TeleGrow
Enhancing the Teleworking Digital Skills for the Middle aged employees

Modules de formation sur le télétravail : La formation ultime au télétravail pour les formateurs professionnels

CWEP

Module 6 - Les bases de la sécurité en ligne

27/6/2022

Erasmus+

Projet financé par : **Appel 2020 Cycle 1 KA2 - Coopération pour l'innovation et l'échange de bonnes pratiques / KA226 - Partenariats pour la préparation à l'éducation numérique**

Index

1. Introduction au sujet

En ces temps difficiles, les gens essaient tous de s'adapter à la nouvelle ère du travail à domicile sans connaître obligatoirement la quantité de risques et de menaces qu'elle comporte, non seulement pour les personnes âgées de plus de 50 ans, auxquelles le projet TeleGrow s'adresse mais aussi pour les travailleurs de tous âges. Un rapport de la Commission européenne de 2020 indique qu'environ 40 % des travailleurs de l'UE ont commencé à travailler à distance depuis la pandémie de COVID-19, ce qui représente une multiplication par près de 8 par rapport à l'année précédant son déclenchement. Cette augmentation rapide du télétravail fait qu'il est difficile pour les entreprises de mettre en place de nouvelles et solides mesures de sécurité, ce qui ouvre une fenêtre pour diverses pratiques malveillantes. Avec l'augmentation des activités de cybercriminalité de plus de 600% depuis le début de la pandémie, il est facile de conclure que les personnes âgées de plus de 50 ans qui ont peu ou pas d'expérience du télétravail sont particulièrement vulnérables aux dangers qu'il peut entraîner. Ces dangers concernent des éléments tels que l'usurpation d'identité, les violations de données, les logiciels malveillants (malware) et les virus, les fraudes bancaires et bien d'autres menaces auxquelles les personnes âgées ne sont peut-être pas bien préparées.

Ce module est conçu pour fonctionner comme une brève introduction au sujet de la sécurité en ligne. Il comprendra des descriptions des dangers les plus courants du télétravail et de l'utilisation générale d'Internet auxquels les groupes cibles du projet TeleGrow peuvent être confrontés. Cette partie du module aidera à comprendre ce que sont les spams et le phishing, comment les reconnaître, et quels dangers ils peuvent représenter. D'autres pratiques courantes, comme le piratage, les ransomwares ou l'usurpation d'identité, seront également expliquées en détail. Le module expliquera également les mesures à prendre pour sécuriser une connexion Internet privée et familiarisera l'apprenant avec le règlement général sur la protection des données. Enfin, ce module du projet TeleGrow comprendra également une brève série d'exercices pour ses apprenants, afin de tester leurs connaissances acquises tout au long de ce module.

2. Objectifs d'apprentissage

À l'issue de ce module, l'apprenant pourra :

- Recevoir des informations sur le spam et le phishing et savoir comment les reconnaître
- Comprendre ce qu'est le piratage, comment fonctionne un ransomware et comment se protéger contre le vol d'identité et les conséquences qu'il entraîne
- Savoir quelles mesures prendre pour sécuriser leur connexion Internet et quelle est la différence entre un mot de passe faible et un mot de passe fort.
- La différence entre un mot de passe faible et un mot de passe fort.
- Acquérir des connaissances sur le règlement général sur la protection des données et sur les moyens de protéger les informations personnelles
- Être capable d'établir un environnement de travail à domicile sûr grâce à une activité pratique à la fin du module

3. Contenus d'apprentissage

Chapitre 1 – Spam et Phishing

Le mot "spam" désigne tous les messages numériques indésirables que les gens reçoivent et qui ont été envoyés à un grand groupe de destinataires. Ce processus est le plus souvent le fait de ce que l'on appelle les "spambots", qui sont des programmes automatisés utilisés pour envoyer des messages indésirables à des comptes de messagerie, des sites de réseaux sociaux ou des forums. Même si le spam peut sembler être

Même si le spam peut sembler être un problème relativement nouveau, son histoire remonte à 1978, lorsque Gary Thuerk a voulu promouvoir son produit en envoyant des courriers électroniques non sollicités à des milliers de personnes, ce qui aurait généré environ 12 millions de dollars de revenus.

Aujourd'hui, l'usage des messages de spam reste le même, puisqu'il est utilisé pour générer un profit en faisant la promotion de quelque chose. En général, les produits dont il fait la publicité sont de qualité douteuse, et les sujets dont les messages de spam font la promotion sont le plus souvent les suivants :

- Produits pharmaceutiques
- Contenu pour adulte
- Services financiers
- Jeux d'argent en ligne

- crypto-monnaies

Source: freepik.com

En 2020, environ 50 % de tous les courriels reçus étaient des spams. Les personnes qui créent et envoient des messages de spam s'en prennent aux internautes inexpérimentés, et l'ouverture de ces courriels peut avoir des conséquences très désagréables, comme le partage d'informations privées avec des personnes non autorisées ou l'inscription sur les listes de diffusion de divers vendeurs, ce qui entraînera l'accumulation d'encore plus de courriels indésirables dans la boîte aux lettres d'une personne. Même si les chiffres peuvent sembler écrasants, les gens voient rarement des messages de spam dans leur boîte aux lettres de nos jours. Cela est dû à l'évolution rapide du filtrage du spam. Les statistiques révélées par Google en avril 2020 montrent qu'ils ont réussi à bloquer et à filtrer 99,9 % des courriers électroniques indésirables. Cela signifie que les internautes d'aujourd'hui, ainsi que les personnes de plus de 50 ans, sont beaucoup plus à l'abri de la réception de ce type de messages. Cela ne signifie pas que le filtrage fonctionne parfaitement ; il y a toujours des spams qui passent et, pour pouvoir les filtrer eux-mêmes, les internautes doivent savoir quel type de message ils doivent éviter d'ouvrir. Voici quelques-uns des types de spam les plus courants :

➢ <u>Usurpation de l'adresse email</u>

Ces types de messages essaient d'imiter l'expéditeur en forgeant le même e-mail exact que lui et en faisant croire au destinataire que l'e-mail provient d'une personne ou d'un site Web en qui il peut avoir confiance. Ils demandent souvent à quelqu'un d'effectuer une action, qui peut être une demande de paiement d'une

facture impayée, la validation ou le déblocage d'un compte, ou la vérification d'un achat, et fournissent un lien qui, une fois cliqué, peut être utilisé pour voler les informations personnelles du destinataire. Heureusement, de nombreux fournisseurs de courrier électronique avertissent au préalable l'utilisateur du risque d'être "usurpé".

