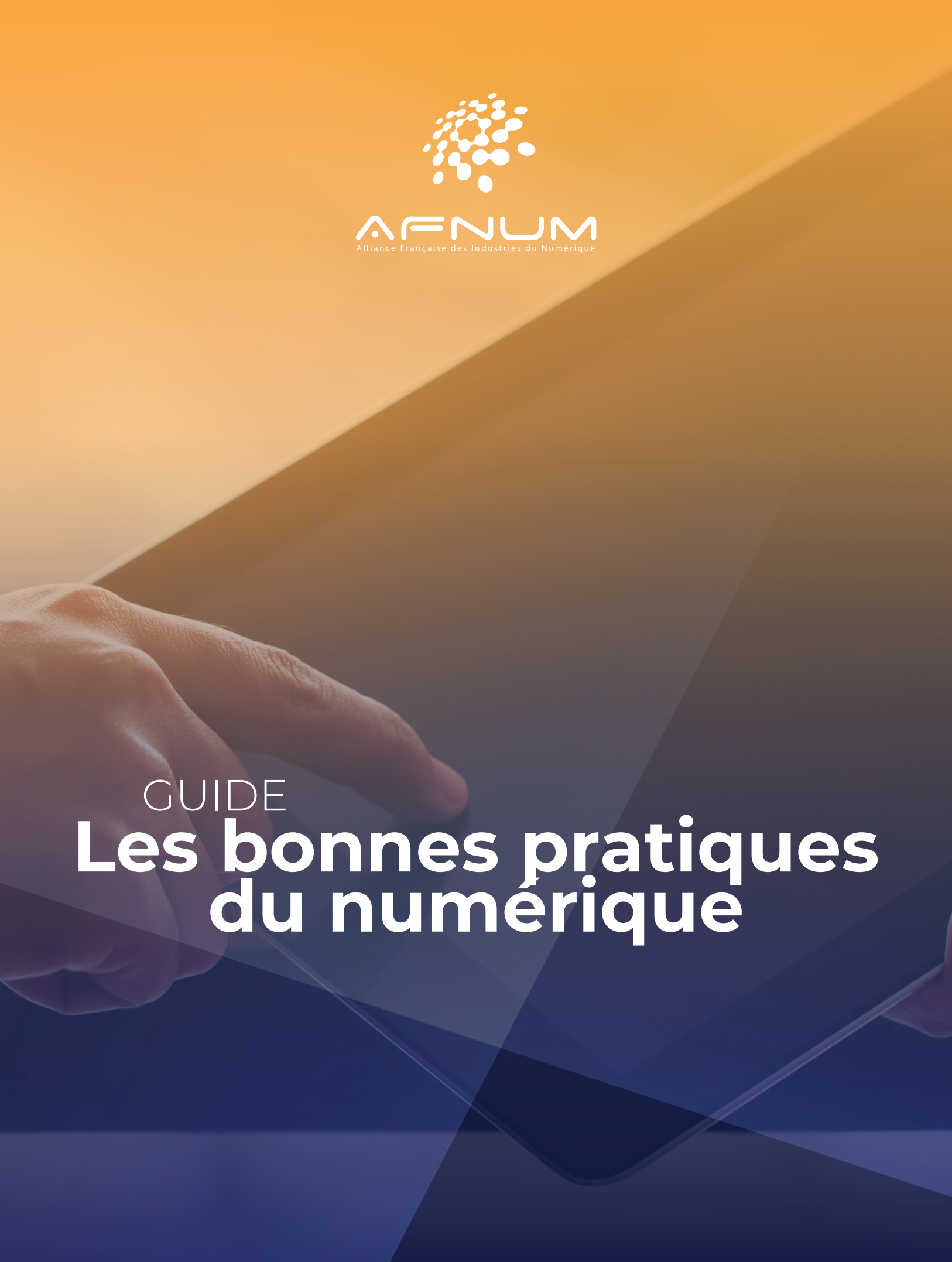
AFNUM
Alliance Française des Industries du Numérique



GUIDE

Les bonnes pratiques du numérique

ÉDITO
Mot de la présidente

Florence ROPION
Présidente de l'AFNUM
Vice-Présidente de Dell Technologies France

Le numérique occupe une place de plus en plus importante dans notre société, ce qui nous oblige aujourd'hui à redéfinir une perspective collective. Car le numérique ne se contente pas de transformer nos modes de vie, il modifie profondément la société elle-même, touchant à l'éducation, au travail, à la santé et à la vie citoyenne. Cette révolution pose des questions essentielles : comment garantir la sécurité des données personnelles dans un monde ultra-connecté ? Comment préserver la santé des utilisateurs et encourager des usages raisonnés, en particulier pour les plus jeunes ? Comment répondre aux préoccupations légitimes de ceux qui craignent un numérique qui divise autant qu'il rapproche ?

À ces défis, des réponses politiques et législatives ont été apportées. Pourtant, une crainte persiste parmi les citoyens : celle d'un numérique envahissant et potentiellement dommageable. Certains en appellent même à un recul de l'usage des technologies pour protéger la société. Mais faut-il, pour répondre à ces inquiétudes, envisager de freiner l'innovation ?

Ce serait négliger la contribution unique du numérique en matière d'émancipation personnelle, d'inclusion sociale et de dynamisme économique. Dans tous les domaines, le numérique élargit l'horizon des possibles, tout en transcendant les barrières géographiques.

Face à cette tension entre progrès et préservation, l'AFNUM, en tant qu'acteur engagé, propose le présent Guide de bonnes pratiques comme une boussole pour naviguer dans le monde numérique en toute confiance. À travers neuf fiches thématiques, ce Guide fournit des conseils clairs et accessibles pour assurer la meilleure utilisation possible du numérique par tous les Français.

Ensemble, faisons du numérique un espace de progrès au service d'une société plus juste et plus durable !

Ensemble, donnons du sens au numérique !

Le sommaire

1 PROTÉGER SES ENFANTS DANS LEURS USAGES NUMÉRIQUES

2 PROTÉGER SES APPAREILS ET SES DONNÉES

3 PROTÉGER SA SANTÉ

Présentation de l'AFNUM

QUI SOMMES-NOUS ?

