SMART 04

Sécurité de vos appareils numériques

Ce module décrit certains aspects importants concernant la sécurité auxquels il faut faire attention lorsque vous utilisez cette technologie.

Commencer >

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

SMART **MODULE 4**

Sécurité de vos appareils numériques

Au cours des dernières décennies, les appareils connectés sont passés d'une simple fonction d'appel à de nombreux autres usages. Ils ont permis l'accès mobile aux services bancaires, aux applications et à Internet. Ces nouvelles fonctionnalités s'accompagnent d'une préoccupation pour la sécurité des données. Dans ce module, nous vous expliquerons ce qu'est la protection des données, comment créer et modifier des mots de passe, comment sécuriser la navigation en Wi-Fi, et comment vous protéger de la cyberintimidation et des trolls d’Internet.

Public visé

Ce module s'adresse à toute personne souhaitant s'informer sur la navigation sécurisée en ligne, la protection des données, les cookies et la manière dont la loi protège ses informations personnelles (RGPD).

Ce matériel peut représenter un défi pour certains apprenants. Dans ce cas, il serait utile de travailler sur le contenu avec un compagnon ou un ami.

Les animateurs pourront utiliser ce matériel pour s'informer et donner des conseils sur la sécurité dans les nouvelles technologies.

Ce que vous allez apprendre dans ce module

1. Protection des données EU/US RGPD et consentement aux cookies.
2. Comment créer et modifier des mots de passe.
3. Qu'est-ce que le piratage informatique et comment s'en protéger ?
4. Comment se protéger du cyber-harcèlement.

Chapitres de ce module

Introduction à la sécurité mobile et à la propriété des données

"L'information, c'est le pouvoir !" Les informations personnelles sont l'un de nos biens les plus précieux. À l'ère moderne, cette ressource importante est totalement sous-évaluée par les consommateurs, mais pas par les entreprises ! Certaines des plus grandes entreprises du monde ont réussi grâce à l'utilisation intelligente de vos données. Ce chapitre explique la propriété des données à l'ère de l'informatique mobile et du "cloud".

Ce que vous allez apprendre dans ce chapitre

1. Qu'est-ce que le règlement général sur la protection des données ?
2. Protection des données personnelles dans le cadre du RGPD.
3. Comment gérer les cookies ?
4. Types de données à caractère personnel.
5. Où sont stockées vos données ?
6. Comment sauvegarder les données de votre appareil connecté ?

L'analyse des données est l'un des secteurs connaissant la plus grande croissance

La collecte et l'analyse des données sont importantes pour les entreprises afin de comprendre les besoins des clients. L'analyse des données a aidé les entreprises à améliorer leur service client.

L'analyse des données rend les sites web et les applications plus faciles à utiliser et permet, par exemple, à l'utilisateur d'une montre intelligente de connaître le nombre de pas effectués en une journée. L'analyse des données est souvent appliquée à (vos) **données personnelles**.

Données personnelles et appareils sans fils

Les **données personnelles** sont des informations qui se rapportent à une personne identifiable.

Les entreprises doivent protéger les informations personnelles des citoyens en vertu de la loi sur **le règlement général sur la protection des données (RGPD)** en codant les **informations** sensibles qui sont stockées ou sont envoyées sur les réseaux publics.

Le RGPD sera abordé plus loin dans ce chapitre.

Pourquoi il est important de sécuriser les données recueillies par les appareils connectés

Lorsqu'une personne ou une organisation a accès sans consentement ni autorisation à des informations personnelles - adresse, âge et sexe, problèmes de santé, situation financière, intérêts, etc. - cela peut poser des problèmes à la personne dont les données sont collectées.

Les **données personnelles** sont des données qui se rapportent à une personne identifiable. Ces informations permettent de personnaliser un service pour vous. Les entreprises doivent protéger vos informations personnelles en vertu de la loi **RGPD** en chiffrant les **informations** sensibles comme les exemples de données personnelles présentés ci-dessus, envoyées à des tiers sur des réseaux publics.

Vous trouverez des informations plus détaillées à ce sujet sur le site https://gdpr-info.eu/.

Qu'est-ce que le RGPD ?

Pour empêcher les entreprises d'obtenir les données personnelles des citoyens sans leur consentement, la Commission européenne a introduit le **Règlement général sur la protection des données (RGPD).**

Le RGPD protège les données personnelles des citoyens qui vivent et travaillent au sein de l'Union européenne. Les organisations opérant dans l'UE doivent obtenir le consentement des citoyens pour traiter leurs données personnelles.

RGPD - Quels sont les droits au sein de l'UE ?

Le RGPD offre les droits suivants aux individus :

- le droit d'être informé
- le droit d'accès
- le droit de rectification et d'effacement
- le droit de restreindre le traitement
- le droit à la portabilité des données
- le droit d'opposition
- droits concernant le profilage automatisé

Quels types de données pourraient être considérés comme des données personnelles ?

Afin de comprendre l'importance des droits à la confidentialité des données dans l'UE, nous devons connaître les types de données personnelles qui pourraient être affectées par le RGPD.

Examinons quelques exemples typiques de types de données qui pourraient être considérées comme des données personnelles et qui méritent donc d'être protégées.

Exemples de données à caractère personnel

1

2

3

Les informations démographiques sont des données à caractère personnel

Lorsqu'une personne remplit un formulaire pour, par exemple, demander une subvention, elle fait confiance à l'organisation qui établit le formulaire pour traiter les informations sensibles de manière confidentielle. Il s'agit d'un type de données à caractère personnel.

Exemples de données à caractère personnel

1

2

Les dossiers médicaux contiennent des données personnelles

Une visite chez le médecin est considérée comme un rendez-vous confidentiel. Les données enregistrées sur un patient sont également confidentielles et peuvent donc être considérées comme des données personnelles.

3

Exemples de données à caractère personnel

1

2

3

Un enregistrement des activités quotidiennes est une donnée personnelle

Un registre des achats effectués, des lieux visités et des voyages effectués par une personne est également une donnée à caractère personnel.

Activités quotidiennes

Les appareils mobiles et les appareils sans fils enregistrent un niveau extraordinaire de détails sur les activités quotidiennes d'une personne. La plupart de ces données personnelles se retrouvent dans les bases de données associées aux applications mobiles et portables du cloud. En disposant de ces données, les entreprises informatiques peuvent vous fournir des informations détaillées sur vos activités.

Types de données à caractère personnel

4

5

Les informations financières individuelles sont des données à caractère personnel

Les états de finance, les crédits et les relevés bancaires constituent une autre catégorie de données personnelles. Elles peuvent être utilisées pour vous classer dans la catégorie des personnes dépensières ou des acheteurs prudents.

Types de données à caractère personnel

4

5

Les images ou les enregistrements de personnes sont des données à caractère personnel

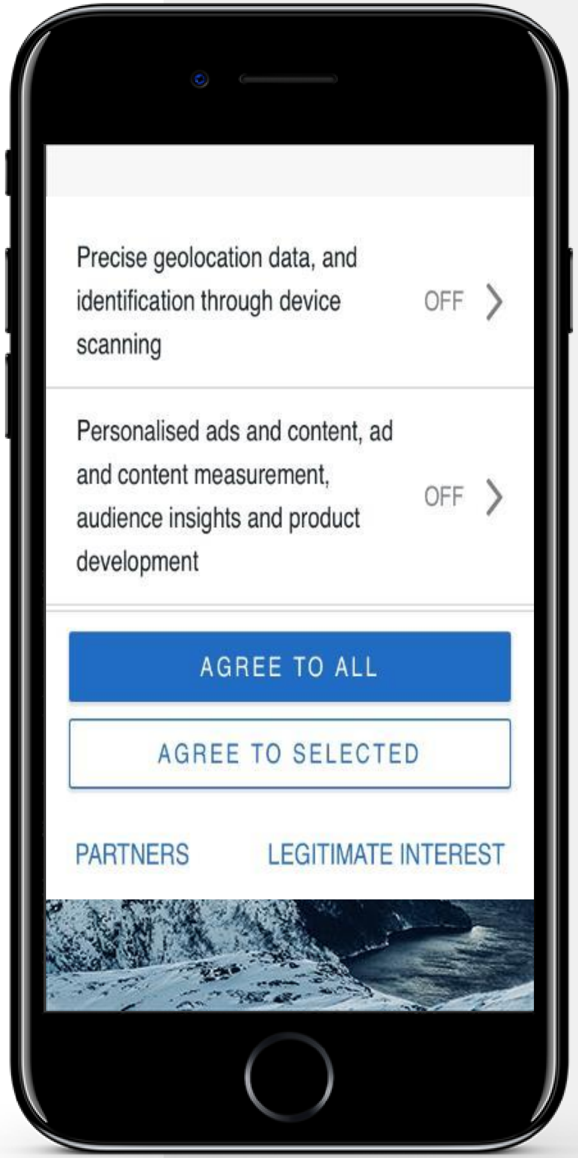
Les propriétaires de caméras de sécurité doivent faire attention au stockage des séquences vidéo, car elles peuvent contenir des données personnelles. Il en va de même pour les enregistrements sonores. Les deux ne doivent être conservés qu'avec le consentement des personnes enregistrées.

