MODULE 10

SECURISER SON PC ET SON USAGE

EPN Gens Clic | Module 10
Intermédiaire
Géraldine Masse CC0

Les programmes malveillants

Les programmes malveillants sont créés par les humains. Ils sont créés majoritairement pour se propager sur Windows. En effet, c'est le système d'exploitation le plus répandu et le moins bien protégé par défaut.

Même en installant un antivirus sur votre ordinateur, vous n'êtes pas totalement protégé. Un virus fraîchement programmé sera capable de passer à travers les mailles de votre antivirus.

Ils provoquent divers effets non désirés comme par exemple :

- Suppression de vos données
- Données cryptées
- Ralentissement des performances de l'appareil
- Dysfonctionnements
- Exploitation de vos données personnelles
- Système qui plante fréquemment
- Perte soudaine d'espace de stockage.
- Apparition de barres d'outils, d'extensions ou plug-ins dans votre navigateur
- Arrêt de fonctionnement de votre antivirus. Impossibilité de le mettre à jour
- Prise de contrôle de votre ordinateur.
- Reformatage de votre disque dur (perte de toutes vos données).

Comment se fait-on infecter ?

Les deux principaux moyens pour les malwares d'infecter vos appareils sont : Internet (surf) et les emails.

Ils peuvent vous contaminer lorsque vous :

- Consultez des sites piratés
- Téléchargez des fichiers infectés
- Installez des barres d'outils de fournisseurs inconnus
- Installez un logiciel gratuit
- Ouvrez une pièce jointe
- Cliquez sur un lien

- Ouvrez un fichier téléchargé sur Internet ou provenant d'une clef USB…

Ces malwares se cachent aussi dans des applications qui semblent sûres. Veillez à toujours installer vos applications mobiles via le Playstore (ou l'App Store).

Toutes ces attaques ont la plupart du temps besoin de **vous** pour fonctionner. C'est vous qui allez cliquer sur un lien ou ouvrir une pièce jointe infectée. Même si vous installez quelque chose qui provient d'une source sûre, si vous ne faites pas attention à la requête qui vous demande l'autorisation d'installer d'autres logiciels groupés en même temps, vous pourriez vous retrouver avec un logiciel que vous ne voulez pas.

Notez qu'il est possible que le simple fait de visiter un site Web malveillant et de consulter une page ou une bannière publicitaire infectée entraîne le téléchargement involontaire d'un ou plusieurs fichiers, malveillants ou non.

Virus

Il s'agit de programmes informatiques malveillants envoyés en pièce jointe d'un email ou via un téléchargement. Visiter un site Internet peut lancer le téléchargement d'un virus. Ils tentent d'infecter votre ordinateur.

Conséquences : spams envoyés avec votre adresse, vol de vos données personnelles, piratage de vos navigateurs Internet, modification de vos paramètres de sécurité, publicités…

Comment savoir si on est infecté par un virus ?
L'ordinateur prend plus temps pour le démarrage.
L'ordinateur ne démarre plus.

L'ordinateur redémarre seul.

Il prend plus de temps pour lancer un programme.

Certains de vos fichiers ont disparus.

Les sites que vous consultez prennent plus de temps pour se charger.

L'ordinateur plante.

Certains programmes se lancent seuls.

Comment réagir ?
Lancer un scan par votre antivirus.
Demandez de l'aide auprès d'un professionnel.

Vers

Il vit dans la mémoire de l'ordinateur et se propage en s'envoyant à d'autres ordinateurs en réseau via la connexion Internet. Les vers ne nécessitent pas d'activation (ou d'intervention humaine) pour s'exécuter ou diffuser leur code dans votre système. L'infection provient souvent d'une faille de sécurité, ils n'ont pas besoin d'action directe de l'utilisateur.

Cheval de Troie

Il s'agit d'un logiciel en apparence légitime qui contient une fonctionnalité malveillante. Il peut aussi s'agir d'un programme malveillant qui est intégré à un logiciel légitime. Lorsque vous le téléchargez.
Conséquences : suppression de fichiers, utilisation de votre ordinateur pour en pirater un autre, utilisation de la webcam pour vous observer, enregistrer les frappes du clavier (identifiants, mots de passe…).

