5. Internet – Répondre aux défis actuels

> « Refuser de reconnaître leurs droits fondamentaux aux individus, c'est remettre en cause leur humanité même »
>
> *Nelson Mandela, lauréat du prix Nobel de la paix en 1993, militant antiapartheid, président de l'Afrique du Sud de 1994 à 1999*
>
> « Les droits de chaque individu sont amoindris si ceux d'un seul homme sont menacés »
>
> *John F. Kennedy, président des États-Unis de 1961 à 1963*

LISTE DE POINTS À VÉRIFIER :

19. CYBERCRIMINALITÉ : SPAM, LOGICIELS MALVEILLANTS, FRAUDE ET SÉCURITÉ

Avez-vous défini des mots de passe solides et différents pour chacun de vos comptes et mis en place une authentification à deux facteurs ?

Avez-vous étudié les paramètres de sécurité de vos appareils/comptes ?

Votre système d'exploitation et vos applications sont-ils à jour ?

Avez-vous effectué une sauvegarde de vos données les plus importantes ?

20. CLASSIFICATION/ÉTIQUETAGE ET FILTRAGE

Avez-vous réfléchi aux conséquences du filtrage au plan culturel et moral ?

Connaissez-vous la différence entre une « liste noire » et une « liste blanche » ?

Connaissez-vous les systèmes d'étiquetage/classification les plus couramment utilisés pour le contenu destiné aux enfants, et leur signification ?

21. HARCÈLEMENT EN LIGNE : INTIMIDATION, TRAQUE ET TROLLING

Votre famille ou votre établissement scolaire ont-ils mis en place des règles claires qui permettent aux enfants de comprendre les conséquences d'une éventuelle implication dans des actes de harcèlement en ligne ?

Protégez-vous suffisamment vos données personnelles ? De nombreux problèmes rencontrés en ligne résultent du partage inconsidéré de photos et d'informations.

Avez-vous cherché des moyens de développer votre intelligence sociale et émotionnelle pour surmonter les difficultés liées à l'anonymat des communications sur Internet, qui facilite de manière générale les actes d'intimidation, le trolling et le harcèlement ?

22. OBTENIR DE L'AIDE

Vos enfants/élèves savent-ils vers qui se tourner pour signaler des contenus illicites ?

Regardez-vous les statistiques fournies par les numéros d'urgence pour comprendre les nouvelles tendances et nouveaux risques dans le cyberespace ?

Quelles sont les cinq principales compétences numériques qui vous protégeront le mieux en ligne ?

Comprenez-vous suffisamment la géolocalisation et le Bluetooth pour utiliser vos appareils mobiles dans les meilleures conditions de confort et de sécurité ?

L'apprentissage mobile et les porte-monnaie électroniques sur appareils mobiles révolutionnent notre façon d'apprendre, de travailler et d'acheter. Que savez-vous de ces évolutions récentes ?

Fiche d'information 19

Cybercriminalité : spam, logiciels malveillants, fraude et sécurité

Internet est un moyen formidable d'accéder à des contenus et des services de qualité, mais il peut également être utilisé par des personnes mal intentionnées dans le but de commettre des escroqueries ou de diffuser du courrier indésirable, des virus et des logiciels malveillants.

- La **cybercriminalité** inclut les infractions contre les ordinateurs et les données, par exemple l'accès illégal à un ordinateur (également appelé piratage), l'interception d'une communication, le fait de bloquer le fonctionnement d'un ordinateur ou d'endommager ou de détruire des données, mais également les infractions commises au moyen d'ordinateurs, comme la fraude ou la violence sexuelle à l'égard des enfants. Les logiciels malveillants, le spam, l'hameçonnage et d'autres formes de vol d'identité font partie des outils et techniques utilisés par les cybercriminels.
- « **Logiciel malveillant** »[1] est un terme générique qui désigne différentes formes de logiciels hostiles ou intrusifs, parmi lesquels figurent notamment les virus et les chevaux de Troie.

1. https://fr.wikipedia.org/wiki/Logiciel_malveillant

Les objectifs des logiciels malveillants sont très divers : ils peuvent simplement chercher à perturber le fonctionnement d'un ordinateur en endommageant le logiciel ou le matériel, ou essayer de voler des informations et des données qui pourront d'une manière ou d'une autre être monnayées. Une fois infecté, votre ordinateur peut également devenir un « bot » contrôlé par des criminels à votre insu ; il peut alors être utilisé avec des millions d'autres ordinateurs dans un « réseau de bots » pour diffuser du spam, orchestrer une fraude ou attaquer des hôpitaux, des aéroports ou des banques.