- Escroquerie aux avances de frais

Parfois appelée "escroquerie du prince nigérian", l'une des idées sous-jacentes est que l'expéditeur promet une grosse somme d'argent mais seulement si le destinataire accorde un petit prêt à l'avance. Ce prêt est généralement nécessaire pour régler une affaire juridique qui permettra de débloquer la somme plus

importante. L'autre type d'escroquerie à l'avance fonctionne de la même manière, mais dans ce cas, l'expéditeur se fait passer pour un ami proche ou un membre de la famille du destinataire qui a besoin d'argent en raison d'une urgence quelconque.

- Publicités et spams malveillants

Le spam publicitaire est simplement un message non sollicité proposant un certain type de produit. Si ces offres peuvent parfois être vraies, dans de nombreux cas, le produit n'existe pas ou ne fonctionne pas. Le spam malveillant est un type de message qui contient divers types de contenus malveillants cachés derrière des liens ou des pièces jointes fournis dans le message. Une fois que la personne a

téléchargé et ouvert le fichier joint ou téléchargé via le lien, les scripts malveillants s'exécutent et infectent l'ordinateur avec différents types de logiciels malveillants dangereux.

Le phishing est une cybercriminalité similaire à l'usurpation d'adresse électronique mais plus complexe. Cette pratique malveillante est utilisée dans le cadre de la fraude, de l'espionnage ou pour mettre en place des cyberattaques visant diverses organisations. Elle consiste à falsifier des courriels ou des appels téléphoniques et à prétendre qu'ils proviennent d'une source légitime pour persuader des personnes de révéler leurs informations personnelles ou financières, souvent sans cible particulière. Les messages de hameçonnage sont également envoyés à partir de faux courriels qui semblent dignes de confiance, mais dans ce cas, le cybercriminel collecte des informations sur la victime à partir de différentes sources, telles que les messages publics sur les médias sociaux, les sites sur lesquels l'adresse électronique de la victime est enregistrée, les profils des amis de la victime sur les médias sociaux ou les informations sur les employés sur le site web de l'entreprise.

Le pirate peut alors rassembler toutes les informations sur cette personne et préparer un message personnalisé, dont le destinataire peut être victime. Ces courriels contiennent souvent des liens malveillants, mais peuvent aussi être utilisés pour établir une connexion entre le criminel et la victime afin de gagner sa confiance et de voler des informations sensibles. Parfois, les attaques d'hameçonnage ciblent les cadres supérieurs d'une entreprise pour les inciter à révéler leurs informations personnelles ou des données précieuses de l'entreprise, qui peuvent ensuite être utilisées à des fins malveillantes. Pour être moins enclins à se laisser piéger par les tentatives de phishing, les internautes doivent prêter une attention particulière et éviter d'ouvrir :

- Les e-mails ayant pour but pour gagner un gros lot
- Les faux sites web ressemblant beaucoup aux sites originaux
- Les menaces concernant la désactivation du compte ou la perte d'accès à celui-ci

- Les messages concernant une fausse infection par un logiciel malveillant
- Les emails à thème portant sur la COVID-19
- Les faux parents demandant de l'argent
- La mauvaise grammaire et des mots mal orthographiés dans des courriels supposés formels

Même si les filtres de contenu malveillant fournis par la plupart des fournisseurs d'e-mail offrent une protection solide contre le spam et le phishing, les gens doivent garder à l'esprit que ce n'est pas sans faille et qu'il existe certaines contre-mesures qu'ils peuvent prendre pour réduire encore plus les risques de se faire voler leurs données personnelles. Pour ce faire, il faut toujours copier et coller le contenu d'un message suspect dans un moteur de recherche (par exemple, Google), car il est possible que le message ait déjà été signalé comme une tentative de phishing. Une autre bonne pratique consiste à contacter la société qui est censée avoir envoyé le message suspect sans cliquer sur les liens ou les pièces jointes qu'il contient. Une bonne idée serait également d'installer des filtres anti-spam et des barres d'outils anti-hameçonnage sur un ordinateur, car ces outils peuvent protéger l'utilisateur de tels messages par eux-mêmes. Dans un environnement de travail, les employés devraient essayer de confirmer verbalement toute demande qui leur est adressée par courrier électronique et changer régulièrement leurs mots de passe.

Chapitre 2 – Piratage, demande de rançons, ou vol d'identité

En raison de l'augmentation récente du télétravail et de la nécessité de rester à la maison et de faire de nombreuses courses en ligne à cause de la pandémie de COVID-19, le monde est également témoin d'une énorme augmentation des cybercrimes. Ceux-ci peuvent être définis comme toute activité illégale réalisée à l'aide d'un ordinateur et sont souvent associés à des personnes appelées "pirates informatiques" ou "cybercriminels", qui peuvent être divisés en plusieurs catégories différentes en fonction de ce qu'ils veulent réaliser et de leurs compétences.