Spyware/ adware (logiciels espions et publicitaires)

Ils recueillent vos informations personnelles. Ils sont présents sous la forme d'un téléchargement gratuit (installé avec ou sans votre accord). Les infos qu'ils récupèrent profitent au pirate. Ce type de virus va modifier le fonctionnement de votre ordinateur, il va vous inonder de publicités et vous diriger vers des sites indésirables. Il est très difficile de les supprimer complètement de votre appareil.

Ransomware

C'est un type de malware qui restreint l'accès à votre ordinateur ou à vos fichiers. Il affiche un message où on exigera de vous un paiement pour vous rendre l'accès. Parfois ce message est faussement signé de la police.

Comment se fait-on infecter ?
les emails de phishing avec une pièce jointe malveillante.
Les écrans publicitaires sur les sites Web.

Il existe 2 types de ransomware :

- Ransomware avec verrouillage de l'écran : on ne peut plus accèder à l'ordinateur.

- Ransomware avec chiffrement : il chiffre les fichiers sur le disque dur et parfois également sur le cloud, sur un disque dur externe ou autre stockage connecté.

Comment réagir ?

Ne surtout pas payer la rançon demandée. Même si vous le faites il est peu probable que vous récupériez vos fichiers ou l'accès à votre ordinateur.

Aller voir un technicien.

Assurez vous de faire des copies de vos données sur un lecteur amovible externe.

Détournement de domaine

Il s'agit d'une technique qui nous dirige vers un site malveillant et illégitime en redirigeant une adresse bien légitime. Vous saisissez l'adresse correcte, et vous arrivez sur un faux site qui est malveillant.

Écoute éléctronique par réseau Wifi

Pour voler vos informations personnelles, des pirates se connectent à votre réseau par la box Internet.

Piratage

Lorsqu'une personne accède à votre ordinateur sans l'autorisation de son propriétaire, il s'agit de piratage. Pour y parvenir, ils trouvent des failles dans les paramètres de sécurité et les exploitent. Le piratage permet d'installer des chevaux de Troie, ce qui offre une porte d'entrée aux pirates pour qu'ils accèdent à votre ordinateur et volent des infos personnelles.
→

Le bon réflexe lorsque l'on veut se protéger au maximum de toutes ces menaces :

Installer un antivirus.

L'antivirus va protéger votre ordinateur ainsi que vos données contre les virus.

Comment fonctionne un antivirus?

Il détecte la signature des virus (une partie du code de ce virus) et les détruit. Il est recommandé de mettre à jour très souvent votre base de signatures. En effet, les nouveaux virus ont parfois des signatures uniques qui ne sont pas reconnues par les bases précédentes. Chaque fois qu'un nouveau virus est détecté dans le monde, les

bons antivirus ajoutent sa signature afin de protéger votre ordinateur d'une éventuelle contamination.

Bien sûr un antivirus ne peut pas garantir une protection à 100% mais il est essentiel d'en installer un sur vos appareils. N'installez qu'un seul antivirus. Vous pouvez bien sûr opter pour une version gratuite, mais pensez à vérifier que les fonctionnalités proposées gratuitement sont suffisantes.

Pour savoir si votre ordinateur a été contaminé, scannez-le :

Vous pouvez bien sûr utiliser votre antivirus, c'est lui qui supprimera ce qu'il faut si nécessaire. Mais vous pouvez également effectuer un scan gratuit via un site :

F-Secure Online Scanner : f-secure.com/fr_BE/web/home_be/online-scanner
Panda Cloud Cleaner : https://www.pandasecurity.com/fr/homeusers/solutions/cloud-cleaner/
ESET Online Scanner : https://www.eset.com/be-fr/particuliers/online-scanner/

Peut-on installer 2 antivirus pour être encore plus protégé ?