- Le « **spam** » (ou « **pourriel** »)[2] désigne l'envoi massif de messages non sollicités à de multiples destinataires. Il est habituellement associé au courrier électronique mais s'applique également aux réseaux sociaux, à la messagerie instantanée, aux téléphones portables et autres. Fort heureusement, la plupart des services de messagerie disposent de filtres antispam efficaces. Le spam peut également servir de vecteur de propagation de logiciels malveillants, par exemple lorsque le destinataire ouvre une pièce jointe ou clique sur un lien contenu dans le message qu'il reçoit.
- *Phishing* (**hameçonnage**)[3] est un terme tiré de l'anglais « fishing for passwords » (pêche aux mots de passe). Cette technique, qui est une forme de vol d'identité, consiste à envoyer à des destinataires des messages qui prennent la forme de courriers électroniques officiels d'institutions reconnues, par exemple une banque ou un réseau social. Dans bien des cas, ces messages contiennent des liens vers de faux sites web qui servent à recueillir des informations confidentielles sur l'utilisateur comme son numéro de carte de crédit ou ses mots de passe. Ces informations sont régulièrement utilisées à des fins de fraude sur Internet.
- La **fraude sur Internet**[4] a fortement augmenté ces dernières années avec le développement du commerce électronique et la multiplication des offres de paiement en ligne. Elle englobe la contrefaçon, la fraude immobilière, les services « premium » de sonneries par SMS, la fraude aux transferts de fonds, etc.

COMMENT PRÉSERVER SA SÉCURITÉ ?

Votre sécurité en ligne est comparable à la sécurité de votre domicile. Vous en protégez l'accès en gardant portes et fenêtres fermées. Une bonne dose de prudence, des capacités de réflexion critique et des compétences en TIC vous éviteront d'être victime de fraude, d'hameçonnage, de logiciels malveillants ou d'escroqueries en ligne.

Nombre de points importants pour la sécurité le sont aussi pour la protection de la vie privée (voir Fiche d'information 9).

DÉVELOPPEMENT PERSONNEL ET INTÉRÊT PÉDAGOGIQUE

La sécurité en ligne est un enjeu tant individuel que collectif. La propagation des logiciels malveillants, virus et spams est le plus souvent le fait des utilisateurs eux-mêmes. En effet, un ordinateur non sécurisé peut compromettre la sécurité d'autres machines, notamment celles des amis et contacts de l'utilisateur.

L'étude des questions de sécurité en ligne peut être le point de départ du développement des compétences numériques des utilisateurs car elle les amène à se pencher en profondeur sur les paramètres et réglages de leurs appareils et sur les services en ligne qu'ils utilisent, tout en améliorant leurs connaissances techniques sur le fonctionnement de ces services, de leurs systèmes d'exploitation et d'Internet.

2. https://fr.wikipedia.org/wiki/Spam
3. https://fr.wikipedia.org/wiki/Hameçonnage
4. https://en.wikipedia.org/wiki/internet_fraud

RISQUES POTENTIELS

Spam (pourriels)

- Le spam n'a généralement pas de conséquences autres qu'une perte de temps à trier des messages ou à cliquer sur des liens.
- Le spam inclut souvent des informations fausses ou frauduleuses. L'expéditeur restant anonyme, il n'est pas possible de le poursuivre pour fausses déclarations.
- Les spammeurs profitent souvent de la bonne volonté des destinataires pour récupérer des adresses de messagerie qui alimentent ensuite leurs bases de données. Le destinataire peut recevoir un courrier lui demandant d'ajouter ses coordonnées à une liste pour soutenir une pétition ou une cause particulière. Évoquant souvent un motif humanitaire, par exemple un enfant malade ayant besoin d'une intervention chirurgicale, le texte du message indique qu'une société ou une organisation s'est engagée à verser une somme d'argent à chaque transfert du message.
- De nouvelles techniques de spam apparaissent chaque jour. Sur les réseaux sociaux, il peut prendre la forme d'un « détournement de clic » (click jacking)[5], avec des messages partagés par des amis portant des titres accrocheurs comme « les 10 meilleures façons de perdre du poids » ou « vous ne croirez jamais ce que fait cette fille devant sa caméra ». En cliquant sur ces messages, vous pouvez soit être redirigé vers un site web qui vous inonde de publicité pour générer des revenus, soit être contraint d'apposer un « j'aime » à une page qui vous enverra d'autres messages du même type.
- Il existe de nombreux types de fraude en ligne et l'évolution de la technologie en crée tous les jours d'autres. L'une des plus courantes porte le numéro « 419 » du nom de la loi nigériane interdisant cette pratique. Le message promet en général une somme d'argent importante à qui aiderait à réaliser des virements bancaires. Une autre fraude consiste à demander à la victime d'envoyer de l'argent via Western Union à titre de dépôt de garantie avant de visiter un appartement à la location.