Cookies : consentement pour fournir des données personnelles à une entreprise

Les cookies sont de petits fichiers que les sites web envoient à votre appareil numérique pour mémoriser certaines informations vous concernant. Par exemple, vos préférences sportives ou les détails de votre connexion.

En vertu de la réglementation RGPD, un site web doit obtenir le consentement d'un utilisateur pour installer des cookies sur son appareil.

Si vous craignez que vos données soient analysées, vous pouvez sélectionner les options "Rejeter tout" ou "Accepter la sélection" (comme indiqué dans l'image ci-dessous). La désactivation des cookies signifie que le site web n'est pas personnalisé et ne peut pas se rappeler des détails tels qu'un mot de passe ou des achats.



Faux messages - Attention !

Parfois, des messages intéressants apparaissent sur votre appareil numérique. Lorsque vous voyez un message pour un cadeau ou une histoire qui semble trop belle pour être vraie, il s'agit généralement d'un piège peut-être destiné à vous voler de l'argent.

Lorsqu'un message de ce type est reçu, il est important de **ne pas remplir de** formulaire, de **ne pas** cliquer sur un lien ou de **ne pas** communiquer d'informations personnelles, telles que des numéros de téléphone, des adresses électroniques ou des adresses postales, à moins de savoir qu'elles proviennent d'une source fiable.

De même, les informations que vous lisez sur votre appareil peuvent être des "fake news", c'est-à-dire des informations fausses ou fabriquées.

Qu'est-ce que le cloud ?

Ce que l'on appelle le "cloud" est un réseau mondial d'ordinateurs puissants, et les logiciels qui fonctionnent sur ces ordinateurs. Vos données personnelles peuvent être collectées et stockées dans un ordinateur du cloud n'importe où dans le monde. Les données que vous avez créées peuvent également être stockées dans le cloud et vous pouvez y accéder à partir de plusieurs appareils numériques.

Le stockage et l'analyse s'effectuent sur des ordinateurs du cloud dans un data center, et non sur l'appareil de l'utilisateur.

https://www.cloudflare.com/en-gb/learning/cloud/what-is-the-cloud

Le cloud est très utile pour les appareils numériques

Problème : le stockage du dispositif est limité

La plupart des appareils numériques n'ont qu'une capacité de stockage et une puissance de calcul limitées. À un moment donné, l'espace de stockage sera épuisé et le traitement sera lent.

Solution : stocker et analyser les données dans le cloud

Les fichiers, les photos et les vidéos peuvent être copiés sur le cloud, il est malgré tout bon de conserver des copies. Les ordinateurs du cloud sont très puissants, cependant il est important de se rappeler que la sécurité du cloud peut être un problème.

Sécurité du cloud

Alors, dans quelle mesure les données sont-elles sécurisées lorsqu'elles ont quitté votre appareil numérique et sont stockées sur un ordinateur du cloud ?

Même en dehors des entreprises qui utilisent les données des utilisateurs pour vendre plus de produits, les données personnelles du cloud peuvent être piratées et utilisées à des fins criminelles. La sécurité du cloud est importante pour les données personnelles et les appareils connectés. Assurez-vous que votre fournisseur de services est basé dans l'UE.

Données dans le cloud : où conserver vos fichiers ? Localement ou dans le cloud?

Avantages

- Personnalisation et amélioration du service.
- Plus d'espace de stockage, car un appareil numérique a un espace de stockage limité.
- Plus de données pour des décisions plus avisées.
- Toutes les données semblent se trouver "au même endroit".

Inconvénients

- L'utilisateur accepte une perte de confidentialité des données au profit du fournisseur de services du cloud.
- Possibilité de vol et de fraude.
- Une fois que les données sont dans le cloud, il est extrêmement difficile de les supprimer.

Quiz

Click the **Quiz** button to edit this object

Le RGPD protège votre droit d'être informé de la manière dont vos données seraient utilisées.

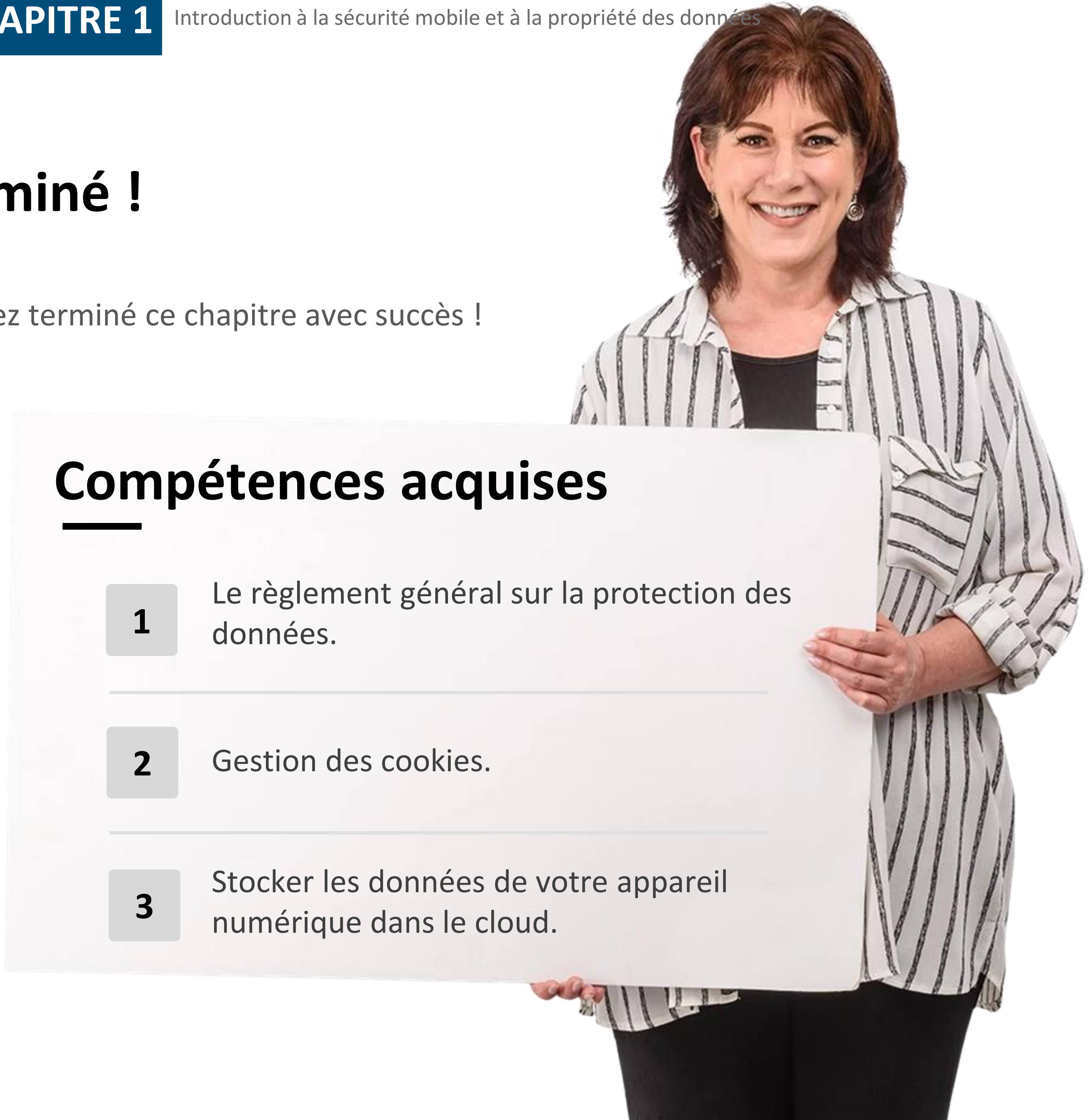
- Vrai
- Faux

Résumé du chapitre

1. Confidentialité des données.
2. Comment le règlement général sur la protection des données protège vos données.
3. Gestion des cookies.
4. Comprendre le cloud.
5. Comprendre comment vos données sont stockées dans le cloud.
6. Ce chapitre vous permettra d'acquérir une connaissance pratique de la confidentialité des données mobiles.