Installer 2 antivirus provoquerait un conflit entre les ressources du système, ils ne fonctionneraient pas correctement et ralentiraient l'ordinateur, évitez absolument cela.

Que choisir comme antivirus ?

Prenez le temps de comparer les différentes offres et les fonctionnalités proposées. Choisissez un antivirus qui s'active dès l'ouverture d'un fichier ou lors d'un clic sur un lien. Il doit comprendre un pare-feu.

Un antivirus vous protège de quoi ?

Les antivirus vous protègent contre les virus classiques, les vers et les autres formes de cybercontagion. Mais il est possible d'ajouter des fonctionnalités supplémentaires.

Les faux virus

Faites très attention lorsque vous cherchez à installer un antivirus ou lorsque vous surfez sur Internet. Certains logiciels qui se présentent comme des antivirus sont en fait des virus. Si vous avez un doute sur la fiabilité d'un logiciel, consultez des avis sur Internet ou demandez conseil à quelqu'un de compétent dans le domaine.

Les arnaques

Le Phishing (hameçonnage)

Il s'agit de faux emails, sites Internet ou messages conçus pour avoir la même apparence que celle de l'entreprise réelle. L'objectif est de vous voler :

- des identifiants personnels
- vos coordonnées bancaires
- de l'argent

En général les mails de phishing vous demandent de :

- Vous mettre à jour.
- Valider votre compte.
- Confirmer votre compte.

Prenez le temps d'analyser les emails que vous recez et posez-vous les bonnes questions lorsque vous trouvez que c'est suspect :

Si vous répondez **oui** à ces questions, faites preuve de vigilance !

- Est-ce qu'il s'agit d'un email inattendu (contact à qui vous n'envoyez pas de mail régulièrement, entreprise inconnue ?,…)
- Est-ce que le mail fait passer un message à caractère urgent ? (somme à payer ou à recevoir rapidement, ami en détresse, vérification urgente de compte,…).
- S'agit-il d'une demande étrange ? Par exemple, une banque ne demandera jamais de donner votre mot de passe par email.
- Le mail comporte-t-il des erreurs de grammaire ou des fautes d'orthographe (même discrètes) ?
- Le mail est-il placé dans votre courrier indésirable ?
- Est-ce que l'on pique votre curiosité ? (Photo de vous, gain d'argent,…)

Si vous répondez **non** à ces questions, soyez vigilants !

- Le mail est-il adressé à vous personnellement ? Ou s'agit-il plutôt de Madame, Monsieur,…
- Connaissez-vous l'expéditeur ? Apportez une grande importance à l'expéditeur, est-ce l'adresse habituelle de la personne qui prétend m'écrire ? Contient-elle des erreurs ?

Dans ces mails, vous trouverez généralement un **lien**. Vous devez systématiquement vérifier où il mène. Pour cela, placez votre curseur sur le lien sans cliquer. Analysez ensuite le lien :

Quel est le nom de domaine ? Est-il fiable ou pas ?

Pour connaître le nom de domaine, vous devez regarder la partie placée avant le premier /. Ce qui se trouve après celui-ci est le chemin vers le fichier que l'on souhaite vous faire ouvrir (document, page Web,…).

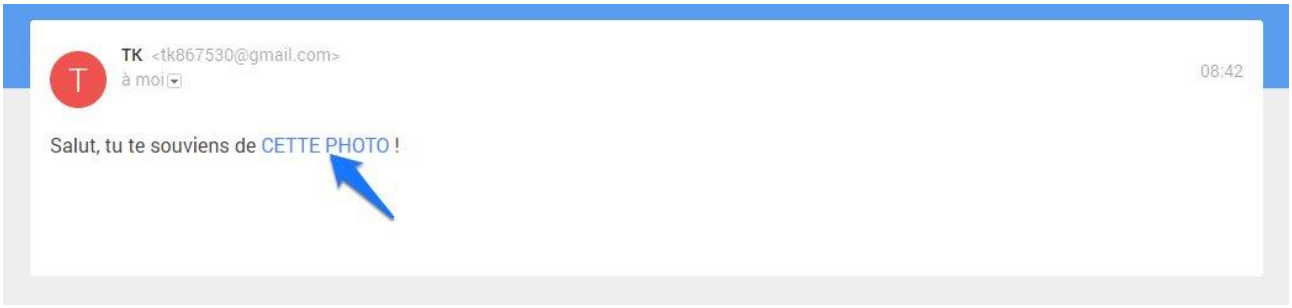
Par exemple :
https://www.epn-nivelles.org/formations.html

