qui harcèlent risquent de leur côté de porter même adulte une forte culpabilité, sans parler des risques légaux.

Gardez en tête qu'il y a plus de harceleurs et/ou harceleuses que d'harcelé·es, il est donc conseillé de sensibiliser vos jeunes à ces questions et de leur donner des clés et des **repères pratiques pour agir correctement dans les 2 situations**.

A noter que le cyberharcèlement est souvent décrit comme le prolongement de situation

requis d'interaction

4. Conseils pour mieux éduquer avec le numérique

Ces conseils ne sont que des propositions et sont listés ici pour vous donner des idées. A vous de construire quelques choses de cohérent en fonction de votre foyer et de votre perception de vos jeunes. Garder en tête que votre expérience et vos habitudes numériques, ne sont pas forcément les leurs. C'est l'occasion de découvrir d'autres façons d'utiliser les outils numériques.

Vous pouvez aussi utiliser le site faminum.com pour construire ensemble une charte du numérique en famille.

3. Penser aussi les bénéfiques

Les bénéfiques des nouvelles technologies sont vendus en permanence par de nombreux acteurs (géants du numérique, administration, etc.).

A l'échelle des jeunes, le numérique peut permettre à un·e ado de :

- développer une **créativité** via ce support (programmation, musique, montage, etc.)
- **accéder à des connaissances en autonomie** et de façon autodidacte dans tous types de domaines qui les passionnent
- rester en phase et en capacité de **comprendre et d'interagir avec le monde dans lequel ils vivent**
- **accéder à des groupes sociaux** qui ont posé inconsciemment le numérique comme pré-

d'harcèlement au collège, mais il peut aussi être totalement en ligne, par exemple certaines communautés nocives se sont spécialisées dans le doxing, c'est-à-dire la publication des coordonnées géographiques et personnelles d'une personne en vue de faciliter son harcèlement.

Sextorsion

Sans doute **une des menaces les plus sérieuses concernant les ados**. Il est malheureusement assez aisé pour des arnaqueurs de faire chanter des jeunes après avoir récolté leurs contacts et convaincu de se dénuder face caméra à travers une visio ou l'envoi de photo supposée éphémère - à tort - par exemple avec Snapchat.

De façon alternative, certains peuvent aussi pirater les comptes ou équipements afin d'espionner leurs victimes, raison supplémentaire pour laquelle le sexting n'est pas sans risque.

D'autres feront des montages ou utiliseront des IA pour produire des deep fakes et faire ainsi croire que la victime aurait pratiqué certains actes.

Les **chats aléatoires comme omegle**, majoritairement fréquenté par des ados sont des espaces à risques où les jeunes peuvent facilement être exposés à du contenu pour adultes ou être piégé-es par des cybercriminels (ou d'autres jeunes par moquerie).

Pédocriminalité

Si la majeure partie des violences sexuelles sur mineurs sont commises par un homme ou un ado de l'entourage de la victime, il n'en reste pas moins que des cyber-pédocriminels rodent sur des applications utilisées par des mineurs. Bien que leurs motivations soient différentes, ils sont susceptibles d'utiliser des méthodes similaires aux arnaqueurs qui pratiquent la

En bref, les objets numériques ne devraient pas être des jouets ni considérés comme des objets jetables tant leurs coûts écologiques et sociaux sont importants. Il est grand temps d'apprendre collectivement à réguler nos usages et à faire durer nos équipements.

création et le partage de fausses images ou vidéos, par exemple à caractères pornographiques, sans pour autant relever d'un chantage. L'optique est souvent d'humilier la personne visée par ce faux. Des jeunes peuvent ne pas prendre conscience de l'impact que peuvent avoir ces faux, tout en étant le plus souvent illégale.

Pollution et coût humain

Pour finir, à l'échelle mondiale, le numérique est de plus en plus énergivore. A moins de faire l'autruche, les conséquences de l'extraction des ressources, avec les minerais de sang responsables de conflits armés et l'exploitation d'enfant dans certaines régions du monde, ne peuvent être ignorées. Les enfants d'aujourd'hui devraient vivre jusqu'en 2100, époque qui selon la plupart des pronostics pourraient être ébranlés par la dette climatique, énergétique et l'épuisement des ressources.

sextorsion. Certains peuvent aussi chercher à rencontrer les jeunes hors lignes.

