isfec. François d'Assise
Formation initiale et continue aux métiers de l'éducation

pix — Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE

Culture numérique 4 – Emmanuel Vilbois

PROTECTION ET SECURITE

Sécuriser l'environnement numérique

Nos environnements numériques – ordinateur, tablette, téléphone portable… - contiennent désormais toute notre vie privée. Il est donc essentiel de savoir protéger ses données et sécuriser ses appels pour empêcher des risques tels que : les virus, le vol de données, l'endommagement…

Compétence numérique : sécuriser les équipements, les communications et les données pour se prémunir contre les attaques, pièges, désagréments…

Comment sécuriser son environnement informatique ?

A RETENIR

Les appareils électroniques contiennent des informations qui peuvent intéresser des personnes mal intentionnées. Pour éviter la perte ou le vol de données, les virus, les escroqueries, il est important de **sécuriser ses équipements, ses communications et ses données.**

Pour cela, il faut :

- vérifier les **mises à jour** de son ordinateur et de son logiciel antivirus.
- Choisir des **mots de passe** forts contenant des chiffres, des lettres et des caractères spéciaux. On peut pour cela utiliser un gestionnaire de mots de passes (ou trousseau).
- Dans sa messagerie, se méfier **des pièces jointes** ou des **liens douteux**, destinés à récupérer des données sensibles comme le nom d'utilisateur et les mots de passe (**hameçonnage**), ou à crypter les données de l'ordinateur contre une rançon (**rançongiciel**).
- Lors d'une connexion internet via une borne wifi publique (hotspot), où les informations ne sont pas chiffrées (cryptées), naviguer en priorité sur des sites Web qui utilisent le **protocole sécurisé HTTPS**.

Sources : cahier d'activités PIX (Delagrave) – Éducation au numérique (Nathan)

- Verrouiller son smartphone avec un mot de passe (**code PIN**), son empreinte digitale ou faciale.

La **sécurité informatique** est l'ensemble des techniques permettant de protéger **l'intégrité** et la **confidentialité** des informations stockées dans un système informatique, que ce soit du matériel ou un logiciel.

Il faut toujours prendre en compte quatre grands aspects :

- la **confidentialité** : il est nécessaire de protéger l'accès aux informations et aux données, pour que seules les personnes autorisées aient des droits ou permissions et ainsi empêcher tout accès indésirable.
- **L'authentification** : c'est le code ou mot de passe attaché à un identifiant unique et qui permet à un utilisateur de prouver qu'il détient bien l'autorisation d'accéder à cet environnement protégé. Il ne faut pas confondre identification et authentification.
- **L'intégrité** : les données doivent être exactes et complètes, il ne faut pas qu'elles soient altérées de manière fortuite, illicite ou malveillante.
- La **disponibilité** : les services et les ressources doivent être accessibles rapidement, de façon permanente et sans faille pour permettre un usage régulier.

Il est très important de savoir **identifier les principaux risques** qui menacent son environnement numérique et de mettre en place les **mesures de protection** appropriées.

Les principaux risques à connaître sont :

- le **virus informatique** : logiciel malveillant qui infecte un appareil et se propage ensuite à la manière d'un virus biologique. Il peut se répandre par tout moyen d'échange de données numériques : clé USB, disque dur externe, réseau informatique…
- Le **cheval de Troie ou « Trojan »** : sorte de logiciel malveillant qui au contraire d'un virus est légitime en apparence, mais qui contient une fonction malveillante dont le but est de la faire installer sur l'ordinateur à l'insu de l'utilisateur.
- Le **spyware** : logiciel espion qui s'installe sur un appareil, pour collecter et transférer des données sans que l'utilisateur le sache.
- Un **spam** : courrier électronique indésirable, en général ce sont des publicités envoyées en masse de manière automatique. Les fournisseurs de messagerie électroniques arrivent souvent à les filtrer et les tirer directement dans un dossier de « Courrier indésirable ».
- Le **phishing ou « rançongiciel »** : technique de hameçonnage qui consiste à se faire passer pour un tiers de confiance (banque, administration…) pour soutirer des données personnelles telles que mots de passe, numéro de carte de crédit, carte d'identité…

Les appareils numériques étant de plus en plus nombreux, les risques sur la sécurité informatique ne cessent d'augmenter. Des actions simples de prévention existent pour se protéger au mieux.