Chapitre terminé !

Félicitations ! Vous avez terminé ce chapitre avec succès !



Quelle est la prochaine étape ?

Maintenant, vous pouvez soit reprendre ce chapitre, soit commencer le chapitre suivant en cliquant sur l'un des boutons ci-dessous :

Recommencer

Suivant

Authentification

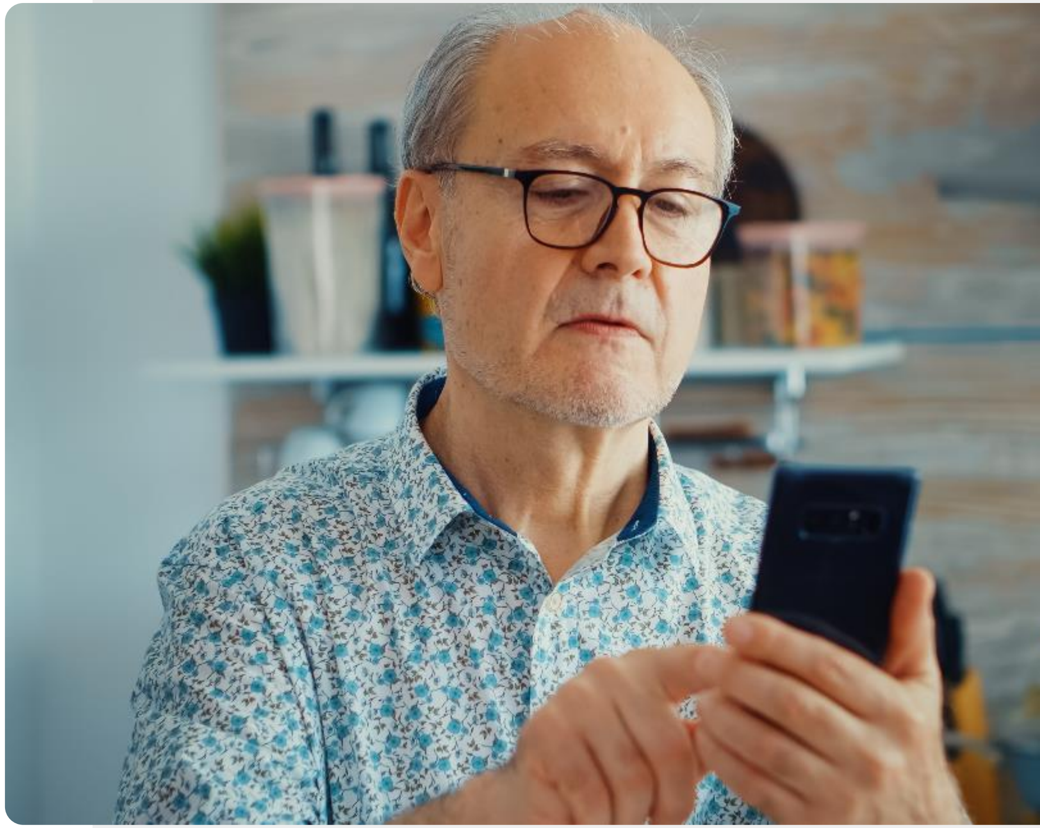
Dans ce chapitre, vous allez découvrir l'authentification d’un utilisateur. C’est le processus de reconnaissance de l'identité d’un utilisateur pour lui accorder l'accès à des services. La technologie d'authentification favorise la sécurité et la protection des informations personnelles. Vous apprendrez les types d'authentification et les approches biométriques de l'authentification, ainsi que la manière de créer des mots de passe forts.

Authentification - comment les appareils reconnaissent l'utilisateur actuel ?

L'authentification est la procédure qui consiste à reconnaître l'identité d'un utilisateur. Elle intervient souvent à l'ouverture d'une application et valide les utilisateurs pour s'assurer qu'un autre utilisateur ne consulte pas leurs données.

Différents systèmes exigent des informations différentes, appelées **justificatifs,** pour confirmer une identité. Ce justificatif est souvent un mot de passe, mais il peut aussi s'agir d'autres formes d'authentification.

(https://www.veriff.com/blog/what-is-authentication)



Ce que vous allez apprendre dans ce chapitre

1. Qu'est-ce que l'authentification et pourquoi en avez-vous besoin ?
2. Types d'authentification.
3. Comment créer un mot de passe fort.
4. Les différents types d'authentification biométrique.

Types d'authentification

Le nombre de méthodes d’identification d’un utilisateur d’un appareil numérique a augmenté rapidement au cours des dernières décennies.

Passons rapidement en revue quelques-uns des principaux types d'authentification qui peuvent être disponibles sur un appareil numérique.

Quelques types d'authentification

1

2

3

Authentification par mot de passe

Les mots de passe sont probablement la forme d'authentification la plus courante. Les mots de passe sécurisés contiennent généralement des lettres, des chiffres et d'autres caractères. Ce sujet sera abordé plus loin dans ce chapitre.

Quelques types d'authentification

1

2

3

Authentification par certificat

Un certificat numérique est un document électronique basé sur l'idée d'un permis de conduire ou d'un passeport. Un exemple est le certificat numérique qui montre les détails complets de la vaccination pour un vaccin COVID-19.

Quelques types d'authentification

1

2

3

Authentification biométrique

L'authentification biométrique est un processus de sécurité qui repose sur des caractéristiques uniques du propriétaire du dispositif, comme le visage, la voix ou les empreintes digitales. Nous verrons que les appareils numériques prennent en charge différents types d'approches d'authentification biométrique.

Quelques types d'authentification

4

5

Authentification par jeton

Cette approche permet aux utilisateurs de ne saisir les informations d'identification qu'une seule fois et crée une clé numérique secrète - le **jeton**. L'utilisateur peut utiliser le jeton comme ce billet de train pour accéder aux systèmes au lieu de saisir à nouveau ses informations d'identification.

Quelques types d'authentification

4

5

Authentification multiple (MFA)

Une fois que l'utilisateur a été identifié d'une manière ou d'une autre, un code est envoyé à l'appareil numérique pour que l'utilisateur le saisisse dans une application ou un site web. Il s'agit d'une **authentification à deux facteurs**.

Authentification par mot de passe

Choisissons quelques-uns de ces types d'authentification et examinons-les de plus près.

Le type d'authentification le plus populaire, et celui qui est utilisé sur les appareils numériques depuis de nombreuses années, est le mot de passe.

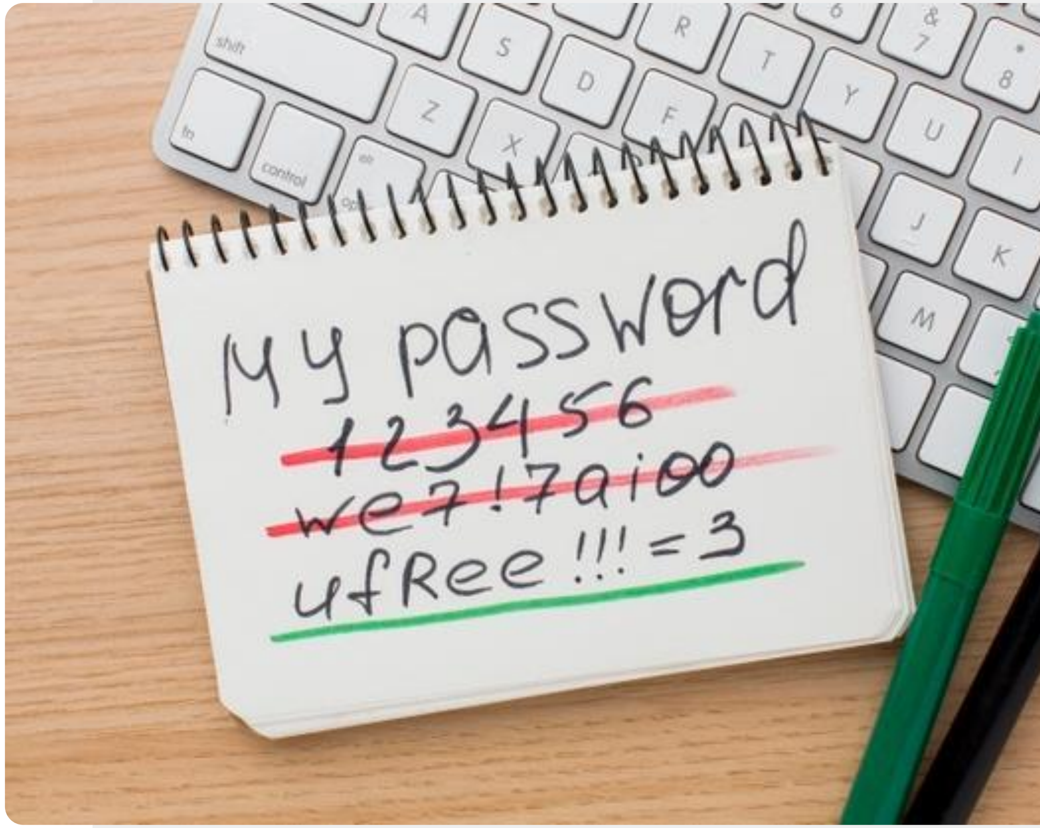
Le mot de passe de l'image est facile à deviner, il n'est donc pas très sûr. Peut-on faire mieux ?