INNOVATION
RESPECT
PARTAGE

L'Alliance Française des Industries du Numérique est un collectif unique d'entreprises, représentatif de toute la chaîne de valeur de notre filière. Notre diversité est le miroir de celle qui compose **le socle numérique industriel français, riche de ses technologies, de ses métiers et de ses compétences.** Ce socle est au cœur des enjeux du futur, car demain nécessitera plus de transparence, de responsabilité et de sécurité dans tous les secteurs. Nous pensons aussi que le socle numérique constitue la base d'un futur attractif pour la société, réducteur d'empreinte carbone et durablement porteur de valeur.

Nous croyons que :

- le numérique irrigue tous les secteurs et transforme tous les usages.
- le numérique doit être utile, simple et sûr.
- le numérique doit se placer au service du progrès économique, social et environnemental.
- l'innovation, au cœur du numérique, améliore le quotidien, favorise l'inclusion et contribue à la protection de l'environnement.
- pour apporter des solutions ambitieuses à ces défis, nos entreprises doivent s'engager et agir ensemble.

Pour toutes ces raisons, **nous pensons** qu'il est essentiel pour nous de **contribuer à répondre aux défis du numérique.**
De représenter nos adhérents dans toutes les instances liées à leur profession.
De simplifier l'interface avec les pouvoirs publics.
De fédérer un écosystème dynamique.
De constituer un ensemble puissant, fort de nos ambitions et de nos compétences.
De fonder, ensemble, les produits, applications et usages du futur.
De soutenir toutes les industries et entreprises qui progressent, rayonnent et innovent pour le bien collectif.

Ensemble, nous formons une **communauté d'experts, de leaders, de passionnés, d'éclaireurs,** déterminés à porter d'une seule voix la vision de nos entreprises auprès de l'écosystème numérique et des pouvoirs publics.

Nos actions sont le reflet de nos valeurs :

Nous promouvons l'innovation numérique responsable, en nous impliquant sur des thématiques transversales et sociétales au travers de nos groupes de travail verticaux.

Nous partageons des informations à valeur ajoutée qui sont le reflet de notre expertise numérique, auprès de nos adhérents et des pouvoirs publics, pour contribuer ensemble à la bonne évolution du numérique.

L'Alliance que nous formons est à la fois **unique et collective**, **agile et pragmatique**, **engagée et influente**.

ADHÉRENTS


AIRBUS DEFENCE & SPACE
ALCAD
amazon
ART-Fi
aws
brother at your side
cae GROUPE
Canon
cisco
Continental
CROSSCALL
DELL Technologies
DOCUP
Dolby
DXOMARK
EPSON
ERARD®
ERICSSON
FRACARRO
FUJIFILM
Google
hp
Hewlett Packard Enterprise
IBM
intel
Kodak alaris
Leica
Lenovo
Lexmark
LG
Microsoft
MobiWire
Nikon
NOKIA
OM SYSTEM
OPTEX
Panasonic
quadient
Qwant
RICOH imagine. change.
SAMSUNG
SEQUANS
SERVIMAT
SIGMA
SONY
TAMRON Focus on the Future
TCL
Televes
TETENAL
UNITRON GROUP
Verbatim
VITEC IMAGING DISTRIBUTION
Western Digital
WISI
xiaomi

1 Accompagner son enfant dans l'usage des outils numériques

Le numérique façonne les expériences de nos enfants bien avant qu'ils aient pleinement conscience des conséquences de leurs interactions en ligne. Face à cette immersion précoce, il est essentiel de développer une véritable culture numérique en famille pour que ces usages s'inscrivent dans un cadre sain et réfléchi. Mais cette approche ne doit pas se limiter à des règles ou des restrictions ; elle doit reposer sur une vision qui articule communication, éducation et autonomie progressive, dans un contexte où chaque parent joue un rôle de guide.

96 %
des mineurs possèdent au moins un équipement numérique[1]

1h17
de temps d'écran moyen par jour la semaine (plus de 2h les jours de week-end)

Construire un dialogue sur le numérique au sein du foyer familial

Le dialogue autour du numérique ne se réduit pas aux mises en garde ou aux consignes coercitives. Il s'agit davantage, pour chaque parent, d'accompagner son enfant dans une réflexion plus large, qui questionne le sens des outils numériques et les implications de leurs usages et des risques liés à ces derniers (cyberharcèlement, accès à du contenu inapproprié, etc.). Sensibiliser les enfants, c'est d'abord les aider à comprendre les valeurs et limites éthiques et morales qui devraient guider leur comportement en ligne : respect de la vie privée, discernement face à l'information et responsabilité vis-à-vis de toute forme d'interaction numérique. Discuter de ces questions permet d'installer les bases de la citoyenneté numérique au sein de laquelle chaque enfant doit se sentir à la fois accompagné et responsabilisé..

Je protège mon **enfant**

La plateforme officielle «Je Protège Mon Enfant» : Développée en partenariat avec des acteurs publics et privés sous l'égide du Secrétariat d'Etat en charge de l'Enfance et des Familles du Secrétariat d'Etat chargé de la transition numérique et des communications électroniques, de l'ARCEP et de l'ARCOM, cette plateforme regroupe des outils et des conseils pratiques pour éclairer les familles dans le cadre de leur parentalité numérique. Nous les invitons à se familiariser avec ces ressources pour mieux protéger les enfants grâce au site web Je Protège Mon Enfant.

[1] *Gouvernement - Campagne nationale de sensibilisation à la parentalité numérique, Pour un usage raisonné des écrans par les enfants, 2023*

Sélectionner un contenu numérique adapté et éducatif

Le numérique possède de nombreuses vertus pour les enfants. Son usage doit être enrichi par des contenus qui stimulent l'imaginaire et encouragent l'apprentissage. Loin de la consommation passive, le numérique est un levier d'épanouissement intellectuel pour les jeunes, à condition que les parents veillent à orienter leurs enfants vers des outils qui attisent leur curiosité et renforcent les compétences essentielles. Le choix de contenus ludo-éducatifs doit s'appuyer sur une réflexion qui place l'enfant au centre de son apprentissage, tout en lui offrant une diversité de points de vue pour former son esprit critique et créatif.