Arnaque (aux sentiments ou au blocage de compte)

Certains arnaqueurs, qu'on nomme des « brouteurs », entament des relations à distance pour créer de l'attachement. Lorsque la relation devient importante, les brouteurs changent d'attitude ou explique qu'ils ont besoin d'argent pour venir les voir, etc.

D'autres se font passer pour des administrateurs de réseaux sociaux ou des supports techniques et demandent de faire des actions pour sécuriser ou débloquent un compte. Typiquement, donner un code reçu par SMS. S'ensuit par exemple un chantage financier pour ne pas supprimer le compte.

Cambriolage

Les cambrioleurs sont aussi sur les réseaux sociaux et n'hésitent pas à chercher les profils qui publient des photos de vacances pour rendre visite au domicile. Certains utiliseront même **les méta-données contenues dans les photos pour déterminer l'heure et l'endroit de la prise.**

Il convient donc a minima de décaler la publication de ses photos une fois rentré de vacances de même pour les autres publications géolocalisées (partage de géolocalisation, parcours de running). Les publications de traces de footing ont même permis de trouver des bases militaires secrètes.

Trafic de drogue

Certains trafiquants se sont modernisés et passent parfois par le net pour vendre ou recruter. Il existe **quelques cas** documentés dans lesquels des trafics ont recruté des guetteurs ou des revendeurs via des jeux en

Nudes et sexting

Depuis que le smartphone est apparu la pratique du nude (échange de photos dénudés) s'est répandue dans la sexualité. Selon une étude belge, en 2022, **75% des 13-25 ans ont déjà envoyées une photo dénudée à une autre personne.** Le problème survient lorsqu'il y a partage secondaire, c'est à dire que l'image est envoyée ou montrée à d'autres personnes que celle qui était destinataire.

Comme pour le cyber-harcèlement, le risque est double, vos jeunes peuvent tout autant être victime de l'exhibition de leur corps que de **ne pas prendre la mesure de la gravité de transmettre (ou de menacer de transmettre) une photo reçue.**

Deepfake / Fakenews

Une pratique qui se développe depuis peu est la

espaces communautaires (réseaux sociaux, forums) et les jeux web n'inclut pas cet indicateur, à vous donc de vous faire un avis.

Les conséquences d'une forte consommation de contenus violents sont en constant débat et à moins d'être chercheur·euses, il est difficile de se faire un avis éclairé. Néanmoins, il est probable que les effets varient en fonction des individus de toute façon, l'observation de vos jeunes restera probablement le plus instructif les concernant. Ont-ils peurs ? Font-ils des cauchemars ? Sont-ils plus violents ou développent-ils un goût pour les armes ?

Promotion de conduite à risques

Internet et les réseaux sociaux regorgent de contenus qui encouragent sous forme de défis ou d'expérience à prendre des risques: il s'agit typiquement des **challenges TikTok** ou des tutos pour construire un pétard qui parfois se terminent par des drames.

ligne.

Piratage

Le piratage est aussi une menace courante, de nos jours **de nombreuses attaques sont automatisées et ratissent très large**. Il n'est jamais agréable de se faire voler, de perdre l'accès à son équipement ou à un compte, d'être filmé à son insu ou d'envoyer accidentellement des virus informatiques à tous ces contacts. Certains pirates sont spécialisés dans la revente de données, d'autres dans le phishing, le chantage ou encore dans le allotage.

Si les ados peuvent comme les adultes être victimes de ces piratages, certaines attaques peuvent aussi être mises en œuvre par des mineurs. Si votre jeune est pris·e de passion pour la technique et l'informatique, il peut être judicieux de les sensibiliser en leur rappelant que de "grands pouvoirs impliquent de grandes responsabilités".

De nombreuses attaques se basent exclusivement sur des failles humaines ; d'autres les mixent avec des failles techniques. Ci-dessous, des exemples de signes alarmant typiques qui permettent d'activer vos boucliers mentaux :

Urgence ou manipulation émotionnelle

De nombreuses arnaques inclut une date limite courte ou font appel à des émotions qui vont biaiser les capacités d'esprit critique (peur, séduction, etc.).