Source: freepik.com

Le piratage informatique consiste à identifier les failles de sécurité d'un système ou d'un réseau informatique afin d'accéder à des données personnelles ou professionnelles. L'utilisation d'un algorithme de déchiffrage de mot de passe pour accéder à un système informatique est un exemple de piratage informatique. Bien qu'il soit souvent considéré comme une pratique malveillante, il est parfois légal et utilisé avec de bonnes intentions, principalement pour améliorer la sécurité en ligne et sécuriser des données précieuses au sein d'une certaine organisation. Une telle pratique est appelée "piratage éthique". Le piratage classique couvre un large éventail de pratiques malveillantes, allant du ralentissement des ordinateurs d'autres personnes au vol d'informations sur les cartes de crédit, en passant par l'intimidation

à grande échelle et les demandes de rançon. Comme indiqué au chapitre 1, les pirates peuvent accéder aux appareils d'autres personnes par le biais de tentatives de phishing et de logiciels malveillants contenus dans des messages de spam suspects, mais ce ne sont pas les seules méthodes qu'ils utilisent. Une technique de piratage courante, à laquelle de nombreuses personnes peuvent être sujettes, consiste à créer un faux point d'accès Wi-Fi dans un lieu public vers un site web qui peut voler leurs informations personnelles. Pour éviter que cela ne se produise, les gens devraient éviter d'utiliser les réseaux Wi-Fi publics et être toujours prudents lorsqu'ils utilisent leurs appareils dans des endroits comme les restaurants, les aéroports, les centres commerciaux ou les parcs.

Une autre forme de logiciel malveillant qui peut être très dangereuse pour les personnes de plus de 50 ans qui commencent à télétravailler est la demande de rançon. Cela peut s’avérer très dangereux car il s'agit non seulement de l'un des problèmes de sécurité Internet les plus préoccupants aujourd'hui, mais il est également très courant. Ce logiciel malveillant crypte les fichiers et les documents d'un ordinateur unique ou d'un réseau entier, y compris les serveurs. Après l'attaque, la victime reçoit des instructions pour payer une rançon afin de déverrouiller les fichiers ; sinon, les précieuses données seront rendues publiques ou vendues à d'autres cybercriminels, d'où le nom de "ransomware".

Ce malware, ainsi que d'autres, se propage le plus souvent par le biais de pièces jointes dans des messages de spam de phishing, c'est pourquoi il est essentiel de traiter tout courriel suspect avec une extrême prudence. Les attaques par ransomware sont très dangereuses car, si elles réussissent, elles peuvent exposer les informations privées et précieuses de milliers d'employés si elles visent une entreprise spécifique.

L'une des formes de cybercriminalité qui se développe le plus rapidement est l'usurpation d'identité. Le criminel vole des données personnelles, telles que des identifiants, des détails de comptes bancaires, des dates de naissance, etc. afin d'usurper l'identité de la victime et d'utiliser ces informations pour en tirer un profit monétaire et causer d'autres dommages aux personnes. Les méthodes utilisées par les pirates pour y parvenir sont similaires à celles d'autres cybercrimes. Ils peuvent acquérir ces précieuses données par le biais de tentatives d'hameçonnage ou en piratant des ordinateurs à l'aide de divers logiciels malveillants et de points d'accès Wi-Fi publics faux ou mal sécurisés. Par la suite, ils peuvent utiliser ces données pour obtenir des prêts, acheter diverses choses ou même commettre des crimes au nom de la victime. Il est bon de vérifier régulièrement les rapports de crédit et de rechercher toute inexactitude ou tout virement bancaire qui pourrait sembler suspect. La somme d'argent manquante ne doit pas nécessairement être importante, car le voleur peut voler des milliers de personnes en même temps. Les victimes de vol

d'identité doivent, dès que possible, signaler ce délit aux autorités, geler leurs

comptes bancaires et en ouvrir de nouveaux. Si cela est possible, les victimes doivent contacter les banques, les agents de recouvrement et les autres endroits où elles savent que le voleur a utilisé leurs informations personnelles. Il est également important de contacter les parents, les employeurs et les collègues de l'entreprise où elles travaillent actuellement, car le voleur pourrait également être en possession de leurs données.

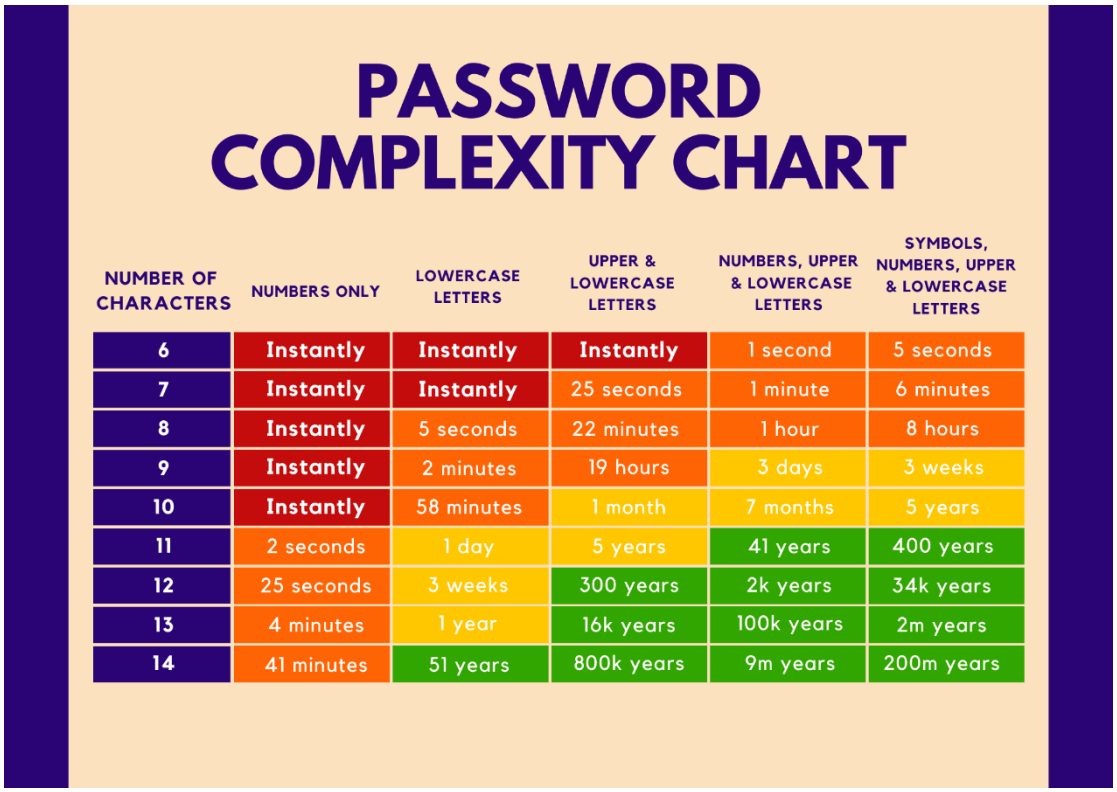
Les techniques utilisées par les pirates informatiques pour voler ou semer le chaos dans la vie des gens sont de plus en plus sophistiquées. Dans cette optique, les gens doivent savoir comment se protéger pour minimiser les risques d'être victimes de cybercrimes. Il existe une contre-mesure de protection qui, une fois mise en œuvre, réduit le risque d'avoir affaire à des cybercriminels.