Définir des limites de temps d'écran pour favoriser la déconnexion

Dans le cadre d'une approche globale, le contrôle du temps d'écran est un outil qui doit préserver des moments de déconnexion.

La mise en place de règles claires, préalablement établies avec l'enfant l'aideront à adopter un rapport beaucoup plus sain aux technologies. Voici quelques exemples de bonnes pratiques en matière de gestion du temps d'écran :

1. Utiliser des outils de limitation du temps d'écran : la plupart des smartphones, consoles, ordinateurs et tablettes proposent une solution de paramétrage permettant de déterminer une heure ou durée limite d'utilisation du terminal et/ou de certaines applications. Un rappel est envoyé quelques minutes avant le blocage. Il est également possible d'accéder aux statistiques d'utilisation du terminal pour évaluer de manière éclairée le temps passé par les enfants sur ce dernier.

2. Instaurer une routine d'arrêt des écrans : mettre en place un horaire fixe d'arrêt quotidien des écrans ou imposer la non-utilisation des écrans un jour ou un moment précis (au coucher, pendant les repas, ...) permet de créer des repères pour l'enfant et de favoriser l'acceptation de la règle.

3. Déterminer la durée d'utilisation des écrans en fonction de l'âge, en se basant par exemple sur les préconisations du psychologue Serge Tisseron[2] :

- Avant 3 ans : pas d'écran
- De 3 à 6 ans : temps d'écran très limité
- De 6 à 9 ans : temps d'écran limité et spécifiquement dédié à des outils ludo-éducatifs
- De 9 à 12 ans : encourager son enfant à gérer son temps d'écran distractif en l'invitant à utiliser un « carnet du temps d'écran ».

[2] *Serge Tisseron, 3-6-9-12 Pour un développement numérique durable, 2013*

2 Utiliser des outils de **contrôle parental**

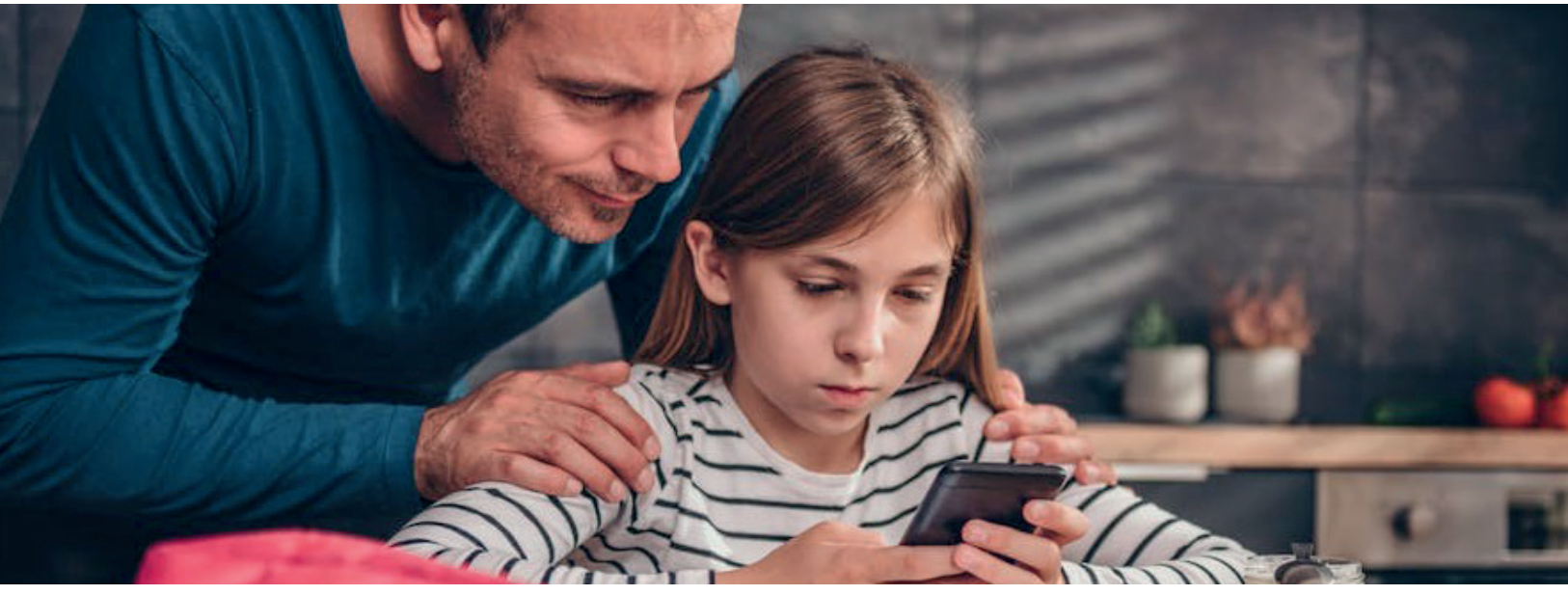
Pour tenir les enfants à l'abri des contenus préjudiciables ou pouvant heurter la sensibilité des plus jeunes, les fabricants de terminaux numériques proposent gratuitement des outils de contrôle parental efficaces et simples à paramétrer par les parents. Depuis l'entrée en vigueur de la loi «Studer» le 13 juillet 2024, ces outils doivent être activables dès l'initialisation d'un équipement donnant accès à internet (les smartphones, les tablettes ou les ordinateurs par exemple).

Les outils de contrôle parental

Les outils de contrôle parental permettent de restreindre, pour les comptes enfants, l'accès aux applications ou l'affichage de sites Internet non adaptés à leur âge. Cette limitation les protège des services conçus pour les adultes ou qui affichent des contenus violents ou pornographiques.

La plupart des outils de contrôle parental permettent une gestion encore plus fine des applications auxquelles l'enfant peut accéder en donnant la possibilité à l'adulte responsable de choisir une à une les applications auxquelles l'enfant peut accéder. En outre, lorsqu'un compte utilisateur a été paramétré en ligne par l'adulte pour son enfant, le blocage des applications et contenus peut s'appliquer sur les différents appareils à sa disposition : smartphones, tablettes, ordinateurs, smart TVs ... Cela peut éviter au parent d'avoir à configurer le contrôle parental sur chacun des terminaux du foyer et assure une sécurité renforcée.

