MIG-DHL

Migrants Digital Health Literacy

Manuel

Module 6

Être actif dans l'environnement de la santé numérique

Auteurs :

Josemar Alejandro Jimenez, Oxfam ; Jenny Wielga, IAT

Co-funded by the Erasmus+ Programme of the European Union

Le soutien de la Commission européenne à la production de cette publication ne constitue pas une approbation de son contenu, qui n'engage que ses auteurs, et la Commission ne peut être tenue responsable de l'usage qui pourrait être fait des informations qu'elle contient. Numéro de projet : 2020-1-DE02-KA204-007679.

Co-funded by the Erasmus+ Programme of the European Union

MIG-DHL Migrants Digital Health Literacy

Le présent Manuel fait partie du projet MIG-DHL, composé de 6 modules d'apprentissage au total, développés dans le cadre du partenariat stratégique Erasmus+ **MIG-DHL- Migrants Digital Health Literacy** [Programme visant l'éducation des migrants en matière de santé numérique].

La formation en un clin d'œil :

Projet MIG-DHL

- Module 1 : Qu'est-ce que l'éducation en matière de santé [Digital Health Literacy], et pourquoi est-ce important ?
- Module 2 : Les principaux enjeux en matière de santé à l'arrivée dans un nouveau pays
- Module 3 : Les services de santé
- Module 4 : Développer ses connaissances numériques
- Module 5 : Découvrir les outils de santé numérique
- **Module 6 : Être actif dans l'environnement de la santé numérique**

De plus amples informations sont disponibles sur le site : https://mig-dhl.eu/

Co-funded by the
Erasmus+ Programme
of the European Union

MIG-DHL
Migrants Digital Health Literacy

Déclaration sur les droits d'auteur :

Co-funded by the
Erasmus+ Programme
of the European Union

MIG-DHL
Migrants Digital Health Literacy

Table des matières

6. Être actif dans l'environnement numérique

Être actif dans l'environnement numérique implique nécessairement de savoir comment protéger la vie privée, pour pouvoir renforcer la protection des données personnelles dans le monde du tout numérique et préserver la santé physique ainsi que la santé mentale.

Le présent module se concentre donc sur la protection de ce caractère privé des données. Les informations qu'il contient font suite aux sujets déjà abordés dans le module 4. Elles sont notamment en lien avec le développement des compétences en matière de sécurité et de protection de la vie privée. Les compétences dont il s'agit sont la capacité de protéger les appareils, le contenu, les données personnelles et la confidentialité au sein de l'environnement numérique. Les conséquences d'une telle démarche permettent par ailleurs de préserver la santé physique et mentale, le bien-être ainsi que l'inclusion sociale des personnes. Cette partie est liée au domaine de compétence 4 « Sécurité » de DigiComp, qui a déjà été abordé dans le module 4.

6.1 La protection de la vie privée et des données à caractère personnel dans l'environnement numérique

Il existe un très grand nombre de facteurs de risque au sein de l'environnement numérique en ce qui concerne la vie privée et les données à caractère personnel. Nous avons décrit de façon plus détaillée certains des plus facteurs de risque les plus importants dans les parties suivantes – de tels facteurs ayant également été abordés dans les supports de formation.

6.1.1 Le piratage (Hacking)

Le piratage (ou *hacking* en anglais) désigne l'ensemble des activités qui visent à compromettre tout matériel numérique, tel que les ordinateurs, les smartphones, les tablettes voire des réseaux entiers. Et, bien que le piratage ne soit pas forcément une pratique utilisée exclusivement à des fins malveillantes, de nos jours, c'est une activité presque toujours considérée comme illégale. De la même façon, ses auteurs, les pirates informatiques (connus aussi sous le terme anglais de *hackers*), sont vus comme des cybercriminels motivés par des

gains financiers, des protestations, la collecte d'informations (espionnage) ou même simplement par le plaisir du défi.