Le nom de domaine est epn-nivelles.
Le .be est l'extension
Formations est le chemin vers la page formations du site de l'EPN.
https est le protocole http sécurisé. C'est-à-dire que le transfert entre les serveurs est chiffré (les pirates à l'heure actuelle se servent du protocole https).

Si vous voyez https://www.epn-nivelles.formations.org/formations.html, ce lien vous amènera vers un site différent de epn-nivelles, soyez donc attentifs !

Si vous voyez https://www.epn-nivellles/formations.html, ici encore il ne s'agit pas du nom de domaine epn-nivelles. Chaque détail compte.

Exemple :

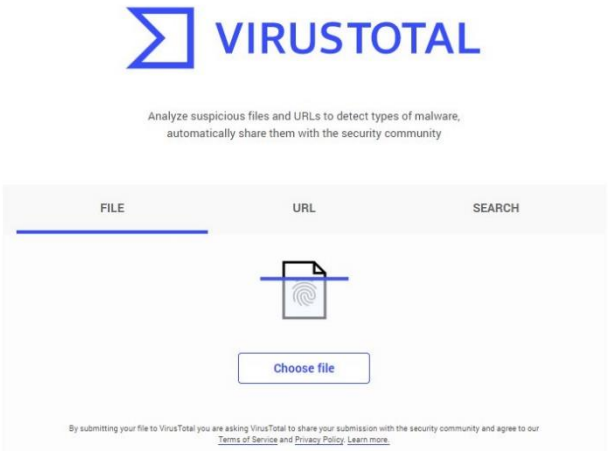


Dans ce mail, placez votre curseur sur le lien : en bas à gauche de l'écran vous pouvez l'analyser :

Le nom de domaine est donc **sytez.net**, en aucun cas **Google drive**, comme ce mail essaie de nous le faire croire.

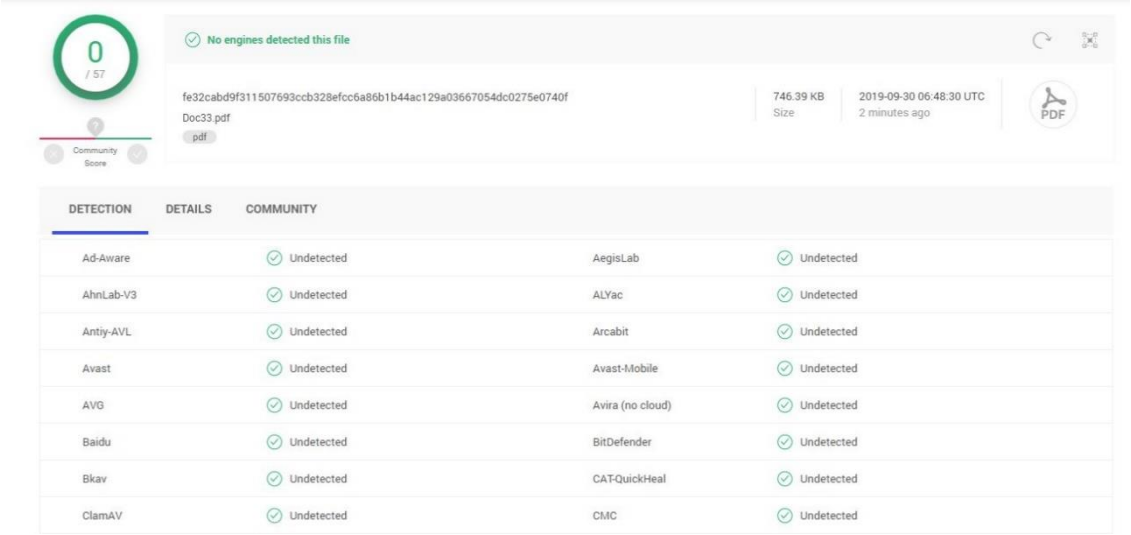
En résumé, si vous avez un doute après toutes ces analyses, n'ouvrez pas les pièces jointes et ne cliquez sur aucun lien. Vous pouvez essayer de contacter l'expéditeur autrement. Par exemple, si vous avez reçu un mail d'un contact qui vous demande de l'argent pour se tirer d'une mauvaise situation, appelez-le via son numéro de téléphone. Si il s'agit d'une entreprise, allez vérifier les propos tenus dans le mail sur leur site officiel ou encore en les contactant.