Enfin, la fonction de filtrage des applications et des contenus intégrés dans les terminaux peut être regroupée avec d'autres fonctionnalités utiles à la gestion de l'utilisation du numérique, comme le contrôle du temps d'écran



Contrôle de l'âge sur les sites et applications

En complément des outils de contrôle parental, il est essentiel que les éditeurs de sites Internet et d'applications proposant des contenus interdits aux mineurs contrôlent l'âge des utilisateurs.

Depuis l'adoption de la loi visant à sécuriser et à réguler l'espace numérique du 21 mai 2024, les éditeurs de sites Internet et d'applications proposant des contenus interdits aux mineurs ont l'obligation légale de contrôler l'âge de leurs utilisateurs. Cette dernière obligation devrait être effective prochainement à la suite de la publication récente d'un référentiel technique par l'ARCOM[3] permettant de contrôler l'âge des utilisateurs de manière efficace.

A savoir

Cyberharcèlement

Au-delà des contenus préjudiciables qu'ils peuvent trouver en ligne, les jeunes peuvent également faire face à des situations de cyberharcèlement et de haine en ligne, notamment sur les réseaux sociaux et les forums. L'association e-enfance/3018 s'est emparée de cet enjeu en créant le 3018, un numéro d'appel gratuit, anonyme et confidentiel, accessible 7j/7 de 9 heures à 23 heures. Il est également accessible via l'App 3018, disponible sur tous les smartphones (iOS et Android) et directement téléchargeable depuis le magasin d'applications de votre appareil. Par téléphone ou par tchat, les écoutants psychologues ou juristes du 3018 répondent aux jeunes victimes de harcèlement et de cyberviolences, mais aussi aux parents pour les accompagner dans la parentalité numérique. Signaleur de confiance auprès des principaux réseaux sociaux, plateformes et sites internet, le 3018 permet de signaler des comptes ou contenus préjudiciables et d'obtenir leur suppression en quelques heures.

Lien du site : https://e-enfance.org/informer/cyber-harcelement/

[3] *ARCOM, 2024, Référentiel déterminant les exigences techniques minimales applicables aux systèmes de vérification de l'âge mis en place pour l'accès à certains services de communication au public en ligne et aux plateformes de partage de vidéos qui mettent à disposition du public des contenus pornographiques*

3 S'authentifier de manière sécurisée

L'utilisation en hausse de services en ligne s'accompagne de la création de nombreux comptes pour l'accès à des sites Internet et à des applications mobiles. Les données qui y sont stockées peuvent être sensibles, notamment lorsqu'elles ont trait à l'identité ou aux informations bancaires de l'utilisateur. Aujourd'hui, selon l'opérateur Verizon, 81 % des notifications de violations de données dans le monde impliqueraient un mot de passe compromis. L'utilisation de méthodes d'authentification robustes et sécurisées devient donc de plus en plus importante. Voici quelques bonnes pratiques à adopter pour protéger de manière efficace ses comptes personnels et les données qui y sont associées :

Créer un mot de passe robuste

Un mot de passe faible (par exemple « 123456 ») peut être piraté en quelques secondes seulement, tandis qu'un mot de passe respectant l'ensemble des paramètres de robustesse (par exemple « w25];Xyp DL9=A# ») mettra de nombreuses années à être déchiffré.

Les quatre caractéristiques d'un mot de passe robuste sont :

1. La longueur : 14 caractères minimum
2. La complexité : combinaison de majuscules, minuscules, chiffres et symboles
3. Le caractère aléatoire : pas d'information personnelle (nom, prénom, date de naissance, ville, etc.)
4. L'unicité : il doit être lié à un compte uniquement, ne pas être réutilisé

De nombreux sites web existent pour créer aléatoirement des mots de passe robustes tels que www.motdepasse.xyz. La CNIL a également développé un outil certifiant la robustesse d'un mot de passe[4].

Enfin, une attention toute particulière doit être portée à la robustesse du mot de passe dirigeant vers certains services majeurs, notamment la messagerie électronique, l'identité numérique (FranceConnect), et les applications bancaires.

Changer régulièrement ses mots de passe et se déconnecter simultanément de tous les appareils

Bien que la règle de ne jamais divulguer ses mots de passe à un tiers soit primordiale, il convient également de ne jamais conserver un même mot de passe trop longtemps, surtout pour les comptes les plus sensibles.

Ainsi, un certain nombre de sites et applications imposent une date d'expiration au mot de passe, contraignant l'utilisateur à le changer régulièrement afin de conserver l'accès à son compte. Pour plus de sécurité encore, cette manipulation devrait être réalisée de manière délibérée par l'utilisateur sur tous ses comptes, idéalement tous les six mois. Le déverrouillage des appareils électroniques (smartphones, ordinateurs) est également concerné, notamment dans la mesure où la robustesse des mots de passe est souvent plus faible.
Quand la possibilité est offerte par le site web ou l'application concernée, il convient aussi de privilégier la déconnexion automatique de tous les appareils, ce qui permet d'éviter l'accès d'utilisateurs tiers à un compte authentifié par le passé sur un autre appareil.

[4] *CNIL,2017, Les conseils pour un bon mot de passe*

La consultation fréquente de l'historique de connexion, accessible depuis les paramètres de la plupart des sites et applications, est utile pour déterminer la provenance géographique et la nature du support utilisé pour accéder aux comptes au cours des dernières semaines.

Utiliser un gestionnaire de mots de passe

L'utilisation d'un gestionnaire de mots de passe – aussi appelé « coffre-fort numérique » – est particulièrement utile pour faciliter la vie des utilisateurs et conserver l'ensemble des mots de passe utilisés. Son fonctionnement est simple : le gestionnaire stocke les mots de passe de l'utilisateur, qui ne doit en retenir qu'un seul, celui qu'il utilisera pour le déverrouiller. Certains gestionnaires proposent également une fonctionnalité de création de mot de passe robuste.

L'utilisation d'un gestionnaire est un bon réflexe qui permet d'éviter la conservation des mots de passe à l'écrit ou sur un fichier facilement accessible sur le terminal de l'utilisateur (un document word ou un post-it par exemple).