Le piratage est considéré, par nature, comme une activité purement technique. Toutefois, les pirates informatiques peuvent aussi passer par des méthodes psychologiques pour tromper l'utilisateur et l'inciter à cliquer sur une pièce jointe infectée par un virus ou à fournir des données personnelles.

En réalité, on peut dire que le piratage est un terme générique qui recouvre les activités à l'origine de la plupart, voire de la totalité, des logiciels malveillants et des cyberattaques contre le public, les entreprises et les gouvernements. Les techniques de piratage les plus courantes sont :

- les botnets
- le piratage de navigateur ou détournement de recherche
- les attaques par déni de service distribué (DDoS)
- les rançongiciels
- les rootkits
- le cheval de Troie
- les virus
- les vers informatiques

Types de piratage/pirates

D'une manière générale, on peut dire que les pirates informatiques tentent toujours de s'introduire dans les ordinateurs et les réseaux pour l'une de ces trois raisons :

- gains financiers criminels à la clé (vol de numéros de carte de crédit ou fraude de systèmes bancaires)
- gagner et renforcer sa crédibilité et sa réputation au sein de la subculture des pirates informatiques (certains pirates informatiques aiment à laisser leur marque sur les sites qu'ils piratent comme preuve de leur acte)

- l'espionnage d'entreprise (les pirates informatiques d'une société cherchent à voler des informations sur les produits et services d'un concurrent pour obtenir un avantage sur le marché)

La prévention contre le piratage

- Installez un antivirus : Avant toute chose, téléchargez un logiciel (ou une application sur le téléphone) antivirus qui soit fiable, et qui peut à la fois détecter et empêcher les logiciels malveillants, ainsi que bloquer les connexions aux sites d'hameçonnage (ou de *phishing* en anglais).
- Faites attention aux applications : Ne téléchargez des applications pour téléphone que sur des boutiques en ligne fiables (Google Play et Amazon Appstore par ex) qui contrôlent elles-mêmes les applications vérolées (notez que la politique d'Apple restreint les utilisateurs d'iPhone à télécharger uniquement à partir de l'App Store). Malgré cela, à chaque fois que vous téléchargez une application, vérifiez d'abord les évaluations et commentaires. Si l'évaluation et le nombre de téléchargements sont bas, il est préférable d'éviter cette application.
- Protégez vos données : Sachez qu'aucune banque ou système de paiement en ligne ne vous demandera vos identifiants de connexion, numéro de sécurité sociale ou numéros de carte de crédit par e-mail.
- Mettez à jour vos logiciels : que ce soit sur votre téléphone ou sur votre ordinateur, assurez-vous que votre système d'exploitation est à jour.
- Faites vos recherches avec prudence : Évitez les sites web non sécurisés, ne téléchargez jamais de pièces jointes non vérifiées et ne cliquez jamais sur des liens contenus dans des e-mails inconnus.
- Assurez la sécurité de vos mots de passe : Tout ce qui précède constitue une sécurité de base et est toujours une bonne chose à mettre en place. Toutefois, les pirates malveillants sont en permanence à la recherche d'un nouveau moyen de pénétrer dans votre système. Si un pirate informatique trouve un mot de passe que vous utilisez sur plusieurs services, ils possèdent des applications qui leur permettent d'accéder à vos

autres comptes. Vous devez donc choisir des mots de passe longs et complexes et éviter d'avoir un même mot de passe pour plusieurs comptes. Il est également conseillé d'utiliser un gestionnaire de mots de passe. Le piratage ne serait-ce que d'un seul compte mail peut entraîner des conséquences catastrophiques ! (Malwarebytes, 2020)