Créer un mot de passe fort. Il s'agit d'un élément crucial pour assurer la sécurité de données précieuses. Un bon mot de passe n'est pas évident mais facile à retenir. Il ne doit pas comporter moins de 12 caractères, car il faut quelques secondes pour déchiffrer des mots de passe courts avec la technologie actuelle. Un mot de passe fort doit comporter des symboles uniques, tels que des chiffres et des lettres minuscules ou majuscules, car cela lui confère un niveau de sécurité supplémentaire. Il est important qu'il soit fort et difficile à oublier. Une technique courante pour créer des mots de passe forts consiste à créer un acronyme à partir d'une citation favorite ou d'une phrase mémorable et à y ajouter quelques symboles spéciaux. Une autre bonne pratique consiste à utiliser des gestionnaires de mots de passe. Ces programmes génèrent et stockent les mots de passe d'un utilisateur dans un compte crypté en toute sécurité. Une autre chose cruciale est de garder les mots de passe privés et de ne jamais les envoyer à qui que ce soit par e-mail ou par SMS. Le graphique ci-dessous

montre à quel point il est facile pour un pirate de casser un mot de passe qui peut sembler complexe pour son utilisateur.

Informations recueillies sur : https://www.security.org/how-secure-is-my-password/

D'après les données recueillies, il est facile de confirmer ce qui a été dit



PASSWORD COMPLEXITY CHART

NUMBER OF CHARACTERS	NUMBERS ONLY	LOWERCASE LETTERS	UPPER & LOWERCASE LETTERS	NUMBERS, UPPER & LOWERCASE LETTERS	SYMBOLS, NUMBERS, UPPER & LOWERCASE LETTERS
6	Instantly	Instantly	Instantly	1 second	5 seconds
7	Instantly	Instantly	25 seconds	1 minute	6 minutes
8	Instantly	5 seconds	22 minutes	1 hour	8 hours
9	Instantly	2 minutes	19 hours	3 days	3 weeks
10	Instantly	58 minutes	1 month	7 months	5 years
11	2 seconds	1 day	5 years	41 years	400 years
12	25 seconds	3 weeks	300 years	2k years	34k years
13	4 minutes	1 year	16k years	100k years	2m years
14	41 minutes	51 years	800k years	9m years	200m years

précédemment. Un mot de passe de 12 caractères devrait être un minimum pour une sécurité optimale et il ne doit même pas être vraiment complexe. Pour le rendre inviolable pendant au moins 300 ans, il suffit d'un mot de passe comportant des lettres minuscules et majuscules. Il convient de noter qu'il est strictement déconseillé d'utiliser son propre nom comme mot de passe, car il peut être facilement craqué, quelle que soit sa longueur.

Chapitre 3 – Connexion Internet sécurisée

Il est bien connu qu'Internet est une source d'information et de divertissement fiable mais dangereuse. En raison de la quantité de logiciels malveillants, d'espions et de pirates qui n'attendent qu'une bonne occasion pour attaquer, il est crucial de savoir comment s'en défendre, car parfois, un bon mot de passe ne suffit pas. Il existe de nombreux moyens de renforcer la sécurité d'une connexion Internet, et beaucoup d'entre eux ne nécessitent pas de connaissances technologiques avancées.

Pour commencer, il est conseillé de mettre en place une **authentification à deux facteurs** (2FA) chaque fois que cela est possible. À elle seule, elle peut dissuader la plupart des pirates de s'introduire dans le compte d'une personne. Il s'agit d'une deuxième couche de vérification lors de la connexion à un compte. Si la première est généralement un mot de passe, la seconde est souvent une clé unique envoyée au numéro de téléphone portable de l'utilisateur, qui doit être saisie après la connexion avec un mot de passe. On considère qu'il s'agit d'une méthode très efficace pour protéger les utilisateurs contre le risque de vol de leur mot de passe, car l'unicité de la clé rend l'accès à un compte beaucoup plus difficile pour un pirate.

Une autre bonne pratique consiste à utiliser un **réseau privé virtuel** (VPN). Chaque fois qu'une personne se connecte à un réseau, un flux de données est échangé entre l'utilisateur et les serveurs. Le VPN crée une connexion sécurisée entre ces deux parties en cryptant les données avant qu'elles ne soient envoyées ou reçues par les utilisateurs. Un VPN cache l'adresse IP et l'emplacement de l'utilisateur, de sorte que les cybercriminels ne peuvent plus découvrir l'emplacement de leurs victimes potentielles car, grâce au VPN, ils les suivraient jusqu'à l'emplacement du serveur VPN, ce qui rendrait beaucoup plus difficile la consultation de leurs données. Il s'agit d'un excellent outil pour sécuriser la connexion lors de l'utilisation de réseaux Wi-Fi publics dans des endroits comme les aéroports ou les restaurants, qui sont facilement piratables.