Voici les principaux gestes à adopter :

- **l'authentification** : protéger l'accès avec un mot de passe sécurisé.
  *Exemple : 8 caractères, au moins une majuscule, un chiffre et un caractère spécial (@, *, !, #).*

- **La confidentialité** : configurer les paramètres de confidentialité et de partage.

- ***L'antivirus*** *: pour contrer les logiciels malveillants et analyser les fichiers.*

- ***Le pare-feu*** *: filtre de flux qui empêche certains types de communications vers certains types de ports (tout système qui permet de recevoir ou émettre des informations).*

- ***Le contrôle parental*** *: pour sécuriser la navigation Internet des enfants et l'accès à certains types de contenus.*

A noter que parfois, il est difficile de se rendre compte à temps que la sécurité a été enfreinte, et alors les dégâts peuvent être considérables, voire irréversibles.

Exemple : quelques indices peuvent être la lenteur de l'ordinateur, la disparition de données, l'envoi automatique des mails…

Protéger les données personnelles et la vie privée

Les données personnelles circulent de plus en plus sur le Web. Les conséquences de leur piratage ou publication peuvent être catastrophiques, c'est pourquoi il est indispensable de savoir protéger ses données.

Compétences numériques : maîtriser les traces et gérer les données personnelles pour protéger sa vie privée et celle des autres et adopter une pratique éclairée.

Comment protéger sa vie privée sur internet ?

A RETENIR

Naviguer sur **internet** et se connecter aux **réseaux sociaux** laissent des traces sur les **serveurs**, si bien que des **données personnelles** peuvent être collectées.

Pour protéger sa **vie privée** il faut :

- connaître les Règlements Généraux sur la Protection des Données personnelles des citoyens (**RGPD**).
- Contrôler son **identité numérique** en vérifiant les informations sur soi présentes dans les moteurs de recherche et les réseaux sociaux.
- Vérifier **l'adresse de l'expéditeur** d'un courriel et signaler s'il est indésirable.
- Savoir effacer son **historique de navigation** et ses **cookies** (témoins de connexion).
- Maîtriser sa **géolocalisation**.

Tout d'abord, il faut bien comprendre la notion de **données personnelles** pour savoir identifier ce que l'on peut partager ou non et ce qui relève absolument de sa vie privée.

Chaque information peut se transformer en donnée personnelle, qui peut ensuite être **collectée, stockée, analysée** ou même revendue. Il faut donc veiller à protéger au mieux les informations que l'on partage en ligne.

Pour bien comprendre, il faut savoir qu'une donnée personnelle permet d'identifier une personne de plusieurs manières :

- **directement** : nom, prénom… ;
- **indirectement** : numéro de téléphone, ; adresse mail, numéro de sécurité sociale… ;
- à partir **d'une seule donnée** : le nom ou un identifiant ;
- à partir du **croisement d'un ensemble de données** : en croisant un prénom avec une adresse et une date de naissance.

Il est important de prendre consciences que toute action sur Internet laisse des **traces** ou **empreintes**, et que celles-ci, croisées avec d'autres informations, forment un ensemble de **données personnelles** qui contribuent à reconstituer une **identité numérique**.

Pour protéger sa vie privée, il convient de laisser le moins de traces possibles en surfant sur le Web.

D'ailleurs, il faut savoir qu'un internaute a des **droits**, notamment que ses données ne soient pas exploitées. Une donnée personnelle doit rester personnelle. Ainsi, depuis mai 2018, il existe une loi concernant la protection des données personnelles sur Internet, appelée **R.G.P.D : le Règlement Général de la Protection des Données**. Il s'agit d'un règlement européen destiné à augmenter la protection des personnes en **encadrant** la collecte, le stockage et le traitement de leurs données personnelles.

Les traces collectées permettant d'analyser les parcours, les requêtes, les achats ou encore les préférences. Grâce à ces données, les entreprises peuvent ensuite définir des **comportements** et élaborer des **modèles de prédiction** afin de mieux cibler et vendre leurs produits.