6.1.2 Les virus informatiques

Un virus informatique est l'une des formes de piratage les plus connues. À l'instar du virus de la grippe, il est conçu pour se propager d'hôte à hôte et a la capacité de se reproduire. Et tout comme la grippe, qui ne peut pas se reproduire sans une cellule hôte, les virus informatiques ne peuvent pas se reproduire et se transmettre sans programmation (telle qu'un fichier). En d'autres termes, un virus informatique est un genre de programme malveillant créé pour modifier le fonctionnement d'un ordinateur et pour se propager d'un ordinateur à l'autre. Un virus opère en s'insérant ou en s'attachant à un programme ou un document légitime qui autorise l'exécution de code via l'utilisation de macros. Au cours de ce processus, un virus peut alors causer des effets inattendus ou dommageables par exemple en détériorant le logiciel système via la corruption ou la destruction de données.

Comment un virus informatique attaque-t-il ? Dès lors que le virus a réussi à s'attacher à un programme, un fichier ou un document, il reste en sommeil jusqu'à ce que l'ordinateur ou le périphérique se mette à exécuter son code. Un virus contamine l'ordinateur lorsque le programme infecté est exécuté, ce qui entraîne l'exécution du code du virus. Un virus peut donc rester en sommeil sur un ordinateur sans présenter aucun signe ni symptôme particulier. Cependant, lorsque le virus se met à infecter un ordinateur, il peut en infecter d'autres dans le même réseau. Voler des mots de passe ou des données, enregistrer les frappes de clavier, corrompre des fichiers, envoyer des spams aux contacts de messagerie électronique et même prendre le contrôle sur l'appareil ne sont que quelques-uns des effets dévastateurs qu'un virus peut produire. Si certains virus sont à visée ludique, d'autres peuvent avoir des effets véritablement néfastes. Ils peuvent par exemple effacer des données ou causer des dégâts

permanents sur le disque dur. Pire encore, certains virus sont conçus dans le but de voler de l'argent.

Comment les virus informatiques se propagent-ils ? Dans un monde constamment connecté, les virus informatiques se transmettent de différentes manières, plus ou moins visiblement. Ils peuvent se propager par le biais de pièces jointes d'e-mails et de SMS, de téléchargements de fichiers sur Internet et de liens frauduleux sur les réseaux sociaux. Les appareils mobiles et smartphones peuvent également être contaminés par des virus de téléphones mobiles lors du téléchargement d'applications douteuses. Les virus peuvent se dissimuler sous la forme de pièces jointes de contenus à partager sur les réseaux sociaux, tels que des images rigolotes, des cartes de vœux ou des fichiers audio et vidéo. Pour éviter à un appareil d'être contaminé par un virus, il est important de faire preuve d'une grande prudence en naviguant sur Internet, en téléchargeant des fichiers et en ouvrant des liens ou des pièces jointes. Pour assurer une bonne sécurité de vos appareils, ne téléchargez jamais les pièces jointes d'un SMS ou d'un e-mail que vous n'attendiez pas, ni les fichiers provenant de sites en lesquels vous n'avez pas confiance.

Quels sont les signes de l'existence d'un virus informatique ? L'attaque d'un virus informatique peut se révéler via différents symptômes. En voici quelques-uns :

- Plein de fenêtres pop-up. Les fenêtres pop-up peuvent vous inciter à vous rendre sur des sites inhabituels, ou bien vous proposer de télécharger un antivirus ou d'autres logiciels.
- Des modifications sur votre page d'accueil. Votre page d'accueil habituelle peut avoir été remplacée par une autre page web par exemple. Il est également possible que vous ne puissiez pas la réinitialiser.
- L'envoi massif d'e-mails à partir de votre compte de messagerie. Un pirate informatique peut prendre le contrôle de votre compte, ou bien envoyer des e-mails en votre nom depuis un autre ordinateur infecté.