Hameçonnage (phishing) et vol d'identité

- L'hameçonnage ou le vol d'identité font courir des risques beaucoup plus graves. Selon les informations que vous avez fournies lors de la tentative de phishing, le préjudice peut aller de la perte de contrôle d'un compte en ligne relativement peu important comme celui d'un forum en ligne à la perte de contrôle d'un compte majeur comme celui de votre messagerie électronique, qui pourra ensuite être utilisé pour pirater tous vos comptes en ligne !
- Si vos comptes ont été piratés, vos données peuvent être mises en péril. Tout votre courrier électronique peut être téléchargé, par exemple, et les informations qu'ils contiennent être utilisées pour vous extorquer de l'argent, ainsi qu'à vos contacts, commander des articles au moyen de vos comptes en ligne ou de votre carte de crédit, endosser votre identité en ligne, etc.

Logiciels malveillants

- Les risques liés aux logiciels malveillants sont comparables à ceux de l'hameçonnage ou du spam, voire pires. Ces logiciels peuvent être utilisés à des fins d'hameçonnage pour accéder à des informations sur vos comptes (au moyen d'un enregistreur de frappe[6], par exemple), à des fins de « spamming » pour vous bombarder de fenêtres intempestives ou de notifications et modifier les pages d'accueil par défaut de vos navigateurs, ou encore pour voler des informations et des données directement sur votre ordinateur, en perturber le fonctionnement ou en prendre le contrôle en vue de commettre des infractions, activer les micros ou des caméras de vos appareils pour vous espionner, voire détruire purement et simplement leur contenu.
- Les techniques visant à berner l'utilisateur pour lui faire installer des logiciels malveillants se développent rapidement elles aussi. Il existe par exemple de fausses fenêtres contextuelles qui reproduisent de manière réaliste une fenêtre d'analyse antivirus de votre ordinateur. À la fin de l'analyse, on vous dit que des virus dangereux ont été détectés sur votre ordinateur et on vous invite à installer un logiciel pour vous en débarrasser, lequel se trouve justement être un logiciel malveillant ou un virus !

5. https://fr.wikipedia.org/wiki/Détournement_de_clic
6. https://fr.wikipedia.org/wiki/Enregistreur_de_frappe

SUGGESTIONS D'ACTIVITÉS EN CLASSE

- Par groupes de trois ou quatre, les élèves sont invités à proposer un mot de passe fiable pour un compte factice en ligne. Précisez que ce mot de passe doit être nouveau et ne pas être l'un de ceux qu'ils utilisent déjà. Invitez chaque équipe à présenter son mot de passe et demandez au reste du groupe d'examiner les propositions et de recenser les caractéristiques d'un mot de passe fiable.
- Un mot de passe fiable :

▶ se compose d'au moins huit caractères ;

▶ ne contient pas de mot que l'on peut trouver dans un dictionnaire, de référence à votre vie privée ou à votre nom d'utilisateur, n'est pas votre véritable nom ou celui de votre entreprise ;

▶ contient des caractères de chacune des catégories suivantes : lettres majuscules, lettres minuscules, chiffres et symboles.

- Un CERT (computer emergency response team) également connu sous le nom de CSIRT (computer security incident response team) est un groupe d'experts qui gère les incidents de sécurité informatique. Demandez à vos élèves de trouver votre CERT/CSIRT national et informez-vous sur le rôle et le fonctionnement de ces équipes.
- Bien souvent, les victimes de cybercriminalité ne signalent pas les infractions à la police, si bien que leurs auteurs poursuivent leurs activités et trouvent de nouvelles proies.