Grâce au nombre croissant de données, de nouveaux métiers sont apparus.
On trouve aujourd'hui des métiers spécialisés dans la collecte et l'analyse des données : le **data scientist** est un expert de la gestion et de l'analyse de données massives qu'on appelle **big data**. C'est un véritable scientifique qui maîtrise l'analytique, l'apprentissage automatique (**machine learning**), l'exploration de données (**data mining**) et l''analyse statistique.

Pour protéger au mieux ses données personnelles, il y a quelques règles élémentaires à suivre pour ainsi **limiter au maximum les traces** que l'on laisse en ligne :

- **Installer un antivirus** : pour éviter les virus et ainsi le vol de données ou encore l'usurpation d'identité ;

- **Identifier les courriers indésirables** : ne pas ouvrir les emails d'expéditeurs inconnus et les signaler au besoin comme contenus indésirables ou spams ;

- **Désactiver la localisation par défaut** : sur son mobile, ne configurer l'utilisation de la localisation par une appli qu'en cas de besoin ;

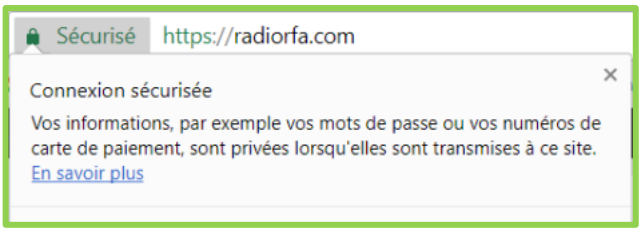
- **Nettoyer régulièrement son historique** : vider son cache (stockage temporaire) et son historique de navigation ;

- **Contrôler les cookies** : définir l'autorisation souhaitée des cookies sur son ordinateur lors de visite de sites et les supprimer régulièrement ;

- **Paramétrage de son profil** : communiquer uniquement les informations essentielles, configurer la confidentialité, utiliser si possible des peudos et une adresse mail non-nominative ;

- **Naviguer en privé** : choisir une fenêtre ou un onglet de navigation privée ; 

- **Vérifier la sécurité d'un site** : ne visiter que des sites connus et de confiance, dont l'url commence par « https:// » (S comme Sécurisé) ;



- **Lire les C.G.U** : lire avant d'accepter les Conditions Générales d'utilisation.

Protéger la santé, le bien-être et l'environnement privé

Les nouvelles technologies améliorent le quotidien mais il faut également prendre conscience des dérives possibles en termes de santé, de bien-être et même de l'impact néfaste que cela peut avoir sur l'environnement.

Compétences numériques : prévenir et limiter les risques générés par le numérique sur la santé, le bien-être et l'environnement.

Comment protéger sa santé et son environnement face au numérique ?

A RETENIR

L'utilisation des appareils numériques (ordinateurs, smartphones, tablettes, montres connectées…) a un impact environnemental non négligeable et peut avoir des conséquences néfastes sur la santé. La protection du bien-être et de la vie privée reste un enjeu important.

Il faut :

- savoir détecter des situations de **cyber violence** notamment de **cyber harcèlement** et y réagir.
- Être conscient des dangers de la **lumière bleue** et des ondes émises par les écrans et communications sans fil. La lumière bleue est néfaste pour la rétine. Les **normes DAS** (Débit d'Absorption Spécifique) contrôlent la quantité d'ondes émises par les appareils électroniques.
- Veiller à sa consommation de papier et d'encre et d'énergie pour limiter **l'impact sur l'environnement.**
- Utiliser sa messagerie électronique de façon responsable en limitant le nombre de destinataires et des pièces jointes dans un courriel car le **stockage** de tous les messages est très **énergivore**.
- Adopter une **bonne posture** sur son poste de travail pour limiter les **troubles musculo squelettiques** (TMS).

Sources : cahier d'activités PIX (Delagrave) – Éducation au numérique (Nathan)

L'utilisation excessive et non réfléchie des technologies numériques peut avoir des impacts négatifs sur la santé et l'équilibre social et psychologique.