Source: freepik.com

Pour mettre en place ce type de connexion, il est nécessaire de trouver un fournisseur de services VPN fiable et de s'y abonner. Il existe quelques fournisseurs sur le marché qui proposent leurs services gratuitement mais il est conseillé d'acquérir un abonnement payant car il offre plus de fonctionnalités pour une connexion plus sûre. Une fois le fournisseur de VPN préféré trouvé, l'utilisateur sera invité à télécharger le logiciel nécessaire. Il doit toujours être téléchargé directement depuis le site Web du fournisseur, car le téléchargement depuis une autre source peut entraîner le téléchargement de fichiers contenant des logiciels malveillants. La plupart des applications VPN sont disponibles sur une grande variété d'appareils et leur processus de configuration est accessible à tous. Une fois l'application téléchargée et le compte créé, il ne reste plus qu'à l'activer et à ne plus craindre que quelqu'un ne pirate notre appareil.

La modification du nom et du mot de passe par défaut du routeur peut également contribuer à la protection du réseau. Chaque routeur est livré avec un nom et un mot de passe génériques, qui sont nécessaires pour le configurer pour la première fois. Ensuite, une bonne pratique consiste à changer son nom et son mot de passe pour quelque chose d'unique, en gardant à l'esprit les directives pour créer un mot de passe fort. Il en est ainsi parce que les noms des routeurs (SSID - service set identifier)

contiennent le plus souvent la marque et le modèle dans leur nom, ce qui permet aux pirates de trouver plus facilement les routeurs qu'ils savent être vulnérables aux violations. Il est également possible de masquer complètement le SSID d'un routeur, de sorte que les chances qu'un pirate découvre la connexion sont proches de zéro.

Source: freepik.com

Gardez tout à jour. La mise à jour semble généralement être un souci inutile, et peut même parfois faire fonctionner un appareil plus mal qu'avant, en ajoutant de nouvelles fonctionnalités qui ne sont pas nécessaires ou en supprimant celles qui étaient utiles. Il est important de prêter attention à toutes les notifications de mise à jour qui peuvent apparaître. Tout logiciel n'est pas sans défaut. La plupart d'entre eux contiennent des vulnérabilités cachées dont même les développeurs n'étaient pas conscients au départ. Une fois découvertes, celles-ci peuvent être exploitées par les pirates. C'est la raison pour laquelle chaque logiciel a besoin de versions plus récentes qui corrigent les points vulnérables. C'est très important du point de vue de la sécurité en ligne, car le fait de tout mettre à jour réduit également les chances de réussite d'une attaque de pirates. Les utilisateurs qui surveillent régulièrement la mise à jour de leurs logiciels réduisent les risques de cyberattaque visant leurs appareils, car il est possible que les anciennes vulnérabilités susceptibles d'être utilisées par les pirates soient déjà corrigées. Il est possible que la mise à jour interrompe certaines fonctions du logiciel, voire le rende inutilisable sur certains appareils, c'est pourquoi, une fois la mise à jour effectuée, il est bon de vérifier si la mise à jour n'a rien interrompu. En

outre, les logiciels qui ne sont pas mis à jour peuvent manquer les nouvelles fonctions qui sont très pratiques. D'autre part, les anciennes versions du logiciel peuvent tout simplement cesser de fonctionner sur les appareils plus récents ou ceux qui sont maintenus à jour. Même si les mises à jour peuvent sembler un peu longues, elles sont très importantes, non seulement pour des raisons de sécurité, mais aussi pour disposer de toutes les dernières fonctions d'un appareil ou d'un logiciel donné. Une bonne pratique serait de faire une vérification hebdomadaire des logiciels utilisés en termes de mise à jour. Il s'agit d'un moyen simple et rapide de sécuriser les données et de renforcer les performances du logiciel utilisé.

Un logiciel antivirus est indispensable, et il devrait être installé sur chaque appareil. Il n'est pas difficile d'être victime d'une attaque par hameçonnage et, de nos jours, avec la popularité croissante du travail à distance, l'infection d'un ordinateur par un virus peut entraîner une interruption obligatoire du travail pendant des jours, voire des semaines. Un antivirus est un logiciel qui vérifie chaque fichier ou élément de données installé ou en cours d'installation sur un ordinateur. Il est conçu pour déterminer si l'un des fichiers d'un ordinateur peut constituer une menace potentielle ou causer des dommages aux utilisateurs et à leurs appareils. L'antivirus fonctionne de deux manières différentes. L'une d'entre elles est une méthode **basée sur la signature** qui fonctionne comme une liste de fichiers connus contenant des logiciels malveillants qui sont publiés par les sociétés d'antivirus. Lorsqu'une correspondance est trouvée entre le fichier de la liste et l'appareil de l'utilisateur, il est bloqué. Il s'agit d'une méthode courante qui fonctionne bien, car des milliers de logiciels malveillants sont découverts chaque jour, de sorte que la liste est vraiment riche en données. Le seul inconvénient de cette méthode est qu'une fois que l'appareil de l'utilisateur est infecté par un virus qui ne figure pas sur la liste, il peut ne pas en être protégé. L'autre façon dont les antivirus protègent les appareils est **basée sur le comportement.** Celle-ci est plus complexe et n'est pas aussi couramment utilisée que les autres méthodes, et seuls les antivirus les plus avancés l'utilisent. Comme son nom l'indique, cette méthode étudie le comportement d'un fichier donné et détermine si ce fichier peut

être dangereux pour l'appareil. Elle vérifie toute tentative de modification ou de cryptage des données de l'appareil, puis le bloque en le signalant comme un virus.

Source: freepik.com

Les antivirus protègent les utilisateurs non seulement en bloquant les fichiers qui se trouvent sur leurs appareils, mais la plupart d'entre eux empêchent également les utilisateurs d'accéder à des sites non autorisés susceptibles de menacer leurs appareils. Certains de ces programmes peuvent également nettoyer les "fichiers indésirables" afin de libérer de l'espace sur l'appareil. Cette procédure peut parfois aussi augmenter la vitesse de traitement d'un ordinateur ou d'un smartphone. L'antivirus est un composant essentiel de tout appareil susceptible d'être infecté par des données malveillantes, et il offre un large éventail d'avantages qui agissent comme une porte fermée ne laissant pas entrer les virus et repoussant les virus existants.