Authentification des mots de passe : des mots de passe plus forts

De nombreux sites Web exigent que vous choisissiez un mot de passe qui présente certaines des propriétés suivantes

- Au moins 8 caractères
- Contient des lettres majuscules et minuscules
- Contient un numéro
- Contient un caractère de ponctuation

Voyons maintenant comment créer un mot de passe facile à retenir à l'aide de ces éléments.



Créer un mot de passe fort

1

2

3

Choisissez un mot que vous connaissez

Prenez un stylo et une feuille de papier. Écrivez un ou plusieurs mots longs ayant une signification forte pour vous, mais qui ne serait pas évidente pour quelqu'un d'autre. Cela peut être "patience", "Byzance" ou "antilope".

Créer un mot de passe fort

1

2

3

Remplacer certains caractères dans le mot ou la phrase

Utilisez des substitutions de caractères, par exemple :

1 = !   e = 3   a = @   8 = %   E =£   l =| S = $ S = 5

C =(T = +   G = 6   O = 0   I = 1   Z = 2   B = 8

Par exemple, **Caroline** pourrait devenir **(@rol1nE**

Créer un mot de passe fort

1

2

3

Utiliser le mot de passe d'un appareil ou d'un site web

Maintenant, détruisez soigneusement le mot de passe sur le papier ou mettez-le dans un endroit très sûr comme un coffre-fort.

Vous pouvez maintenant saisir le nouveau mot de passe fort sur un appareil ou un site Web.

Protégez votre mot de passe

Une fois que vous avez créé votre mot de passe, vous devez le protéger.

Il est préférable d'essayer de s'en souvenir, mais si vous décidez de l'écrire, il faut le conserver dans un endroit vraiment sûr.

Vous ne devez JAMAIS stocker un mot de passe avec ou à proximité de votre appareil numérique.

Faites le travail !

Antonio veut créer un mot de passe sécurisé. Comment doit-il s'y prendre ?

- ✓ Rencontrez et apprenez à connaître António. Vous pouvez trouver des informations sur António ici.
- ✓ António choisit la phrase **nolimits** comme mot de base pour son mot de passe.
- ✓ Suivez les étapes décrites pour aider António à créer un mot de passe fort à partir de **nolimits** en utilisant cette approche.

Mots de passe de l’appareil numérique et codes SIM

Les appareils numérique peuvent être configurés avec des **mots de passe** pour protéger les fichiers. Les **cartes SIM** d'un appareil le connectent à un réseau téléphonique et sont accompagnées d'un **code PIN** que vous saisissez pour accéder au réseau. Elles donnent accès aux contacts de votre carte SIM et, en cas de vol de l'appareil, la carte SIM peut également être déplacée vers un autre appareil pour utiliser votre crédit. Si le code PIN est saisi incorrectement 3 fois, un deuxième code appelé **code PUK** est nécessaire. C'est pourquoi il est important de conserver votre code PIN et votre code PUK dans un endroit sûr une fois que vous les avez obtenus avec votre appareil ou votre carte SIM.

Authentification biométrique

Nous avons mentionné qu'un système d'authentification biométrique reconnaît les caractéristiques uniques de l'utilisateur du dispositif pour lui permettre d'accéder au dispositif ou au système.

Passons maintenant en revue certaines de ces approches.

Authentification biométrique pour la technologie mobile

1

2

3

Scanners d'empreintes digitales

Les empreintes digitales sont uniques et peuvent donc être utilisées pour identifier un utilisateur. De nombreux appareils numériques modernes sont dotés d'un scanner d'empreintes digitales intégré, et l'utilisateur peut déverrouiller l'appareil en plaçant son doigt sur le scanner d'empreintes digitales pour le déverrouiller.

Authentification biométrique pour la technologie mobile

1

2

3

Scanner de la rétine

Tout comme les empreintes digitales, les motifs de l'œil sont uniques à chaque personne. La caméra de certains appareils numériques peut reconnaître le motif rétinien du propriétaire et l'utiliser pour déverrouiller l'appareil.

Authentification biométrique pour la technologie mobile

1

2

3

Reconnaissance faciale

Une autre approche similaire d'authentification de l'utilisateur est le scan facial. Là encore, une caméra est utilisée pour reconnaître les caractéristiques faciales uniques du propriétaire de l'appareil afin de déverrouiller ce dernier.

Faites le travail !

Tom souhaite utiliser l'authentification sur son appareil numérique. Pouvez-vous l'aider à choisir une approche appropriée ?

- ✓ Rencontrez et apprenez à connaître Tom. Vous pouvez trouver des informations sur Tom ici.
- ✓ Tom a travaillé dans une société du secteur informatique, il est donc un utilisateur averti de la technologie, mais il n'est pas familier des approches modernes d'authentification. Il aimerait sécuriser son smartphone, afin que d'autres personnes ne puissent pas accéder à ses informations.
- ✓ À partir des informations que vous avez apprises dans les diapositives précédentes, conseillez TOM sur l'approche d'authentification qu'il pourrait souhaiter utiliser.

Autorisation

Une fois que le dispositif a authentifié l'utilisateur, ce dernier a l'**autorisation** (permission) d'accéder au dispositif ou au système.

Un utilisateur peut avoir l'autorisation d'utiliser toutes les fonctions de l'appareil, ou seulement certaines d'entre elles.

Il est facile de confondre l'**authentification,** qui identifie l'utilisateur, et l'**autorisation, qui** intervient après.

Quiz

Click the **Quiz** button to edit this object

L'authentification est conçue pour protéger vos données.

- Vrai
- Faux

Résumé du chapitre

1. Vous avez appris ce qu'est l'authentification et comment elle est utilisée pour protéger votre accès et vos informations.

2. Vous avez vu un certain nombre de types d'authentification.

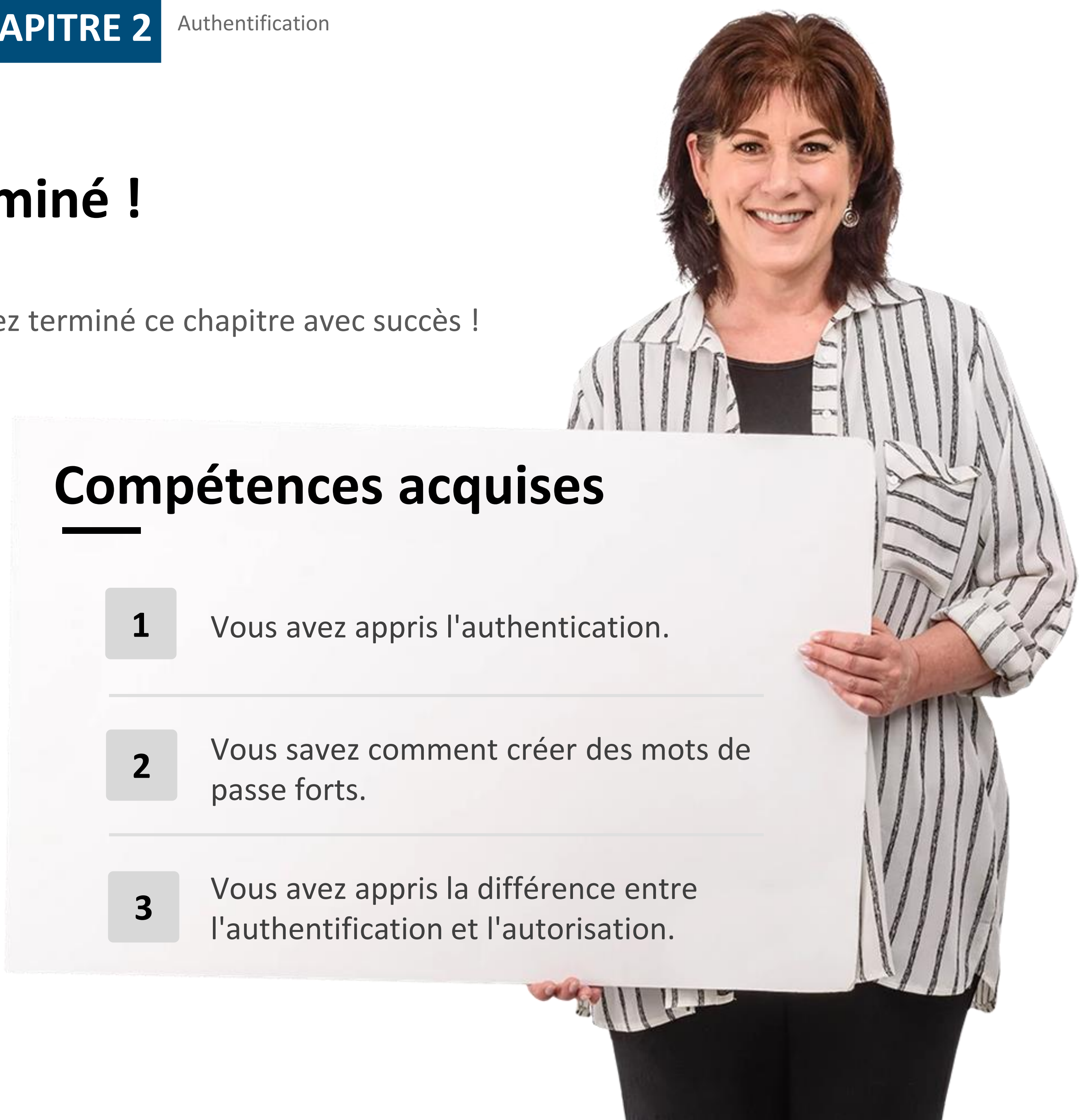
3. Vous avez appris à créer et à retenir vos mots de passe.