- Des pannes d'ordinateur fréquentes. Un virus peut causer des dommages importants à votre disque dur et figer l'appareil ou le rendre totalement hors service. Le virus peut également empêcher votre appareil de se rallumer.
- Des performances anormalement lentes de l'ordinateur. Un changement brutal de vitesse de performance peut être le signe d'une attaque de virus sur votre ordinateur.
- Des programmes inconnus qui démarrent lorsque vous allumez votre ordinateur. Un virus peut se révéler au moment de démarrer votre ordinateur, et vous pouvez aussi le remarquer en consultant la liste des applications actives de votre ordinateur.
- Des activités inhabituelles comme des changements de mots de passe. De telles modifications peuvent vous empêcher d'accéder à votre ordinateur.

Comment peut-on contribuer à la protection des appareils contre les virus informatiques ? Voici quelques mesures que vous pouvez mettre en place pour renforcer la sécurité de votre ordinateur :

- Utilisez un antivirus fiable et assurez-vous d'installer les dernières mises à jour contre les nouveaux virus.
- Évitez de cliquer sur les fenêtres pop-up publicitaires.
- Procédez chaque fois à une analyse des pièces jointes de vos e-mails avant de les ouvrir.
- Procédez chaque fois à une analyse des fichiers que vous téléchargez à l'aide de programmes de partage de fichiers (Norton, 2020).

6.1.3 Le vol de données personnelles

(Comprend : L'usurpation d'identité, les données de comptes de cartes de crédit, les informations d'identification des clients)

Le vol de données est le fait de voler des informations numériques stockées sur les ordinateurs, les serveurs ou les appareils électroniques d'une victime inconnue, dans le but de compromettre sa vie privée ou d'obtenir des informations confidentielles. Il peut s'agir autant d'informations financières (numéros de carte et les comptes bancaires par ex) que

d'informations personnelles (numéro de sécurité sociale, numéro du permis de conduire ou dossiers médicaux par ex).

Comment se produit le vol de données ? Il existe plusieurs moyens de voler des données personnelles. Le plus souvent, le vol de données a lieu au moment du piratage d'un système informatique exécuté dans le but de voler des informations sensibles (telles que les données d'une carte de crédit), ou bien à la suite de la mauvaise gestion des données par le personnel d'une entreprise. Dans un monde où tout est de plus en plus numérisé, des centaines d'entreprises et d'organisations diverses et variées détiennent des données personnelles (numéro de sécurité sociale, adresse postale, date de naissance, informations bancaires…).

Comment se protéger contre ces vols ? Le vol de données est un problème bien réel, qui peut arriver à n'importe qui. Bien qu'il n'y ait aucun moyen de l'empêcher, il existe de nombreuses mesures que vous pouvez mettre en place dès aujourd'hui pour limiter les risques.

- Payez en espèces plutôt qu'avec des cartes de crédit ou de débit.
- Utilisez une carte de crédit ou de débit dotée d'une puce électronique.
- Protégez votre ordinateur contre les virus et programmes malveillants en installant (et en mettant à jour !) des antivirus et des logiciels anti-espions sur tous vos ordinateurs et autres appareils électroniques.
- Assurez-vous que tous les systèmes d'exploitation, navigateurs et logiciels soient à jour en installant régulièrement les mises à jour de sécurité dès qu'elles sont disponibles.
- N'ouvrez pas les e-mails ou pièces jointes douteuses, qui peuvent potentiellement cacher du phishing.
- Vérifiez régulièrement vos relevés de carte de crédit et vos dossiers de crédit pour voir si des frais non autorisés ou de nouvelles lignes de crédit y apparaissent.
- Utilisez un mot de passe fort et unique pour chaque site web nécessitant une connexion. Changez régulièrement vos mots de passe, surtout si le mot de passe d'un compte a été compromis lors d'une violation de données.
- Utilisez uniquement des connexions Wi-Fi sécurisées.

- Jetez correctement vos documents contenant des informations sensibles en déchiquetant les papiers et en supprimant toutes les données de vos appareils électroniques (Michaud, 2021).