▶ Demandez à vos élèves de trouver la marche à suivre pour signaler une infraction à la police ou à une autre administration publique, notamment par l'intermédiaire des numéros d'urgence.

▶ Demandez à vos élèves de trouver la définition de la cybercriminalité dans les lois de leur pays.

BONNES PRATIQUES

- Les utilisateurs espérant souvent pouvoir obtenir tout d'Internet sans rien débourser, il est de plus en plus fréquent de voir des logiciels malveillants ou spams associés aux logiciels ou services « gratuits » en ligne. La sécurité de l'environnement en ligne est une responsabilité partagée et résulte des comportements et choix individuels de chacun. En soutenant financièrement des services/du contenu/des logiciels de qualité (par des dons à des initiatives open source ou des abonnements auprès d'organisations commerciales), il est possible de contribuer à rendre l'environnement virtuel plus sûr.
- La convivialité peut être l'ennemi de la sécurité. Vous pouvez configurer votre système d'exploitation de manière à ce qu'il vous demande un mot de passe administrateur à chaque action importante (par exemple, installation d'un nouveau logiciel). Cela peut sembler contraignant, mais c'est le prix à payer pour plus de sécurité. Souvenez-vous-en lorsque vous réglez les paramètres de sécurité de votre système d'exploitation.
- Si vous gérez plusieurs utilisateurs ou un réseau, veillez à ce que chaque utilisateur dispose de droits appropriés. La suppression de certains droits d'accès inutiles peut contribuer à éviter des problèmes de sécurité, volontaires ou accidentels.
- Vérifiez la fiabilité de la source avant de télécharger quoi que ce soit sur votre ordinateur. Soyez particulièrement vigilants lors de l'utilisation de logiciels peer-to-peer[7], ces derniers étant connus pour favoriser la propagation de logiciels malveillants (voir Fiche d'information 14 sur la musique et les images). Quand vous installez un logiciel, lisez bien les instructions à chaque étape avant de cliquer sur le bouton « Suivant ». Faites particulièrement attention aux cases précochées qui pourraient installer des logiciels malveillants sur votre ordinateur !

7. https://fr.wikipedia.org/wiki/Pair_à_pair

- Installez un logiciel antivirus[8] et mettez-le régulièrement à jour.
- Installez les correctifs de sécurité ou mises à jour des systèmes d'exploitation dès leur sortie. Vous pouvez paramétrer certains systèmes d'exploitation ou programmes de manière à ce qu'ils se mettent à jour automatiquement ou vous informent dès qu'un correctif est disponible au téléchargement.
- Installez un pare-feu[9] pour contrôler le trafic entrant et sortant de votre ordinateur.
- Créez des comptes de courrier électronique différents pour chaque usage (par exemple, enregistrement sur des forums, formulaires à remplir, etc.) pour éviter de donner systématiquement votre adresse de courrier électronique « personnelle » et de la diffuser à grande échelle. N'oubliez pas que si vous publiez votre adresse de courrier électronique sur un site web, elle peut être repérée par des robots d'indexation et ajoutée à des listes de diffusion de spam. De la même manière, ne répondez pas aux spams car cela confirmerait votre adresse de courrier électronique à celui qui les envoie. Il faut savoir que les liens qui promettent de retirer votre adresse de messagerie des listes de diffusion ne sont pas tous authentiques.
- Si vous devez impérativement diffuser votre adresse de messagerie, vous pouvez la maquiller en y ajoutant des caractères, par exemple Tom[point]Smith[arobase]gmail[point]com, ou la poster sous forme d'image de manière à ce qu'elle ne puisse être copiée automatiquement.
- Soyez vigilant quand vous recevez du courrier électronique. N'ouvrez pas les messages dont la source vous semble douteuse. Vérifiez toujours l'adresse de courrier électronique de toute notification que vous recevez pour vous assurer qu'elle est bien réelle.
- Faites particulièrement attention aux pièces jointes. Si vous n'attendez pas de pièce jointe d'un expéditeur, ou si une pièce jointe vous semble suspecte, supprimez-la immédiatement sans l'ouvrir.
- Ne cliquez jamais sur les liens de destinataires en qui vous n'avez pas confiance, et en particulier sur les URL réduites qui masquent l'adresse d'origine. N'oubliez pas que même les destinataires auxquels vous faites confiance peuvent vous envoyer des messages infectés si leur compte ou leur appareil a été piraté.
- N'envoyez jamais d'informations privées comme un nom d'utilisateur, un mot de passe ou un numéro de carte de crédit par courrier électronique. Aucun service en ligne ne vous demandera jamais votre identifiant/mot de passe par ce biais, et il ne vous sera que rarement demandé de fournir des données comme le numéro de votre carte de crédit (celui-ci peut vous être demandé pour réserver une chambre d'hôtel, auquel cas vous devrez l'envoyer à l'adresse de courrier électronique officielle de réservation de l'hôtel).
- Utilisez un mot de passe différent pour chacun de vos principaux comptes et mettez en place une authentification à deux facteurs chaque fois que cela est possible (ajout de votre numéro de téléphone portable ou d'une phrase/question de sécurité). Veillez à ce que vos mots de passe n'aient aucun lien évident avec vous, qu'ils aient au moins huit caractères et utilisent une combinaison de lettres (majuscules et minuscules), de chiffres et de symboles.
- Effectuez des sauvegardes régulières de l'ensemble de vos données sur un disque dur externe. Il existe de nombreux programmes de sauvegarde qui enregistrent automatiquement et régulièrement vos données. Certains sont même inclus dans votre système d'exploitation (Windows, MacOS, Linux, etc.). Informez-vous régulièrement sur les solutions proposées[10].