Grâce à toutes ces suggestions, il est extrêmement rare que quelqu'un soit victime d'une cyberattaque, et même si quelqu'un tente de voler les données de l'ordinateur de quelqu'un, il est extrêmement improbable qu'il y parvienne.

Chapitre 4 – RGPD et sécurité des informations personnelles

Le règlement général sur la protection des données (RGPD), qui est entré en vigueur le 25 mai 2018, trouve ses origines dans les années 1950. C'est alors que la Convention des droits de l'homme a été créée, posant les premières bases de la protection des données personnelles. Trois décennies plus tard, avec l'essor de l'informatique, la Convention sur la protection des données a été créée, déclarant que la vie privée était, en fait, un droit humain. Le 24 octobre 1995, la directive sur la protection des données a vu le jour pour réglementer les lois sur la protection des données et le transfert des données personnelles en dehors de l'Union. 17 ans plus tard, une mise à jour de cette réglementation a été proposée et, 4 ans après cette proposition, le Règlement général sur la protection des données a été adopté par le Parlement européen pour devenir

pleinement applicable dans toute l'Union européenne deux ans plus tard, en mai 2018.

Source: freepik.com

L'objectif principal du RGPD est de donner aux citoyens de l'UE un plus grand contrôle sur leurs données personnelles. Il s'agit d'un ensemble massif de 99 articles qui régissent les règles de protection des données et la manière dont les données peuvent être consultées. Il a remplacé la précédente directive sur la protection des données de 1995, car l'environnement technologique était très différent de ce qu'il est

aujourd'hui. Aujourd'hui, presque chaque citoyen européen possède au moins un smartphone, et les entreprises proposant des biens ou des services en ligne sont devenues aussi populaires que leurs équivalents traditionnels. Avec le GDPR, il est plus facile de contrôler quelles informations personnelles peuvent être stockées, partagées ou collectées par diverses parties. Ces informations peuvent aller des adresses IP aux habitudes alimentaires d'une personne en passant par ses revenus mensuels.

Dans le cadre du RGPD, il existe 7 principes fondamentaux qui doivent servir de guide sur la manière dont les données des utilisateurs doivent être gérées. Ces règles peuvent être perçues comme un cadre conçu pour montrer l'objectif principal du règlement. Parmi ces 7 règles, on trouve :

- Légalité, équité et transparence

Cela signifie que les données doivent être stockées et traitées de manière légale. Elles ne doivent pas induire en erreur les autres utilisateurs quant à la manière dont elles sont stockées et utilisées.

- Limitation de l'objectif

Cela suggère que les données à caractère personnel soient collectées et conservées pour des finalités claires, non ambiguës et légales et qu'elles ne soient pas traitées ultérieurement de manière contradictoire avec ces finalités.

- Précision

Cela signifie que toutes les mesures raisonnables doivent être prises pour garantir que toute donnée personnelle inexacte est immédiatement effacée ou corrigée. Les données à caractère personnel doivent être exactes et, si nécessaire, mises à jour.

- Minimisation des données

Les organisations ne devraient pas collecter plus de données qu'elles n'en ont besoin auprès de leurs utilisateurs. Les données doivent être adéquates et limitées à ce qui est nécessaire au regard des objectifs pour lesquels elles sont traitées.

- Limitation de stockage

Cela signifie que les données ne doivent pas être conservées plus longtemps que nécessaire.

- Intégrité et confidentialité

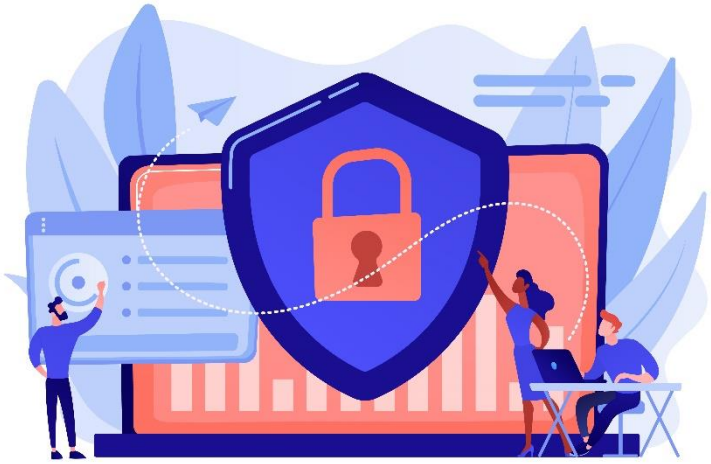
En d'autres termes, il s'agit de la sécurité des données stockées. Elles doivent être traitées avec des mesures techniques ou organisationnelles adéquates pour garantir la meilleure sécurité possible des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illégal et contre la perte, la destruction ou les dommages involontaires.

- Responsabilité

Cela signifie que les entreprises doivent fournir la preuve qu'elles suivent les règles énumérées ci-dessus et s'assurer qu'elles prennent des mesures pour traiter les données personnelles de manière éthique.

Le RGPD a été conçu pour protéger les utilisateurs et leurs données. En gardant cela à l'esprit, ils ont fourni **huit droits** aux individus. Les plus importants sont :

- Le droit à l'information sur la collecte et l'utilisation des données personnelles.
- Le droit d'accéder, d'examiner et de recevoir une copie des données personnelles qui sont recueillies et traitées par certaines parties.
- Le droit d'obtenir l'effacement des données personnelles.



Source: freepik.com

Les cinq autres droits des personnes sont : le droit de rectification, le droit de restreindre le traitement, le droit à la portabilité des données, le droit d'opposition et le droit de ne pas être soumis à une prise de décision automatisée.