« Bonjour,

A la suite de signalements, nous avons suspendu votre compte car il est suspecté de faire partie d'une galaxie de faux comptes.

Merci de transmettre le code reçu par SMS avant 8:15.

Passé ce délai, votre compte sera clôturé et votre adresse IP bannie de notre réseau

Certains **sites d'achats ou de jeux en ligne** peuvent aussi être très vicieux, et vont user de **dark pattern pour faire souscrire des abonnements**. Parfois, elles profitent du fait que l'option Internet+ (paiement par la facture de son fournisseur d'accès à internet) est activée par défaut, notamment chez Free et Red-by-sfr.

Enfin, **les plateformes de cryptomonnaie** et plus globalement toutes méthodes pour gagner de l'argent facilement 'ont tendance à attirer les jeunes qui pour certains seront prêt à tenter de dompter les cours du bitcoin avec la CB de leurs parents.

Violences

De nombreuses vidéos, films, musiques, forums ou jeux vidéos sont particulièrement violents. **Des notations existent pour classifier les contenus en fonction de l'age** pour les films et les jeux vidéos en vente. Mais, les contenus des

Parmi les risques de la consommation de porno, on peut citer l'exposition à des contenus illégaux ou encore **la construction ou l'amplification de représentations biaisées ou de désirs illégaux** notamment vis-à-vis du **consentement** ou des violences sexistes. Consulter du porno c'est rencontrer **les désirs et les idées des réalisateurs de ces contenus, qui parfois sont extrêmes voire hors de la légalité**. Si l'exposition est précoce, il est aussi possible de provoquer des **traumatismes** proches de ceux produits par une agression sexuelle.

Argent en ligne

Au-delà du porno, il existe d'autres types d'activités inadaptés aux mineurs.

Par exemple, les sites de **jeux d'argents (paris, poker, casino)** peuvent créer de vraies **addictions** chez leurs usager·e·s et sont censés être interdits aux mineurs.

social, une voie de recours restera alors possible en envoyant une réclamation par lettre recommandée à notre service juridique : 34 rue de la Paix »

« [...]Si tu ne transmets pas le coupon PCS avant lundi 9:00, je diffuserais la vidéo à tous tes proches »

« Les garçons sont dégueulasses avec leur classement des moches, ignore-les. »

« J'adore ton style, tu m'as l'air vraiment gentil... »

Ciblage et usurpation d'identité

En utilisant les nombreuses fuites de données (entreprises, administration) ainsi que les données accessibles publiquement ou par le biais d'un·e proche déjà piraté, les pirates vont cibler et adapter l'attaque afin de viser des personnes vulnérables OU d'éviter la méfiance en se faisant passer pour d'autres.

« Salut Sam, je me suis fait volé mon tel, voici mon nouveau numéro 07 XX XX XX XX, A+ Tim. »

« Bonjour Mr Dupont, je suis Tom du service commercial Free, vous utilisez actuellement un abonnement à 2€/mois pour votre smartphone Galaxy S9. Pour le black friday, Free vous propose l'option appel illimité pour seulement 1. »

« Vérifiez dès à présent la date de péremption de votre coupon PCS. Vérifier mon coupon
Merci de votre confiance
TRANSCASH » (venant d'un autre mail) »

Coïncidence

Certaines attaques de phishing de masse se base sur le fait qu'un faux SMS de suivis de colis tombera quelques jours après une commande en

ligne.

« Colissimo : Votre colis ne peut être livré. Veuillez régulariser les frais de 2,99€ sous 24h pour éviter le retour. Suivre mon colis »

Contenus inadaptés ou dangereux

Porno

Quand on parle de contenus pour adulte, la plupart des gens pensent immédiatement à la pornographie essentiellement vidéo. Il convient toutefois d'élargir cette représentation car **la pornographie peut aussi prendre la forme d'écrits, de jeux vidéos ou de tchats** qui peuvent parfois sembler plus anodins.

Selon l'Arcom et les données de Médiamétrie, plus de la moitié des garçons de 12 ans se rend en moyenne chaque mois sur ces sites.