4. S'il vous plaît, essayez les fonctions de sécurité de votre appareil numérique. Ils le protégeront.

5. Nous espérons que vous pratiquerez la technique de création de mots de passe pour créer des mots de passe sûrs.

Chapitre terminé !

Félicitations ! Vous avez terminé ce chapitre avec succès !



Quelle est la prochaine étape ?

Maintenant, vous pouvez soit reprendre ce chapitre, soit suivre notre recommandation en cliquant sur l'un des boutons ci-dessous :

Redémarrer

Suivant

Protéger un appareil numérique

Dans le monde physique, vos biens, y compris votre appareil numérique, peuvent être volés. Dans le monde numérique, votre appareil est également vulnérable aux piratages et aux virus. Ce chapitre porte sur la manière de protéger votre smartphone, votre vie privée et vos informations contre les cyberattaques, telles que les virus.

Ce que vous allez apprendre dans ce chapitre

1. Comment protéger vos appareils contre les accès non autorisés ?
2. Comment protéger vos appareils contre les virus.
3. À propos des ransomware, des logiciels malveillants et des attaques DDoS.
4. Comment utiliser une connexion Wi-Fi publique en toute sécurité.

Comment protéger un appareil numérique contre les accès non autorisés ?

1

2

3

Verrouillez votre appareil mobile

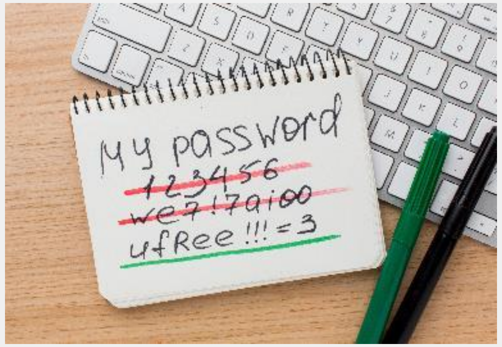
Verrouillez votre appareil à l'aide de mots de passe ou, mieux encore, en activant l'authentification biométrique. Verrouillez votre carte SIM à l'aide d'un code PIN et conservez vos codes PIN et PUK dans un endroit facile à retenir mais sûr.

Comment protéger un appareil numérique contre les accès non autorisés ?

1

2

3



Utilisez des mots de passe forts

Dans le dernier chapitre, vous avez appris à créer et à utiliser des mots de passe forts, avec des lettres majuscules et minuscules, des chiffres et des caractères spéciaux. Cela vaut la peine de s'asseoir avec un stylo et du papier pour le faire.

Comment protéger un appareil numérique contre les accès non autorisés ?

1

2

3

Surveillez vos téléchargements

Ne téléchargez des fichiers, tels que des documents, des vidéos, de la musique ou des images, qu'à partir de sites Web auxquels vous faites confiance, tels que les fabricants d'appareils, les grandes sociétés de logiciels ou les sociétés de médias. Certains fichiers téléchargés depuis des sites non fiables peuvent contenir des virus et endommager votre matériel. Les sites Web dont l'adresse commence par **https** vous protègent contre ce risque.

1

2

3

Que sont les virus ?

Les virus sont des programmes auto-réplicateurs qui se propagent d'un appareil à l'autre par le biais de mails et de téléchargements malveillants.

Comment protéger un appareil numérique contre les accès non autorisés ?

4

5

6

Maintenez l'appareil à jour avec les mises à jour logicielles

Le fabricant d'appareils mobiles envoie des notifications concernant les nouvelles mises à jour logicielles. Les mises à jour permettent de protéger un appareil contre les failles de sécurité qui pourraient permettre à quelqu'un de prendre les données de votre appareil. Téléchargez ces mises à jour logicielles sur l'appareil et mettez-le à jour.

Comment protéger un appareil numérique contre les accès non autorisés ?

4

5

6

Chiffrer les données sur le dispositif mobile

La plupart des appareils mobiles disposent d'une option permettant de chiffrer vos données. Si un appareil est volé, le cryptage rendra plus difficile pour une personne non autorisée de voir les données stockées sur l'appareil. Un utilisateur autorisé pourra utiliser l'appareil normalement.

4

5

6

Qu'est-ce que le chiffrement ?

Le chiffrement est la méthode par laquelle les informations sont converties en codes illisibles qui cachent la véritable signification des informations, sauf pour l'utilisateur qui possède la clé.

WhatsApp, l'application de réseaux sociaux de Facebook, est dotée d'un système de chiffrement de bout en bout, de sorte que les communications entre deux utilisateurs ne peuvent pas être "écoutées" par une autre personne.

Comment protéger un appareil numérique contre les accès non autorisés ?

4

5

6

Méfiez-vous des réseaux Wi-Fi publics

Le Wi-Fi dans les espaces publics comme les aéroports et les cafés peut être risqué. Parfois, ce que vous pensez être le Wi-Fi du café est en fait l'ordinateur portable d'un pirate qui peut utiliser la connexion à votre appareil à des fins inappropriées. En cas de doute, ne vous connectez pas !

Wi-Fi et criminalité

Les cybercriminels espionnent parfois les réseaux Wi-Fi publics et collectent les données qui sont transférées par Wi-Fi.

De cette façon, le criminel peut obtenir des coordonnées bancaires, des mots de passe et d'autres informations sensibles.

Avantages et inconvénients : utiliser le Wi-Fi public ou non ?

Avantages

- Gratuit
- Vos données mobiles ne sont pas utilisées
- Facile d'utilisation
- Disponible

Inconvénients

- Non sécurisé
- Le Wi-Fi d'un "hotspot" d'une organisation pourrait être usurpé
- Généralement, la vitesse est inférieure à celle de votre propre couverture mobile

Qu'est-ce qu'une cyberattaque ?

L'objectif d'un piratage informatique est d'obtenir un accès pour commettre des méfaits, voler des données ou détruire les données d'une entreprise.

Malware, Ransomware, DDoS

*"**Malware (logiciel malveillant)** désigne tout logiciel conçu intentionnellement pour causer des dommages à un ordinateur, un serveur, un client ou un réseau informatique. En revanche, un logiciel qui cause des dommages involontaires en raison d'une déficience quelconque est généralement décrit comme un bogue logiciel. Il existe une grande variété de types de logiciels malveillants : les virus informatiques, les vers, les chevaux de Troie, les rançongiciels, les logiciels espions, les logiciels publicitaires, les essuie-glaces et les logiciels d'alarme"*

(Source: https://en.wikipedia.org/wiki/Malware).