La plupart des éditeurs de systèmes d'exploitation ou de navigateurs Internet proposent un système embarqué de gestion de mots de passe. Cela permet de faciliter leur utilisation.

Utiliser la biométrie

La plupart des terminaux numériques proposent aujourd'hui des systèmes d'authentification par biométrie (empreinte digitale, reconnaissance faciale, etc.). Cette méthode est plus sûre qu'un mot de passe et surtout plus rapide et facile à utiliser.

La biométrie se combine souvent avec un mot de passe, dans les contextes où la reconnaissance est difficile (luminosité, humidité, etc.). Cela permet également des vérifications de sécurité, notamment basées sur un mécanisme d'authentification multi-facteurs.

Privilégier l'authentification multi-facteurs

Le mécanisme le plus fiable de protection des comptes est celui de la multi-authentification, aussi appelée «vérification en plusieurs étapes», qui permet de réduire de 99,9% les risques de compromission[5]. Contrairement aux mécanismes d'authentification classique comme le mot de passe unique, l'authentification multi-facteurs rajoute une ou plusieurs étapes de vérification de l'identité de l'utilisateur. Ainsi, même si le mot de passe est compromis, la couche de sécurité supplémentaire empêche un accès non-autorisé aux services. Cela peut être réalisé par biométrie, envoi d'un code ou lien par mail, validation dans une application tierce, etc.

La multi-authentification se base souvent sur une combinaison entre un élément que connaît l'utilisateur (par exemple un code), et un élément qu'il possède (par exemple une empreinte, une clé USB, un carnet de codes) ou qu'il reçoit sur son terminal (code reçu par email ou SMS).

[5] *Microsoft, 2024, Stratégie d'accès conditionnel courante : exiger l'authentification multifacteur pour les utilisateurs*

4 Gérer et conserver correctement ses données

L'usage quotidien d'appareils numériques implique la génération d'un grand nombre de données. Certaines sont sensibles (informations bancaires ou identité) et doivent donc être stockées de manière sûre. Les solutions de stockage existantes présentent un degré de sécurité variable. Par ailleurs, les bonnes pratiques à adopter reposent sur une utilisation conjointe de supports différents.

Types de stockage des données existants

1. Stockage physique

Les données peuvent être stockées en local sur le terminal ou bien répliquées sur des supports externes (clé USB, disque dur).

AVANTAGES

- L'accès et la gestion des données se réalise en mode hors ligne, une connexion Internet n'est pas nécessaire ;
- Les coûts sont limités à l'achat du support, pour une utilisation illimitée, dans la limite du stockage disponible.

INCONVÉNIENTS

- Possibilité de perte partielle ou totale des données en cas de support endommagé ou de vol ;
- Impossibilité d'accéder aux fichiers à distance et de les partager à distance avec des tiers.

2. Cloud

Il s'agit de stocker les données sur des serveurs distants, accessibles sur Internet. Ces serveurs sont hébergés dans des centres de données (data centers).

AVANTAGES

- Une capacité de stockage modulable selon les besoins ;
- Des données accessibles depuis n'importe quel appareil numérique connecté à Internet ;
- Un accès aux données très sécurisé, notamment chez les fournisseurs utilisant le chiffrement de bout en bout ;
- Une conservation des données garantie, même en cas de problèmes techniques des serveurs, du fait de la duplication des données dans des data centers différents (redondance).

INCONVÉNIENTS

- Nécessite selon l'espace de stockage un abonnement mensuel ou annuel qui peut s'avérer sur le long terme plus coûteux qu'un stockage physique ;
- Risque de piratage à distance permettant à des individus malveillants d'accéder aux données si le compte est mal protégé (voir Fiche 3 - S'authentifier de manière sécurisée) ;
- Nécessite un accès à Internet pour accéder aux données stockées ou pour les mettre à jour.

Bonnes pratiques de sauvegarde et de gestion des données

1. Sauvegarder régulièrement ses données sur plusieurs supports : pour se prémunir du vol d'un smartphone ou d'un ordinateur, la sauvegarde hebdomadaire ou mensuelle des données qu'ils stockent (fichiers, photos, etc.) est un bon réflexe. Le suivi de la règle du « 3-2-1 » est un réflexe facile à mémoriser : 3 copies ; 2 types de supports (cloud et stockage physique) ; 1 copie hors du domicile.

2. Utiliser et conserver adéquatement ses supports physiques de stockage : les fortes variations de température ou d'humidité peuvent sérieusement endommager les supports de stockage, d'où le besoin de les conserver en sécurité dans un endroit de préférence sec, sombre et frais. Vérifier fréquemment leur état permet d'éviter les risques de panne. De même, pour se prémunir de tout risque de virus, déconnecter son support de stockage de manière sécurisée dès la fin de son utilisation est un bon réflexe.

3. Pour plus de facilité, privilégier les solutions Cloud directement embarquées : les systèmes d'exploitation installés sur les smartphones et ordinateurs offrent la possibilité directe de stocker les fichiers et données en ligne dès leur création. Cette solution est utile pour se passer d'une première étape de sauvegarde régulière.

Sources : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes

5 Mettre à jour ses logiciels et son système d'exploitation

De nombreux secteurs ont vu apparaître au cours des dernières années des objets connectés (smartphones, smart TV, jouets connectés, montres connectées, ampoules connectées, etc.…). Cette tendance entraîne une augmentation du nombre de mises à jour à réaliser. Renforçant la sécurité des appareils, facilitant leur utilisation ou ajoutant de nouvelles fonctionnalités, les mises à jour sont devenues des opérations essentielles au bon fonctionnement de nos appareils. Voici quelques conseils et bonnes pratiques à adopter pour s'assurer que vos appareils bénéficient toujours des dernières fonctionnalités :

Recenser l'ensemble de ses objets connectés

Afin de s'assurer que ses appareils soient bien à jour, il convient de savoir lesquels d'entre eux sont connectés et nécessitent donc une attention particulière. Ainsi, certains appareils comme les ampoules, les frigos ou les téléviseurs peuvent être concernés par des mises à jour, sans que cela ne paraisse pour autant intuitif. Afin de procéder à l'inventaire de ses équipements connectés, il est possible d'utiliser des applications fournies par les fournisseurs d'accès à Internet qui permettent de visualiser en un coup d'œil l'ensemble des objets connectés au réseau local.