Il existe un site qui permet de scanner un fichier en ligne : https://www.virustotal.com/gui/home/upload



Cliquez sur **Choose file**, sélectionnez le fichier à analyser. Cliquez ensuite sur **Confirm upload**. L'analyse débutera.

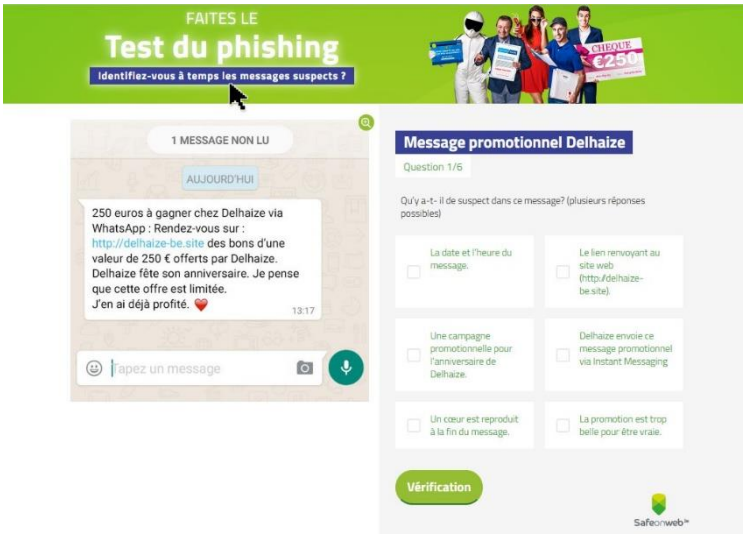
Patientez quelques secondes pour obtenir les résultats de l'analyse :



Bien sûr si vous avez un antivirus sur votre ordinateur c'est celui-ci qui se chargera de ça.

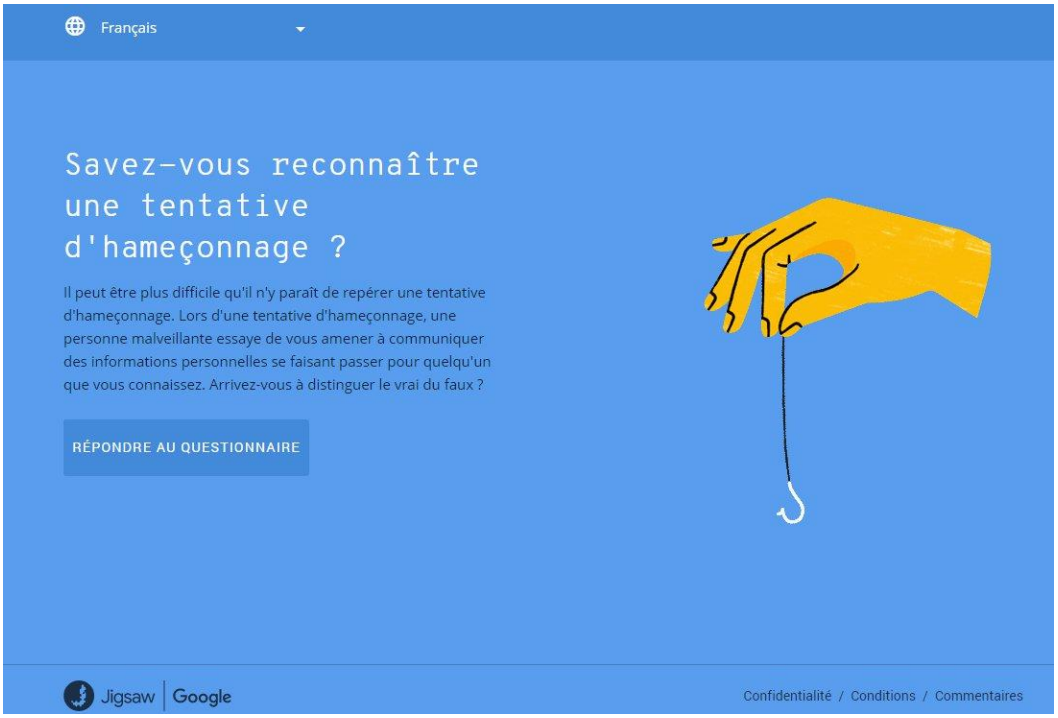
Vous pouvez vous entrainer à reconnaître les mails dangereux en faisant le test suivant :