*"**Le rançongiciel** est un type de logiciel malveillant qui empêche la victime d'accéder à de nombreux fichiers sur son ordinateur. Il est généralement téléchargé via un lien dans un e-mail, sur un site web ou sur les réseaux sociaux. Une fois téléchargé, il crypte tous les fichiers de données sur l'ordinateur et un écran de blocage apparaît alors, exigeant le paiement d'une rançon pour permettre la libération des fichiers. NE cliquez **PAS** sur les liens contenus dans les textes ou les e-mails suspects !"*

(Source: https://www.bankofireland.com/security-zone/protect-your-business/ransomware/)

*"**L'atténuation des DDoS** désigne le processus consistant à protéger avec succès un serveur ou un réseau ciblé contre une attaque par déni de service distribué (DDoS). En utilisant un équipement réseau spécialement conçu ou un service de protection basé sur le cloud, une victime ciblée est en mesure d'atténuer la menace entrante.".*

(Source: https://www.cloudflare.com/en-gb/learning/ddos/ddos-mitigation/)

Faites le travail !

Tom a ajouté l'authentification à son appareil numérique. Pouvez-vous suggérer d'autres moyens de protéger ses informations ?

- ✓ Rencontrez et apprenez à connaître Tom. Vous pouvez trouver des informations sur Tom ici.
- ✓ Tom a travaillé dans une société du secteur informatique, il est donc un utilisateur averti de la technologie. Il utilise désormais l'authentification mais souhaite utiliser son smartphone de manière sécurisée afin que d'autres personnes ne puissent pas accéder à ses informations.
- ✓ A partir des informations que vous avez apprises dans les diapositives précédentes, suggérez d'autres actions que Tom peut entreprendre pour protéger ses informations.

Quiz

Click the **Quiz** button to edit this object

SMART | MODULE 4 | CHAPITRE 3 Protéger un appareil numérique

Une cyber-attaque DDoS se produit lorsqu'une personne tente de perturber le trafic normal d'un serveur ciblé.

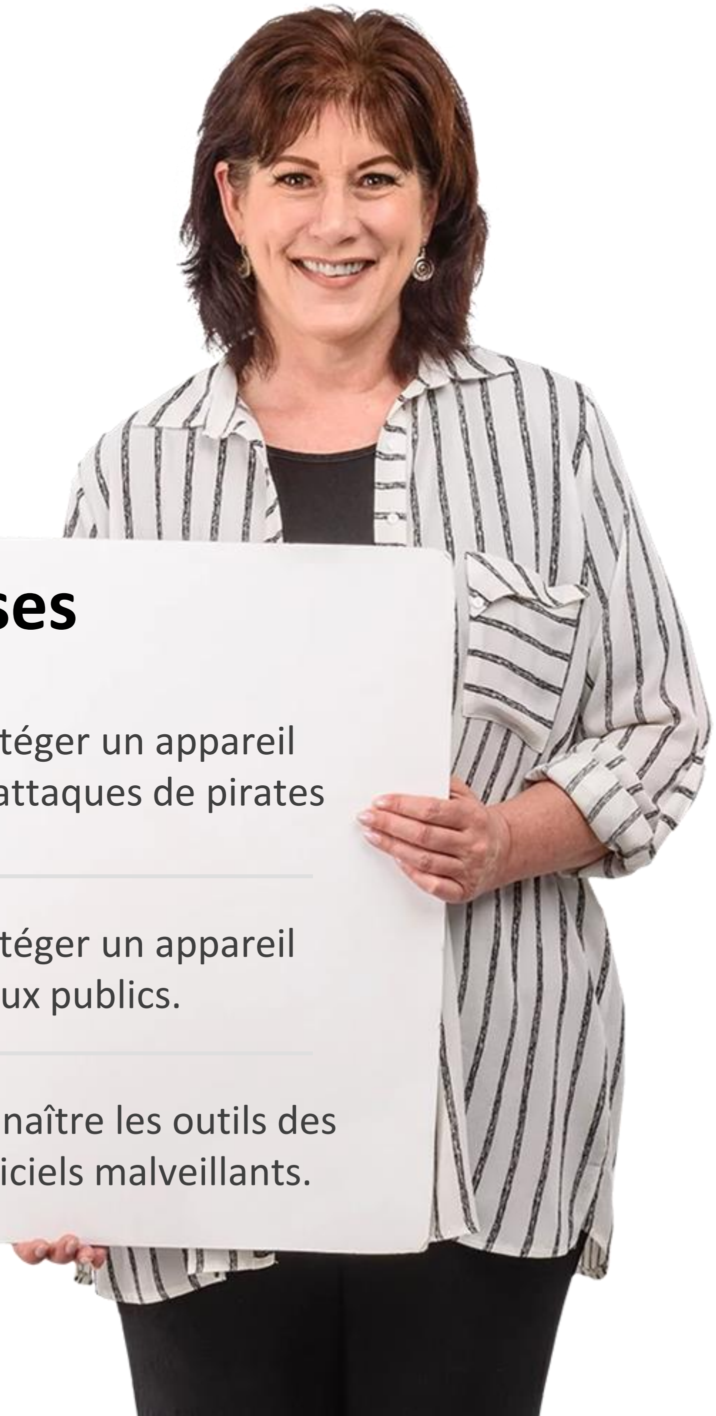
- Vrai
- Faux

Résumé du chapitre

1. Vous avez appris à protéger un appareil numérique.
2. Vous avez appris à faire la différence entre les virus et les attaques informatiques.
3. Vous avez appris à connaître les rançongiciels, les logiciels malveillants et les DDoS.
4. Vous êtes conscient des risques liés à l'utilisation du Wi-Fi public.

Chapitre terminé !

Félicitations ! Vous avez terminé ce chapitre avec succès !



Compétences acquises

1. Vous avez appris à protéger un appareil numérique contre les attaques de pirates et les virus.
2. Vous avez appris à protéger un appareil numérique dans les lieux publics.
3. Vous avez appris à connaître les outils des pirates, comme les logiciels malveillants.

Quelle est la prochaine étape ?

Maintenant, vous pouvez soit reprendre ce chapitre, soit suivre notre recommandation en cliquant sur l'un des boutons ci-dessous :

Redémarrer

Suivant

SMART | MODULE 4 | CHAPITRE 4

Cyber-harcèlement et traitement des contenus inappropriés

Que faire si vous êtes la cible de cyber-harcèlement ? Si l'on ne voit pas la personne, il est plus facile de ne pas se rendre compte du mal qui est fait par la cyberintimidation. Dans ce chapitre, nous examinerons les aspects humains de la communication numérique et ce qu'il est approprié ou non de partager en ligne.

Ce que vous allez apprendre dans ce chapitre

1 Être conscient du cyber-harcèlement.

2 Comment traiter les contenus inappropriés.

3 Ce qu'il faut partager ou non en ligne.

4 Amis en ligne : quel est le niveau de sécurité ?

Qu'est-ce que le cyber-harcèlement ?

La cyber-harcèlement se définit comme ***un acte agressif et intentionnel réalisé par un groupe ou un individu, en utilisant des formes de contact électroniques, de manière répétée et dans la durée, à l'encontre d'une victime qui ne peut pas se défendre facilement. - Smith 2018***

On dit généralement que le cyber-harcèlement implique trois éléments :

1. l'intention de nuire
2. déséquilibre du pouvoir
3. la répétition de l'acte

Types de cyber-harcèlement

La cyberintimidation peut se produire par le biais de messages textuels, d'appels téléphoniques, d'e-mails, de messageries instantanées, de plateformes de réseaux sociaux ou de groupes de conversation.

Elle peut prendre la forme d’insultes, de commentaires désobligeants, de la publication de fausses informations sur des forums ou des blogs publics, du piratage de comptes pour des menaces personnelles de nature violente ou sexuelle.

- Rao 2018

Comment faire face au cyber-harcèlement

Selon les experts, il existe plusieurs façons de faire face à du cyber-harcèlement.

Ignorez : Dans la mesure du possible, ignorez et coupez les ponts avec le harceleur.

Enregistrez : Notez l'heure, la date et le contenu de tous les actes de harcèlement, afin de pouvoir les signaler si nécessaire.

Soutien des amis : partagez votre expérience avec vos amis et vos proches, afin de ne pas vous sentir isolé.