Procéder à la mise à jour le plus rapidement possible

Lorsqu'une mise à jour est disponible, elle est généralement proposée à l'utilisateur dès qu'il utilise l'appareil ou l'application. Si ce n'est pas le cas, l'utilisateur peut se rendre directement sur le magasin d'applications de son appareil pour accéder à la liste des mises à jour à effectuer. Il est vivement recommandé que toutes les mises à jour soient installées dès que possible et ceci même si un redémarrage de l'appareil est nécessaire. Outre un meilleur fonctionnement du produit, les mises à jour apportent leurs lots de correctifs de sécurité qui s'avèrent essentiels si l'on souhaite protéger correctement ses données.

Activer la recherche et l'installation automatique des mises à jour

Si les mises à jour sont bien proposées aux utilisateurs dès leur disponibilité, il est possible que celles-ci soient uniquement présentes dans les paramètres de l'appareil. Afin d'éviter de passer à côté d'une mise à jour, il est recommandé de configurer la recherche et l'installation automatique des mises à jour. Certains appareils proposent cette fonctionnalité par défaut, tandis que pour d'autres, une activation manuelle dans les paramètres sera nécessaire.

Rechercher les mises à jour uniquement sur le site officiel du fabricant

Si la plupart des produits intègrent dans leurs interfaces un onglet propre aux mises à jour (via le système d'exploitation ou l'application "Paramètres"), il est parfois nécessaire d'aller chercher directement la mise en jour sur Internet. Par exemple, sur les ordinateurs, certains « drivers » (logiciels permettant le fonctionnement de composants comme les cartes graphiques ou les cartes son) nécessitent de passer directement par le site du fabricant afin de télécharger les

mises à jour. Dans ce cas, il est primordial de bien vérifier que le site en question est le site officiel du fabricant de l'appareil ou du développeur du logiciel. L'absence sur le site de mentions légales, l'absence de la mention "https" dans l'URL ou la présence de fautes d'orthographes peuvent être des indices que le site en question n'est pas fiable (voir Fiche 6 - Eviter les arnaques et les virus informatiques).

Planifier l'installation des mises à jour en dehors des périodes d'activité

S'il est possible d'automatiser l'installation des mises à jour, certaines notifications d'installation ou de téléchargement peuvent survenir à des moments inopportuns (lors de la rédaction d'un document, pendant un film, une partie de jeux-vidéo, etc.). Ainsi, les fabricants ont intégré dans la plupart des appareils une fonctionnalité permettant d'installer les mises à jour lors des périodes d'inactivité, notamment la nuit. Combinant automatisation et confort, il est recommandé d'activer cette fonctionnalité.

6 Eviter les arnaques et les virus informatiques

Si les mises à jour permettent de répondre à la plupart des risques, la sécurité informatique des équipements passe également par une vigilance et des comportements attentifs lors de la navigation en ligne.

Quelles mesures adopter pour se prémunir des risques d'escroqueries ?

Si les logiciels antivirus et les mises à jour logicielles permettent de se prémunir de la majorité des logiciels malveillants, certaines escroqueries continuent de prospérer et peuvent constituer une menace pour les données personnelles et/ou professionnelles.

Afin de s'en prémunir, il est conseillé d'adopter les mesures suivantes :

- Toujours bien vérifier l'adresse d'expédition lorsque l'on reçoit un mail, même s'il provient d'un expéditeur a priori sûr (entreprises, administrations etc..). Par exemple, un mail d'une administration doit toujours se terminer par « .gouv.fr ». Les fautes d'orthographe ou la formulation employée peuvent également être une piste permettant de différencier un faux mail ou sms d'un vrai.

- Lors des achats en ligne, bien vérifier que le site Internet affiche une adresse qui commence par « https » et qu'elle est bien précédée d'un cadenas. Ces mentions indiquent que la connexion est sécurisée et qu'elle ne peut être affectée par des utilisateurs tiers.

- En cas de doute, même infime, sur l'origine d'un mail ou d'un sms, il convient de ne jamais cliquer sur les liens et de ne jamais ouvrir les pièces jointes.

- Ne jamais envoyer d'argent ou des renseignements bancaires sur les sites de rencontre, réseaux sociaux et applications de messagerie. De la même manière, il ne faut jamais encaisser un chèque d'une source inconnue, même en échange d'un futur transfert d'argent.

- Se méfier des réseaux Wi-Fi inconnus comme comme les Wi-Fi publics (accessibles sans code ou via une simple inscription).

- Activer le filtre anti-escroquerie proposé par le navigateur Internet.

- Sauvegarder régulièrement ses données. Certaines attaques pouvant faire disparaitre ou verrouiller les données, les sauvegardes permettent de les récupérer.

- S'inscrire sur le registre Bloctel afin d'empêcher les démarchages téléphoniques qui bien souvent sont des escroqueries.

- Reconnaître les indicatifs téléphoniques utilisés pour le démarchage : les 12 préfixes réservés aux démarcheurs en France métropolitaine sont les suivants : 0162, 0163, 0270, 0271, 0377, 0378, 0424, 0425, 0568, 0569, 0948 ou 0949. Si une personne voit l'un de ces numéros apparaître, celle-ci peut s'attendre à du démarchage téléphonique.

Que faire en cas d'attaque ?

Malgré toutes les mesures adoptées pour se prémunir des arnaques en ligne, une erreur peut survenir. Dans une telle situation, la première des réactions à avoir est de rester calme et d'adopter les gestes suivants :

- **Si vous pensez avoir été victime d'une arnaque ou d'une tentative d'intrusion** dans votre appareil, contactez directement l'organisme ou l'entreprise concernée pour s'assurer que le message/appel que vous avez reçu était bien officiel.

- **Déconnectez votre appareil du réseau local** : en attendant d'en savoir plus sur la nature de l'attaque, il est plus prudent de déconnecter l'appareil ciblé du réseau local (Wi-Fi, Ethernet) afin d'éviter que l'attaquant ne profite de cette connexion pour récupérer des informations stockées sur d'autres équipements.