6.1.4 Les spams

Il arrive parfois (voire souvent) que l'on reçoive des e-mails indésirables, appelés « spams ». C'est non seulement ennuyeux car cela demande du temps pour trier ses e-mails et supprimer ces spams, mais également parce qu'ils peuvent être dangereux et contenir des virus ou autres programmes malveillants qui viennent s'installer sur l'ordinateur et qui, lorsque l'on ouvre le spam, peuvent par exemple espionner les données d'accès. Le phishing (ou hameçonnage en français) est également un type courant d'escroquerie en ligne, qui consiste en l'envoi d'e-mails d'apparence officielle par des cybercriminels, dans le but d'amener l'utilisateur à révéler des informations qui peuvent être utilisés pour usurper notre identité.

- Par conséquent :
    - évitez d'ouvrir les pièces jointes, à moins qu'elles ne soient préalablement passées par un anti-virus,
    - n'oubliez pas de vous déconnecter, surtout lorsque vous utilisez un ordinateur public partagé,
    - supprimez tous les e-mails provenant de personnes inconnues,
    - ne répondez jamais aux spams.
- Comment identifier les courriers indésirables ? Voici quelques signes pouvant vous aider à repérer un courrier indésirable ou « spam » :
    - fautes de grammaire et d'orthographe
    - e-mails écrits en langue étrangère
    - absence de nom
    - demande d'agir dans l'urgence (notamment avec une menace)
    - demande de saisie de données personnelles (code PIN ou n° de sécurité sociale par ex)
    - demande d'ouvrir un fichier

- e-mail d’une banque que vous n’avez encore jamais reçu, ou bien e-mail d’un établissement bancaire dont vous n’êtes pas client à ce jour.

  (Verbraucherzentrale, 2021).

Bibliographie

Carretero, S.; Vuorikari, R. and Punie, Y. (2017). *DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use*. doi:10.2760/38842

Michaud, Katelyn. (2021). *What is Data Theft?* https://safety.lovetoknow.com/personal-safety-protection/what-is-data-theft

MOZ (2022). *Google Search Operators.* https://moz.com/learn/seo/search-operators

Norman, C.; Skinner, H. (2006). eHealth Literacy: Essential Skills for Consumer Health in a Networked World. *J Med Internet Res* 8(2):e9. DOI: 10.2196/jmir.8.2.e9

Norton. (2020). *What is a computer virus?* https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html

Malwarebytes. (2020). *Hacking definition: What is hacking?* https://www.malwarebytes.com/hacker

Verbraucherzentrale (2021). *Spam: E-Mail-Müll im Internet*. https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/spam-emailmuell-im-internet-10757

Wikipedia (2022) *Botnet.* *https://fr.wikipedia.org/wiki/Botnet*

Support Mozilla *Qu'est-ce qu'un détournement de recherche?* https://support.mozilla.org/fr/kb/quest-ce-quun-detournement-de-recherche

OVHcloud *Qu'est-ce qu'une attaque DDoS?* https://www.ovhcloud.com/fr/security/anti-ddos/ddos-definition/

Economie.Gouv.fr *Qu'est-ce qu'un rançongiciel?* https://www.economie.gouv.fr/entreprises/methodes-piratage#rancongiciel

Avast *Qu'est-ce qu'un rootkit et comment s'en débarrasser* ? https://www.avast.com/fr-fr/c-rootkit

Malwarebytes (2022) *Trojan : Tout savoir sur les chevaux de Troie* https://fr.malwarebytes.com/trojan/

Cybermalveillance.gouv.fr *Les cybermenaces : Virus informatique, que faire ?* https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/virus-informatiques

Norton *Confidentialité : Qu'est-ce qu'un ver informatique ?* https://fr.norton.com/blog/privacy/what-is-a-computer-worm

WebsiteSetup (2021). https://websitesetup.org/evaluating-online-resources

Organisation Mondiale de la Santé [OMS]. 2017. *Digital Health Literacy*. https://www.who.int/global-coordination-mechanism/working-groups/digital_hl.pdf