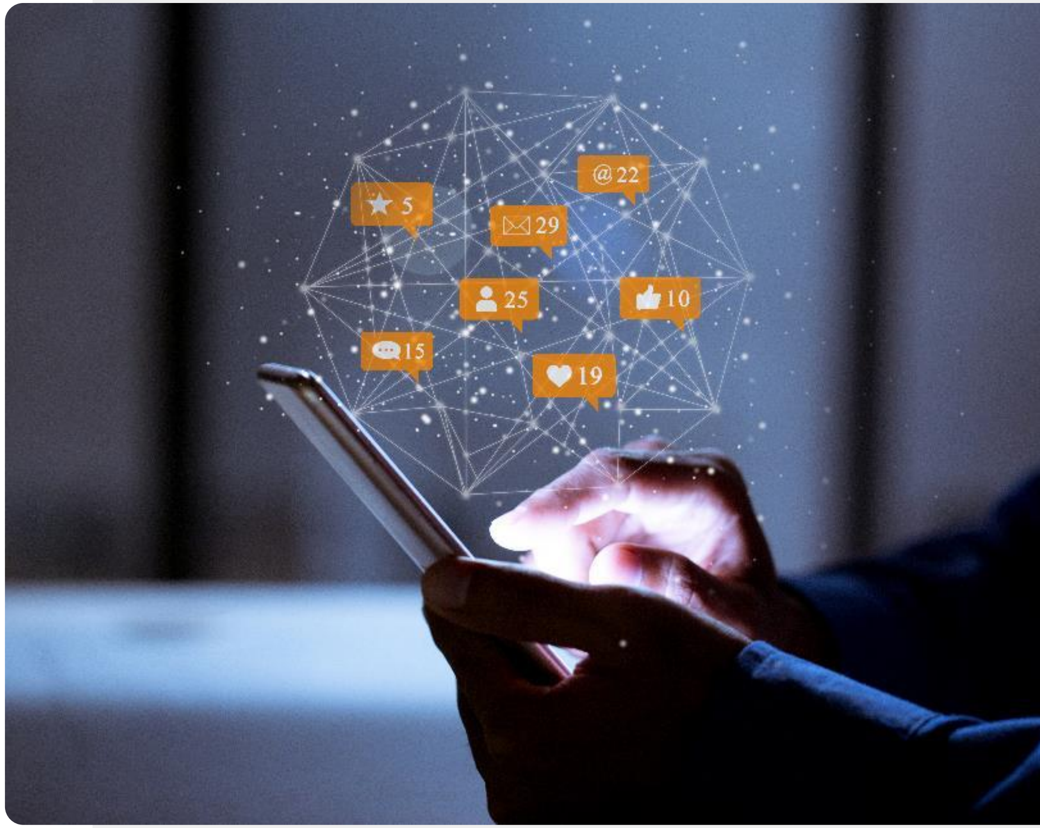
Rapport : Contactez le modérateur du site ou du forum.

Partager des informations personnelles sur les réseaux sociaux

Lorsque vous partagez des informations sur les réseaux sociaux, vous devez partir du principe qu'elles y resteront longtemps. Demandez-vous si votre message ne risque pas de causer des problèmes.

"Bien qu'il puisse sembler que les informations ne soient partagées qu'avec vos amis et votre famille, elles peuvent également être partagées avec les pirates et les escrocs qui sont sur les réseaux sociaux". "Une fois que vos données sont dans la nature, elles restent dans la nature et peuvent être utilisées par un grand nombre de personnes sans scrupules".

Joseph Turow - Penn State



Où signaler le cyber-harcèlement

Votre fournisseur de services ou votre fournisseur de réseaux sociaux peut vous aider à bloquer les messages et appels indésirables.

Si la situation est plus grave, la police peut enquêter sur les communications menaçantes.

Suppression des identités en ligne

Sur les applications de réseaux sociaux, vous pouvez souvent modifier votre profil, afin qu'il ne soit pas visible pour le grand public.

Il n'est pas toujours possible de supprimer vos messages sur les réseaux sociaux ou les forums Internet, mais vous pouvez supprimer votre identité, de sorte que ces messages deviennent anonymes.

Dans certains cas, vous pouvez envoyer une demande à un **moteur de recherche**, tel que Google, afin que vos données n'apparaissent pas dans les recherches.

Tu t'es fait avoir ?

Si quelqu'un a accès à votre compte de messagerie ou de réseaux sociaux, il peut l'utiliser pour envoyer de faux courriers à vos contacts et commettre d'autres méfaits. C'est ce qu'on appelle le **"pwning"** (prononcer "*pawning*").

Cela peut notamment se produire lorsqu'une importante fuite de données concernant un service en ligne contient votre mot de passe. Si vous utilisez le même mot de passe pour différents comptes, comme votre messagerie électronique, vos différents comptes peuvent être piratés.

https://haveibeenpwned.com/

Choisissez soigneusement vos amis en ligne

Choisir des amis en ligne : vérifiez les informations que vous avez reçues de vos "nouveaux" amis.

Ne partagez pas vos informations personnelles, tenez des conversations neutres.

Ne prêtez pas d'argent à un "nouvel" ami.

Un véritable ami sera intéressé par vos intérêts et ne vous utilisera pas pour résoudre ses problèmes.

Se faire de nouveaux amis en ligne

Avantages

- Vous pouvez vous connecter avec des personnes du monde entier.
- Vous pouvez découvrir beaucoup plus d'amis qui partagent vos intérêts en ligne que dans une communauté locale.
- Les discussions en ligne peuvent être plus faciles qu'en personne.
- Vous pouvez fermer votre compte si quelque chose ne va pas.

Inconvénients

- Si vous préférez communiquer en personne, la distance peut être un problème.
- Vous devez faire attention à ne pas divulguer d'informations personnelles à un inconnu. Leur identité pourrait être fausse.
- Il est plus facile pour les gens de harceler en ligne, car ils ne voient pas l'autre personne.

Qu'est-ce qu'un contenu inapproprié ?

Les contenus inappropriés comprennent des images "d'*attaques terroristes, de décapitations et d'attentats à la bombe ; de cruauté envers les humains et les animaux ; de sites d'automutilation ; de contenus favorables à l'anorexie et aux troubles de l'alimentation ; de contenus favorables au suicide ; d'abus sexuels et de viols ; de contenus violents et pénibles ; de sites haineux ; de pornographie en ligne*".

https://www.nspcc.org.uk/keeping-children-safe/online-safety/inappropriate-explicit-content/

Dans le vocabulaire d'Internet, une personne qui publie du contenu inapproprié dans le but de provoquer ou d'insulter d'autres lecteurs est appelée un **troll**.

Traitement des contenus inappropriés

La plupart des fournisseurs de services de navigation disposent d'options permettant de prendre en charge cette fonction. Par exemple, la fonction SafeSearch de Google se trouve à l'adresse https://www.google.com/preferences.

C'est la première chose sur la page. Ouvrez cette page et cliquez sur l'icône située à côté de "Activer SafeSearch".

Vous pouvez également choisir de verrouiller SafeSearch, et Google bloquera à la fois les textes des sites Web pour adultes et les images associées à ces sites.

https://www.dragonblogger.com/how-to-block-inappropriate-content-on-google/

Faites le travail !

Teresa est bouleversée par un incident de cyber-harcèlement. Pouvez-vous l'aider ?

- ✓ Rencontrez et apprenez à connaître Teresa. Vous pouvez trouver des informations sur Teresa ici.
- ✓ Teresa utilise la technologie pour rester en contact avec ses amis, mais elle a récemment été victime de cyber-harcèlement. Pour l'instant, il ne s'agit pas d'un cas grave, mais elle aimerait tout de même savoir comment y faire face, surtout si cela continue.
- ✓ À partir des informations que vous avez apprises dans les diapositives précédentes, donnez des conseils à Teresa sur la façon de gérer le cyber-harcèlement.
- ✓ Si le cyber-harcèlement devient plus grave, quelle personne Teresa doit-elle contacter ?