- **Faites opposition** : peu importe la nature de l'escroquerie de laquelle vous pensez avoir été victime, si vous estimez que des données bancaires ont pu être compromises, faites immédiatement opposition auprès de votre banque/organisme financier.

- **Déposez plainte** : une fois une escroquerie établie ou si vous pensez que vos données personnelles risquent d'être utilisées pour une usurpation d'identité, déposez plainte auprès de la police/gendarmerie.

- **Modifiez l'ensemble de vos mots de passe** : si vous pensez que votre mot de passe a été compromis, changez-le immédiatement ainsi que l'ensemble des mots de passe équivalents ou proches de celui ayant été compromis (voir Fiche 3 - S'authentifier de manière sécurisée).

- **Conservez l'ensemble des preuves** : s'il peut être rassurant de supprimer le mail et/ou le document à l'origine de l'attaque, cette action ne fera que ralentir, voire complexifiera, le travail d'enquête de la police. De plus, cette suppression n'empêchera en aucun cas l'attaquant d'utiliser les données récupérées ou d'en récupérer de nouvelles en cas d'intrusion de logiciels malveillants (malwares) dans l'appareil. Laissez l'appareil en état et ne tentez pas de l'utiliser.

7 Comprendre et savoir utiliser **les outils d'intelligence artificielle**

Les récents progrès des systèmes d'intelligence artificielle ont donné lieu à des outils puissants qui peuvent servir à de nombreux usages dans l'éducation, la santé et la recherche d'information. Néanmoins, ces systèmes permettent de générer des textes, des images ou des vidéos d'une manière si réaliste qu'il est parfois difficile de savoir que ces contenus ont été créés par une machine. Or, ces derniers peuvent contenir des erreurs involontaires ou des manipulations. Il faut donc être vigilant dans leur utilisation.

Être vigilant face aux « hallucinations » des IA

Contrairement à ce que l'on pourrait penser du fait de son appellation, une intelligence artificielle (IA) n'est pas intelligente, du moins au sens où on l'entend pour un être humain. Lorsqu'elle répond à une demande ou à une question, par exemple « *Pourquoi Léonard de Vinci a-t-il peint la Joconde ?* », elle analyse d'abord l'ensemble des données à sa disposition, puis elle rédige une réponse en utilisant les mots et la grammaire qu'elle a également appris à partir de l'ensemble des textes d'une langue. Ayant accès à une quantité d'information très élevée, la réponse sera ainsi très étayée et reflétera généralement les connaissances disponibles à ce jour sur ce sujet.

Or, il arrive que certaines données utilisées par l'IA pour faire son travail soient fausses. Cela est notamment le cas lorsque l'IA n'a pas pris en compte les dernières connaissances disponibles sur un sujet (par exemple pour les dernières actualités ou les sujets qui ont fait l'objet de découvertes scientifiques très récentes). Cela peut aussi être le cas lorsqu'en fonction de la question posée, l'IA ne peut s'appuyer que sur un nombre limité de connaissances fiables à sa disposition, notamment pour les questions farfelues comme « Quelle est la capitale de la Lune ? ». Pour cette question, l'IA peut répondre en utilisant des théories ou des histoires fictives, mais en faisant comme si elles étaient vraies.

On appelle ces erreurs des « hallucinations » de l'IA et il faut s'attendre à en rencontrer lorsqu'on utilise ces outils. Pour éviter de se faire piéger, il ne faut pas hésiter à aller vérifier la réponse de l'IA à partir de sources fiables (sites institutionnels et gouvernementaux, médias reconnus, sites scientifiques et universitaires, encyclopédies).

Renforcer l'esprit critique face aux médias synthétiques

Les outils d'IA peuvent être utilisés par des personnes malveillantes pour manipuler d'autres personnes, en leur faisant croire que les images générées ou modifiées par l'IA sont authentiques. On parle aussi de « deep fakes ». Si le phénomène des « fake news », apparu avec les réseaux sociaux, n'est pas nouveau, il peut être amplifié par la facilité d'accès aux outils d'IA.

Comme pour les hallucinations de l'IA, le premier réflexe à adopter face à une image distribuée par Internet est de douter de son authenticité, notamment si l'image ou la vidéo est distribuée via les réseaux sociaux, les applications de messagerie ou des sites web n'appartenant pas à des médias reconnus. Il faut également éviter de partager les contenus sans avoir préalablement vérifié leur origine et leur authenticité. En outre, lorsque l'on crée soi-même des contenus grâce à une IA, il est important de le signaler expressément, par exemple avec la mention « Contenu créé par une IA ».

Les grands acteurs du numérique ont récemment mis en place un outil permettant aux producteurs de contenus et aux utilisateurs d'obtenir des informations plus détaillées sur les conditions de création des images ou vidéos : «Content Credentials». Cette technologie, disponible en open source, permet de savoir exactement d'où vient un contenu, qui l'a créé et quelles modifications y ont été apportées en cours de route. Celle-ci indique notamment si l'intelligence artificielle a été utilisée et de quelle manière. Il s'agit en quelque sorte d'une « étiquette nutritionnelle » numérique. Dans l'exemple ci-dessous, ces informations seront présentées en cliquant sur les références du contenu ou sur le logo « » .

Source : https://contentcredentials.org/

8 Protéger ses yeux et réduire la fatigue oculaire

L'utilisation quotidienne et intensive d'outils numériques et d'écrans sollicite fortement nos yeux, jusqu'à parfois donner une sensation d'inconfort visuel. Les symptômes sont facilement reconnaissables : vision trouble ou double, yeux rouges et secs, larmoiements, maux de têtes ... Cette situation est souvent le fait de trois mauvaises pratiques : une exposition prolongée aux écrans, une mauvaise ergonomie de travail et un éclairage inapproprié. Pour se prémunir le mieux possible de ces effets, quelques bons réflexes peuvent être adoptés :

Eviter l'exposition prolongée en faisant régulièrement des pauses

Pour limiter la sollicitation intensive des yeux et éviter les irritations oculaires, la solution la plus directe est de limiter l'exposition continue aux écrans. Pour cela, il est utile de mémoriser la règle du 20-20-20, développée au Canada : après 20 minutes d'utilisation d'un appareil numérique, il faut prendre 20 secondes de pause et regarder loin devant soi, à une distance de 20 pieds (6 mètres). Le respect de cette règle permet de réduire la fatigue et d'améliorer la concentration.