Il est donc nécessaire de limiter les risques en ayant un **usage raisonné** des outils numériques.

Une utilisation excessive d'Internet peut produire un état de **manque** et des conséquences négatives : c'est ce qu'on appelle la **cyberaddiction** ou **cyberdépendance**.

On reconnait trois facteurs pour déterminer si une personne va trop loin dans sa pratique des écrans :

- elle ne peut pas s'empêcher de se connecter tous les jours ;
- elle sous-estime le temps passé et ne parvient pas à s'autoréguler ;
- surtout, elle délaisse sa vie réelle au profit du monde virtuel.

Le filtre de l'écran peut aussi nuire aux **rapports sociaux**, la dérive le plus grave étant le **cyberharcèlement**, ou harcèlement en ligne, qui correspond à une violence répétée, consistant à intimider ou à humilier une personne via Internet.

Pour préserver sa santé, il est essentiel d'adapter son espace de travail et de réguler ses pratiques. Il y a notamment un programme mis en place appelé **Safe Internet Day**, une journée mondiale de sensibilisation pour un Internet meilleur.

Exemple : limiter son temps de connexion par jour, limiter sa production de données ou ne plus avoir d'écran allumé à partir de 20h00.

Il est aussi nécessaire de savoir reconnaître les **comportements** et **contenus** qui relèvent du cyberharcèlement, qui se définit par différentes actions **répétitives** :

- envoi incessant de messages (SMS, mails, MP…) ;
- diffusion de photos ou de vidéos dégradantes pour la victime ;
- diffusion de photos intimes ;
- diffusion de rumeurs mensongères…

Après avoir considéré les technologies numériques comme une grande innovation, on s'aperçoit qu'elles consomment énormément d'électricité et que les données transitent par des datas centers très **énergivores**.

Pour réduire son **impact écologique**, on peut commencer par éteindre son appareil lorsque l'on ne s'en sert pas ou le mettre en mode « **économie d'énergie** ».

Les impacts du numérique sur la santé et le bien-être des utilisateurs peuvent être assez négatifs au niveau physique et psychique.

*Par exemple, en cas d'abus, donc de **cyberdépendance**, c'est tout l'équilibre social et psychologique qui peut être brisé. Le **sommeil** peut être perturbé et l'exposition continue aux **ondes** peut favoriser les maladies.*

Deux grandes approches pour se **protéger** sont à prendre en compte :

1°) **définir un temps d'écran** : pour éviter les risques d'addiction, les troubles du sommeil ou du comportement, on peut obtenir un rapport sur l'utilisation des applications et sites Web, tous écrans confondus (tablette, mobiles, ordinateur), grâce à la synchronisation du compte. On peut ainsi prendre conscience de son temps d'écran et le limiter.

2°) **Rendre le temps d'écran productif**
: ce qui permet également de se concentrer uniquement sur les choses essentielles en ligne (répondre à un mail ou faire des recherches pour un dossier)

Par exemple, il est plutôt recommandé de privilégier une application éducative que de regarder des vidéos sur TikTok…

Lorsqu'un internaute est victime de cyberharcèlement, il est essentiel d'en parler, à des proches ou des associations, que l'on soit victime ou témoin, pour extérioriser le problème et trouver des solutions.

Pour cela il existe des plateformes comme **Netecoute.fr et Nonauharcelement.education.gouv.fr** qui proposent une assistance gratuite et anonyme en ligne ou par téléphone respectivement au **0800 200 000** et au **3020**.

La **prise de conscience écologique** est en cours et les entreprises, dans la démarche **GreenTech**, commencent à développer des produits et services prenant en compte l'environnement.

Mais il est primordial que chacun contribue, à sa petite échelle, à réduire les impacts de la **pollution numérique** sur l'environnement par une action quotidienne.

Quelques bons gestes adopter :

- acheter du matériel économe et adapté, moins énergivore ;
- éteindre ou désactiver les appareils connectés lorsqu'ils ne sont pas utilisés ;
- faire le tri et supprimer d'anciens fichiers, emails… ;
- optimiser la taille des documents, en compressant les fichiers ou en optant pour des images en basse résolution.