En raison de la prise de conscience croissante de la valeur des informations personnelles, les gens ont commencé à faire plus attention à la quantité de données qu'ils donnent aux entreprises, et préfèrent choisir les parties qui sont transparentes sur la collecte des données. Avec le RGPD, les entreprises doivent être plus attentives aux données qu'elles collectent et à la manière dont elles les sécurisent, en raison des amendes élevées associées au non-respect de la réglementation RGPD.

La connaissance du RGPD et des autres pratiques mentionnées dans ce guide peut non seulement garantir un niveau élevé de sécurité des informations personnelles de l'utilisateur, mais aussi rendre plus difficile aux cybercriminels de s'introduire dans les bases de données des entreprises. Des mots de passe forts et des connaissances sur les différentes pratiques malveillantes telles que le phishing et les virus, s'ils sont appliqués et compris correctement, peuvent permettre aux personnes travaillant à distance de se sentir beaucoup plus en sécurité à une époque où le télétravail est devenu une pratique courante dans le monde entier.

Chapitre 5 – Activité pratique

Exercice 1. Créer un mot de passe fort et mémorable

Un mot de passe fort est long, compliqué et contient beaucoup de symboles, mais il est aussi facile à retenir. En gardant cela à l'esprit, créons-en un en suivant ces quelques étapes simples :

1. Pensez à une phrase ou à une citation à laquelle vous pensez souvent. Par exemple, une célèbre citation de Wayne Gretzky :
   Vous ratez 100 % des tirs que vous ne faites pas.
2. Maintenant, faites un acronyme de cette citation en anglais :
   Y(ou) **m**(iss) **100 p**(ercent) **o**(f) **t**(he) **s**(hots) **y**(ou) **d**(‘ont) **t**(ake) =
   Ym100potsynt
3. Maintenant, ajoutez-y des caractères spéciaux. Par exemple, changeons “1” avec “!”, “p” avec “%”, ajouter un trait de soulignement et mettez des majuscules, de sorte que l'effet final ressemblera à ceci :
   Ym!00%ots_Ydt

Le mot de passe semble compliqué, mais si nous l'analysons, nous constatons qu'il est assez simple et facile à retenir. Une bonne pratique consiste à s'entraîner à l'écrire pendant un certain temps, afin que notre mémoire musculaire se souvienne de l'ordre des boutons pressés.

Source: freepik.com

Exercice 2. Vérifiez que votre boîte aux lettres ne contient pas de SPAM ou d'éventuelles tentatives d'hameçonnage.

Nous avons appris à reconnaître les différents courriels malveillants qui peuvent nous être envoyé.

Ouvrez votre boîte aux lettres et vérifiez s'il n'y a pas de publicités pour des produits dont vous n'avez jamais entendu parler ou des notifications vous annonçant que vous allez gagner un prix. Vérifiez également les courriels suspects concernant des factures impayées ou des suspensions de compte. Analysez-les, mais **n'ouvrez en aucun cas** les liens ou les pièces jointes fournis dans les messages. Ensuite, effacez ces messages et réfléchissez au nombre d'e-mails suspects qui ont été envoyés.

Liens utiles :

Quel est le niveau de sécurité de votre mot de passe ? :
https://www.security.org/how-secure-is-my-password/

Comment installer une connexion VPN ? :
https://www.businessnewsdaily.com/15710-how-to-install-a-vpn-connection.html

4. Références

Anderson, S. (2022). *What Is Phishing? Guide with Examples for 2022*. SafetyDetectives. Retrieved May 10, 2022, from https://www.safetydetectives.com/blog/what-is-phishing-and-how-to-protect-against-...

Awati, R., & Teravainen, T. (2021). *What is email spam and how to fight it?* SearchSecurity. Retrieved May 9, 2022, from https://www.techtarget.com/searchsecurity/definition/spam?msclkid=9aeb4557cf8211ec82e6cfc07708ec54

Barracuda. (2020). *Spear Phishing: Top Threats and Trends* (Vol. 5). Barracuda. Retrieved May 10, 2022, from https://lp.barracuda.com/rs/326-BKC-432/images/BEU-AMER-Spear-Phishing-Vol5...

Castagna, R., & Lavery, T. (2021). *General Data Protection Regulation (GDPR)*. WhatIs.Com. Retrieved June 24, 2022, from https://www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR

Cheema, A. N., & Aamir, R. (2021). Trends of cyber crimes. *Proc. 18th International Conference on Statistical Sciences*, *35*, 261–269. https://www.researchgate.net/profile/Muhammad-Suhail-6/publication/353070981_Comparison_of_Ridge...

Chng, S., Han Yu, L., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, *5*. https://doi.org/10.1016/s2451-9588(22)00018-5

Digital Marketing Experts – Editorial Review Board. (2021). *The Importance of Updating*. THAT! Company. Retrieved June 24, 2022, from https://www.thatcompany.com/the-importance-of-updating...

D'Mello, Y. (2018). *How did we get here? A brief history of the GDPR*. AiThority. Retrieved June 24, 2022, from https://aithority.com/technology/analytics/how-did-we-get-here-a-brief-history-of-the-gdpr/

Edwards, R. (2022). *How Can I Secure My Internet Connection?* SafeWise. Retrieved June 24, 2022, from https://www.safewise.com/online-security-faq/secure-internet-connection/

Elvin, A. E., Sundström, F., & von Heland, W. (2021). *Understanding the Effects of Cyber Security Risks and Threats on Forced Teleworking Organizations* (Master's dissertation). Department of Informatics, Lund School of Economics and Management, Lund University. Retrieved June 24, 2022, from https://lup.lub.lu.se/student-papers/search/publication/9052971

FIT Information Technology. (2022). *What is antivirus and why is it important?* Retrieved June 24, 2022, from https://it.fitnyc.edu/what-is-antivirus-and-why-is-it-important/

Fogg, S. (2022). *What is GDPR? The Basics of the EU's General Data Protection Regulation*. Termly. Retrieved June 24, 2022, from https://termly.io/resources/articles/what-is-gdpr/

Fruhlinger, J. (2020). *Ransomware explained: How it works and how to remove it*. CSO Online. Retrieved May 11, 2022, from https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it...