Le Haut Conseil de la Santé Publique recommande de réaliser régulièrement des pauses plus longues, notamment aux enfants : au moins 20 minutes toutes les 30 minutes à une heure[6].

Régler correctement l'écran

Le réglage de l'écran et la bonne disposition de l'environnement de travail sont cruciaux pour limiter la fatigue oculaire. Voici une liste de bonnes pratiques à adopter :

- Se placer à une distance d'au moins 50 centimètres de l'écran (davantage si l'écran est plus grand que celui d'un ordinateur portable ou d'un smartphone).
- Les yeux doivent êtres positionnés à la hauteur du haut de l'écran.
- L'écran doit être propre et loin des sources externes de lumières : empreintes digitales, poussière et lumière extérieure peuvent réduire la clarté et solliciter davantage le regard.

Utiliser les fonctionnalités en faveur de la santé visuelle embarquées dans les terminaux

L'usage de fonctionnalités embarquées dans les terminaux peut être un complément intéressant au correct réglage de l'environnement d'utilisation. Ainsi, plusieurs systèmes d'exploitation proposent d'activer un filtre anti-lumière bleue automatiquement sur l'écran. Le passage en mode nuit est également utile en cas de baisse de la luminosité extérieure. Enfin, certains terminaux sont spécifiquement conçus avec un écran façon papier (à l'image des liseuses) et garantis sans lumière bleue. A savoir que la lumière bleue, si elle est naturellement émise par le soleil, est susceptible, à forte exposition, de retarder l'endormissement et d'affecter la qualité du sommeil.

[6] *Haut Conseil de la Santé Publique, 2024, Effets de l'exposition des enfants et des jeunes aux écrans*

S'équiper de terminaux offrant un bon confort visuel

En plus d'appliquer les bons gestes au niveau individuel, il existe des labels permettant de distinguer les écrans garantissant un niveau de confort visuel élevé pour se prémunir au maximum des symptômes liés à la fatigue oculaire. C'est le cas notamment du label « Eye Comfort Display » développé par le laboratoire indépendant DXOMARK.

Ce label vise à garantir un confort visuel optimal de l'utilisateur, en certifiant le respect de critères de scintillement, de niveau de luminosité, de filtrage de lumière bleue et de cohérence des couleurs.

9 Utiliser le numérique tout en restant en bonne forme physique

En raison des nombreux avantages qu'ils offrent, notamment en termes de productivité et d'accessibilité, l'utilisation d'outils numériques dans nos activités quotidiennes et dans le cadre professionnel est de plus en plus intense. Ainsi, il convient d'adopter les bons gestes pour préserver sa santé et prévenir de potentiels inconforts posturaux.

La posture devant les écrans

Lorsque l'on reste trop longtemps assis devant un écran d'ordinateur, des douleurs musculaires peuvent s'installer. S'il ne semble pas exister de consensus scientifique sur la posture idéale, quelques bonnes pratiques sont à privilégier pour un travail confortable sur écran :

- Faire reposer les pieds à plat sur le sol ou sur un repose-pied.
- Garder les coudes proches du corps.
- Aligner ses mains avec les avant-bras.
- Garder le dos droit.
- Positionner l'écran à hauteur des yeux et à une distance suffisante, selon la taille de l'appareil (voir Fiche 8 - Protéger ses yeux et réduire la fatigue oculaire).
- Utiliser l'ensemble des doigts pour écrire sur le clavier.

L'illustration suivante préparée par l'INRS[7] résume la position qu'il est conseillé d'adopter devant son écran d'ordinateur :

© Odeka / L'un & l'autre pour l'INRS – 2021

[7] *INRS Institut national de recherche et de sécurité, 2023, Travail sur écran - Prévention des risques*

La **position debout** offre, quant à elle, de nombreux avantages tels qu'une grande liberté de mouvements et une zone de travail disponible plus large. En travaillant debout, l'ensemble des muscles sont sollicités, ce qui permet également de réduire les risques d'obésité. Pour cela, des bureaux réglables qui donnent la possibilité de travailler aussi bien assis que debout sont aujourd'hui largement disponibles dans les enseignes de mobilier.

Les outils numériques pour rester en forme

Certains outils numériques, comme les montres connectées et les trackers d'activité, apportent de nouvelles façons d'être actif et de suivre facilement l'état de sa santé[8].

Ces équipements possèdent certaines fonctions d'usage (chronomètre et notifications), de performance et surtout de santé. On trouve notamment les fonctions de :

- Cardiofréquencemètre : mesure de la fréquence cardiaque.
- Podomètre : calcul du nombre de pas quotidiens effectués.
- GPS : calcul de la distance parcourue.
- Calorimètre : calcul du nombre de calories brûlées.
- « *Sleep tracker* » : recueil des données de sommeil (durée, qualité, apnée…).

Ces fonctionnalités offertes par les objets connectés encouragent la pratique d'activités physiques et représentent de bons compléments aux efforts posturaux.

[8] Ces dispositifs ne sont toutefois pas destinés à être utilisés pour la détection, le diagnostic, le traitement, le suivi ou la gestion d'une condition médicale ou d'une maladie. Les mesures sont données à titre informatif et elles ne se substituent pas à la consultation d'un professionnel de santé.

L'AFNUM EN QUELQUES CHIFFRES

16
commissions & groupes de travail

60
adhérents

5 000
emplois en R&D

30Mds
d'euros de chiffre d'affaires cumulés

35 000
emplois directs

CONTACTS

Stella MORABITO
Déléguée Générale
smorabito@afnum.fr

Philippe de CUETOS
Directeur des Affaires Techniques et Réglementaires
pdecuetos@afnum.fr

Gabriel COLRAT
Chargé de mission Affaires publiques et Communication
gcolrat@afnum.fr

AFNUM
Alliance Française des Industries du Numérique

Guide - Les bonnes pratiques du numérique
17 rue de l'Amiral Hamelin - 75016 Paris
contact@afnum.fr - 01 45 05 72 25
www.afnum.fr
@AFNUM