Quiz

Click the **Quiz** button to edit this object

Quels sont les éléments qui s'appliquent normalement à la cyberintimidation ? (cochez trois éléments) :

- [ ] intention de nuire
- [ ] l'acte est répété
- [ ] C'est quelqu'un que vous connaissez
- [ ] Social network hotline

Résumé du chapitre

1. Vous avez appris ce qu'est le cyber-harcèlement, comment le reconnaître et le signaler.

2. Vous avez appris à connaître les contenus inappropriés et à les bloquer.

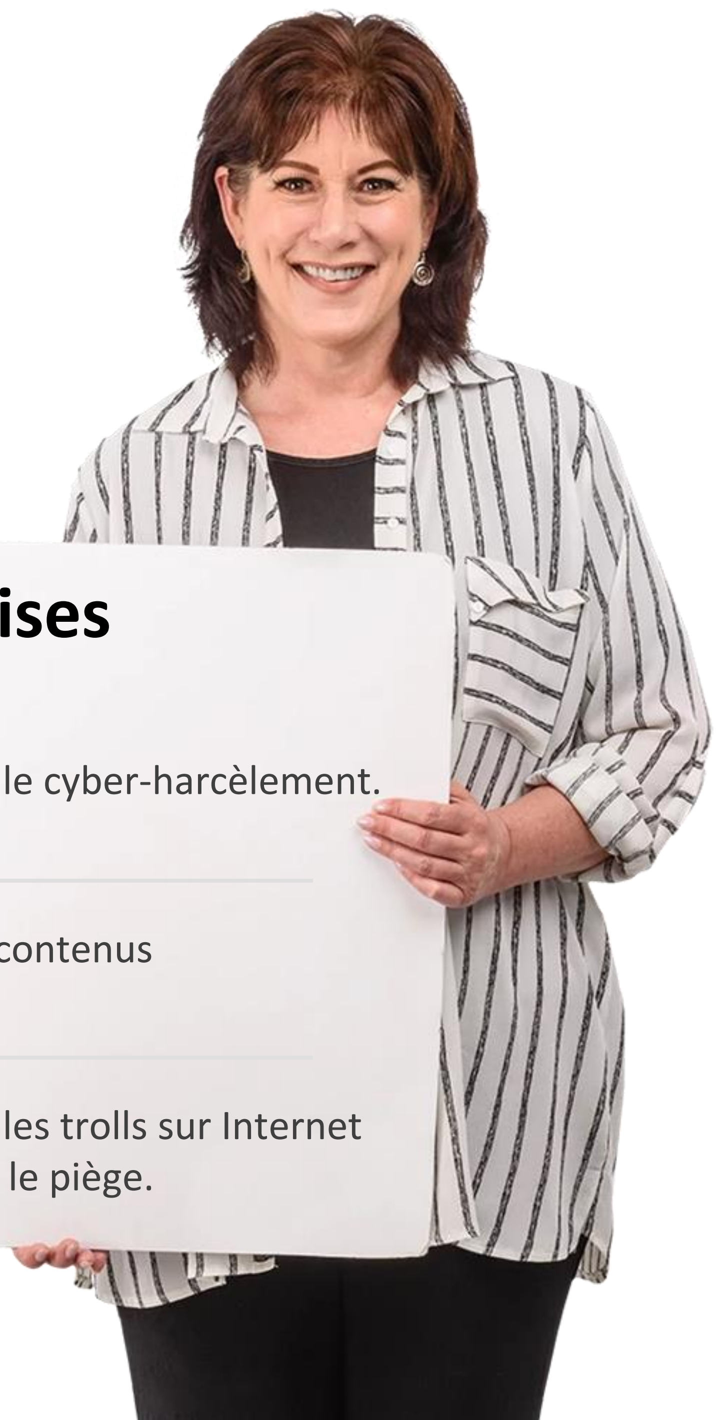
3. Vous avez appris à vous protéger lorsque vous rencontrez de nouveaux amis en ligne.

4. Vous avez appris à être prudent lorsque vous partagez des données en ligne : une fois publiées, il est difficile de les supprimer.

5. Si quelque chose ne vous plaît pas : vous pouvez le bloquer, le signaler ou fermer votre compte.

Chapitre terminé !

Félicitations ! Vous avez terminé ce chapitre avec succès !



Compétences acquises

1. Comment reconnaître le cyber-harcèlement.
2. Comment bloquer les contenus inappropriés.
3. Comment reconnaître les trolls sur Internet et ne pas tomber dans le piège.

Quelle est la prochaine étape ?

Maintenant, vous pouvez soit recommencer ce chapitre, soit suivre notre module suivant en cliquant sur l'un des boutons ci-dessous :

Recommencer

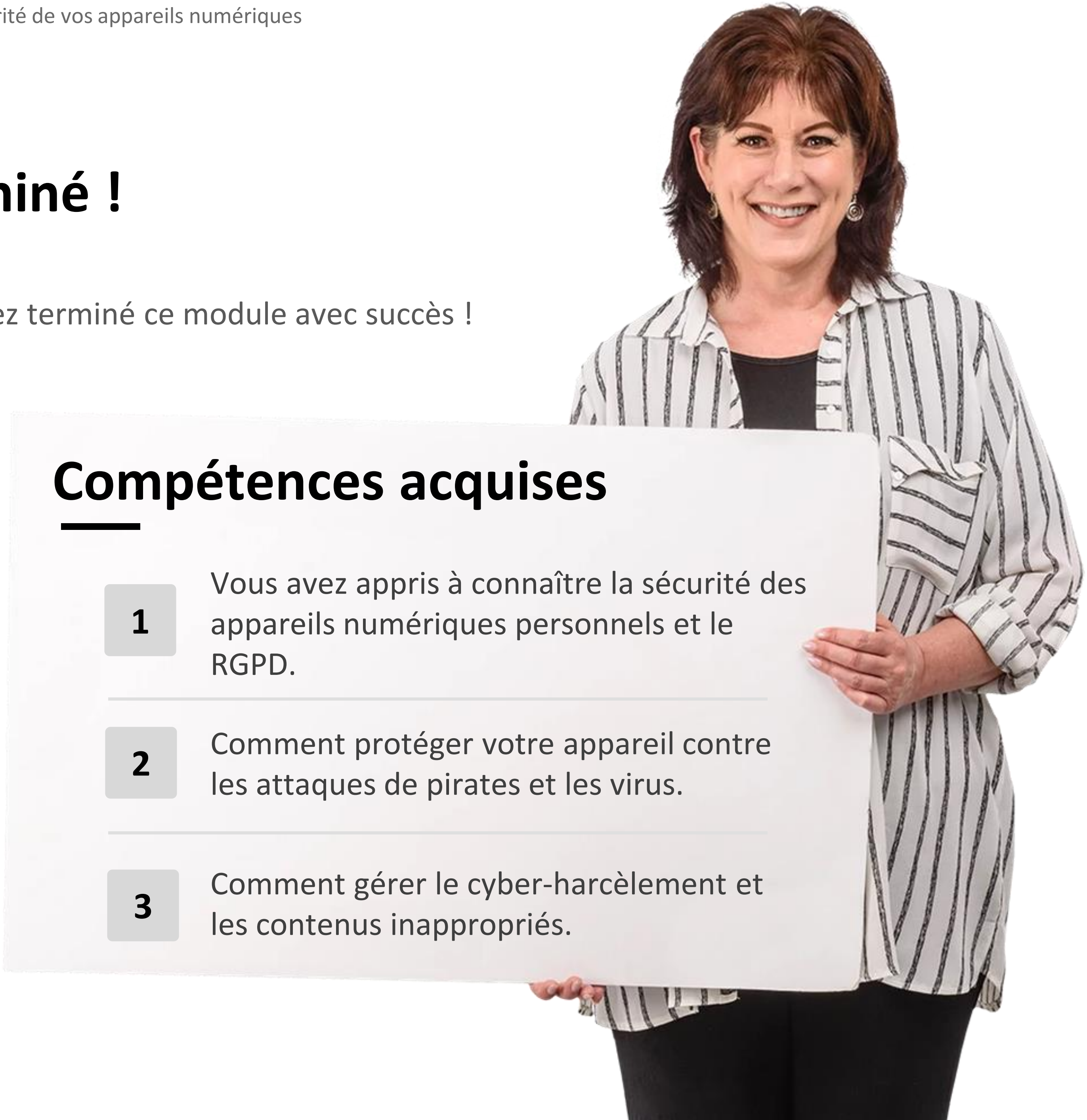
Suivant

Résumé du module

1. Vous vous êtes renseigné sur la sécurité des appareils numériques.
2. Vous avez appris le règlement général sur la protection des données, le RGPD.
3. Vous avez appris les types d'authentification.
4. Vous avez appris à créer des mots de passe forts.
5. Vous avez appris à connaître les outils des attaques informatiques : logiciels malveillants, ransomware, DDoS.
6. Vous avez appris ce qu'est le cyber-harcèlement et comment ne pas en être victime.
7. Vous avez appris à ajuster les paramètres SafeSearch de Google pour éviter les contenus inappropriés.

Module terminé !

Félicitations ! Vous avez terminé ce module avec succès !



Compétences acquises

1. Vous avez appris à connaître la sécurité des appareils numériques personnels et le RGPD.
2. Comment protéger votre appareil contre les attaques de pirates et les virus.
3. Comment gérer le cyber-harcèlement et les contenus inappropriés.

Quelle est la prochaine étape ?

Maintenant, vous pouvez soit recommencer ce module, soit suivre notre recommandation en cliquant sur l'un des boutons ci-dessous :

Recommencer

Suivant