Gajić, A. (2022). *Spam Statistics*. 99firms. Retrieved May 9, 2022, from https://99firms.com/blog/spam-statistics/?msclkid=18264839cf8b11ec8144c5ced7add618

General Data Protection Regulation (GDPR) – Official Legal Text. (2019). General Data Protection Regulation (GDPR). Retrieved June 24, 2022, from https://gdpr-info.eu/

Gibson, K. (2022). *6 Famous Identity Theft Cases in Recent Years*. Home Security Heroes. Retrieved May 12, 2022, from https://www.homesecurityheroes.com/famous-identity-theft-cases/

Gupta, M. (2021). Identity Theft in Cyberspace in India. *International Journal of Research Publication and Reviews*, *2*(7), 1700–1701. https://www.ijrpr.com/uploads/V2ISSUE7/IJRPR791.pdf

Hiley, C. (2021). *Brief history of cybersecurity and hacking*. CyberNews. Retrieved May 11, 2022, from https://cybernews.com/security/brief-history-of-cybersecurity-and-hacking/?msclkid=ebaaa52cd10911ecbb48b6bc018d0384

Jančis, M. (2022). *How to create a good and strong password*. CyberNews. Retrieved June 16, 2022, from https://cybernews.com/best-password-managers/how-to-create-a-strong-password/

Janssen, D. (2022). *VPN Explained: How Does It Work? Why Would You Use It?* VPNoverview.Com. Retrieved June 1, 2022, from https://vpnoverview.com/vpn-information/what-is-a-vpn/

Johansen, A. G. (2018). *What to Do If Your Identity Is Stolen: 14 Steps*. LifeLock. Retrieved May 12, 2022, from https://www.lifelock.com/learn/identity-theft-resources/do-these-things-immediately-if-your-identity-has-been-stolen

Lopez, A. (2021). *Top 10 Reasons Why an Antivirus Is Important*. Business 2 Community. Retrieved June 24, 2022, from https://www.business2community.com/cybersecurity/top-10-reasons-why-an-antivirus-is-important...

Malwarebytes. (n.d.). *What is spam?* Retrieved May 11, 2022, from https://www.malwarebytes.com/spam...

Martens, B. (2021). *The Ultimate Internet Safety Guide for Seniors (2022)*. SafetyDetectives. Retrieved June 24, 2022, from https://www.safetydetectives.com/blog/the-ultimate-internet-safety-guide-for-seniors/?msclkid=9e7ed272cf5f11ecbe3d195abee11879

Milasi, S., González-Vázquez, I., & Fernández-Macías, E. (2020). *Telework in the EU before and after the COVID-19: Where we were, where we head to*. Joint Research Centre. Retrieved June 24, 2022, from https://joint-research-centre.ec.europa.eu/system/files/2021-06/...

Minahan, B. (2020). *How to Create a Strong Password in 6 Easy Steps*. aNetworks. Retrieved June 1, 2022, from https://www.anetworks.com/how-to-create-a-strong-password-2021/

Mitra, A. (2017). *What is a spambot and how to stop spambots?* TheSecurityBuddy. Retrieved May 11, 2022, from https://www.thesecuritybuddy.com/anti-spam/what-is-spambot-and-how-to-stop-spambots...

Molinaro, D. (2022). *How Does Two-Factor Authentication (2FA) Work?* Avast. Retrieved June 1, 2022, from https://www.avast.com/c-how-does-two-factor-authentication-work...

Movassagh, N. (2021). *Awareness and perception of phishing variants from Policing, Computing and Criminology students in Canterbury Christ Church University.* (Master's dissertation). Canterbury Christ Church University School of Law. https://repository.canterbury.ac.uk/item/8yq89/awareness-and-perception-of-phishing-variants-from-policing-computing-and-criminology-students...

Peterson, S. (2019). *The Ultimate Guide for Online Security and Privacy in 2020*. The Hack Post. Retrieved June 1, 2022, from https://thehackpost.com/the-ultimate-guide-for-online-security-and-privacy-in-2020.html

Proofpoint. (n.d.). *What is Email Spoofing? Definition & Examples*. Retrieved June 24, 2022, from https://www.proofpoint.com/us/threat-reference/email-spoofing?msclkid=df4910a2d03511ecb958bcffa531b6ab

Spoofing and Phishing. (2022). Federal Bureau of Investigation. Retrieved May 10, 2022, from https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing?msclkid=8cb3cf19d04d11ecb7c47a9f8893c5e8

Tanwar, R., Choudhury, T., Zamani, M., Gupta, S., & Tajpour, A. (2021). Information Security and Optimization. In *Information Security and Optimization* (pp. 25–26). CRC Press. Retrieved May 10, 2022, from https://books.google.nl/books?id=...

TechFunnel Contributors. (2020). *Most Common Hacking Techniques for Beginners*. Techfunnel. Retrieved May 11, 2022, from https://www.techfunnel.com/information-technology/hacking-techniques/?msclkid=94348692d12111eca373f0ead6ff7fe9

Tschabitscher, H. (2021). *What Is an Example of Spam Email?* Lifewire. Retrieved May 9, 2022, from https://www.lifewire.com/what-and-why-spam-email-1173993#toc-what-are-some-examples-of-spam

Tsonchev, A. (2020). *Six of the biggest security threats facing the remote workforce*. TechRadar. Retrieved June 24, 2022, from https://www.techradar.com/news/six-of-the-biggest-security-threats-facing-the-remote-workforce?msclkid=9e80a80ccf5f11ec92c0ce7275373494

Williams, L. (2022). *What is Hacking? Types of Hackers | Introduction to Cybercrime*. Guru99. Retrieved June 24, 2022, from https://www.guru99.com/what-is-hacking-an-introduction...

Source de la photo en page de garde : freepik.com