8. https://fr.wikipedia.org/wiki/Logiciel_antivirus
9. https://fr.wikipedia.org/wiki/Pare-feu_(informatique)
10. https://fr.wikipedia.org/wiki/Liste_de_logiciels_de_sauvegarde

INFORMATIONS COMPLÉMENTAIRES

- Truth or Fiction est un site web qui permet aux Internautes de contrôler la véracité des informations contenues dans les messages les plus couramment transférés : <*http://www.truthorfiction.com/*>.
- Pour plus d'informations sur la lutte contre le spam : <*http://spam.abuse.net*> et <*http://www.spamhelp.org/*>.
- Pour plus d'informations sur Microsoft et la sécurité, voir : <*http://www.microsoft.com/security/*>.
- Pour plus d'informations sur Apple et la sécurité, voir : <*http://www.apple.com/support/security/*>.
- L'ENISA, Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information, fait régulièrement le point sur les questions de sécurité numérique : <*http://enisa.europa.eu*>.
- Le Conseil de l'Europe dispose d'une page web intitulée « Lutte contre la cybercriminalité » : <*www.coe.int/cybercrime*>.
- TechTarget est un magazine consacré à la sécurité de l'information : <*http://informationsecurity.techtarget.com/*>.
- On trouvera des informations utiles et des questionnaires sur des sujets allant des cookies aux adresses IP en passant par les vérifications de navigateur à l'adresse : <*http://www.2privacy.com/*>.
- On trouvera des conseils du gouvernement britannique sur la sécurité en ligne à l'adresse <*https://www.getsafeonline.org*> et pour les États-Unis à l'adresse <*http://www.us-cert.gov/*>.
- Trouvez votre CERT national en tapant « CERT + nom de votre pays » sur un moteur de recherche.
- Bien que les lignes directrices en matière de sécurité de la Direct Marketing Association <*http://www.the-dma.org/guidelines/informationsecurity.shtml*> s'adressent plutôt aux organismes de marketing direct, les conseils qui y figurent peuvent être utiles à toute personne qui s'intéresse à la sécurité en ligne.
- Articles pertinents de la Convention des Nations Unies relative aux droits de l'enfant :

Article 16 – L'enfant a le droit au respect de sa vie privée et à la protection de la loi contre toute atteinte ou immixtion dans son mode de vie, sa réputation, sa famille ou son domicile

Article 17 – Les enfants ont un droit d'accès à des informations fiables provenant des médias. La télévision, la radio et les journaux devraient fournir l'information dans un langage que les enfants comprennent et les protéger contre les contenus qui nuisent à leur bien-être.

Article 34 – Les États parties protègent les enfants contre toutes les formes d'exploitation sexuelle et de violence sexuelle.

Article 36 – Les enfants sont protégés contre toute activité susceptible de nuire à leur développement.