https://safeonweb.be/fr/participation/add/55



ainsi que :

https://phishingquiz.withgoogle.com/



Le phising par pop-up

Vous pouvez rencontrer des tentatives de phishing par pop-up lorsque vous visitez des sites. Il s'agit de fenêtres qui apparaissent pendant que vous surfez. En général il s'agit de remporter un prix, de participer à un concours ou des choses dans cette veine. Fermez ces pop-up et surtout ne remplissez jamais les formulaires.

Pour éviter de les voir apparaître à l'écran, bloquez les pop-up dans les paramètres de votre navigateur

Vous pouvez également télécharger une extension sur votre navigateur telle qu' **Adblock**.

Le skimming RFID

Qu'est-ce que la technologie RFID ?

La technologie RFID (Radio Frequency Identification) est un système de communication sans fil qui permet de transférer des données à distance entre un lecteur et une étiquette ou une puce RFID. C'est cette technologie qui a révolutionné les transactions bancaires en les rendant plus rapides.

Les cartes de crédit et de débit équipées de puces RFID peuvent être vulnérables au skimming, une méthode de vol de données où les fraudeurs utilisent des lecteurs RFID portables pour intercepter les informations de carte sans devoir la toucher. Le skimming RFID est relativement rare.

Faut-il mettre une protection sur sa carte de banque ?

Ces protections (souvent une pochette en aluminimum) bloquent les signaux RFID. Elles utilisent des matériaux qui empêchent les lecteurs RFID non autorisés d'accéder aux informations de la carte. Il semblerait que ces protections ne soient pas infaillibles. De plus, la présence d'élément en aluminium présente un risque de démagnétiser la carte bancaire.

Peut-on bloquer autrement le RFID de sa carte de banque ?

Vous pouvez désactiver la fonction de paiement sans contact. Cela se fait directement depuis l'appli mobile ou en contactant votre banque.

Que faut-il faire pour protéger sa carte bancaire ?

Il est primordial de protéger votre code PIN :
Ne le notez pas sur un papier dans votre portefeuille.
N'utilisez pas un code facilement trouvable comme une date de naissance.
Soyez vigilant lorsque vous saisissez votre code. Faites-le à l'abri des regards.

→ Les 6 mythes du paiement sans contact

https://www.mastercard.com/news/europe/fr-be/points-de-vue/fr-be/2021/les-6-mythes-du-paiement-sans-contact/

L'arnaque aux sentiments

Vous discutez avec un inconnu sur Internet (sites de rencontre, réseaux sociaux…). Vous êtes séduit et vous pensez vivre une belle histoire. Cet inconnu va rencontrer un problème d'argent et vous sollicitera pour obtenir de l'aide. Cette personne souhaitera aussi certainement venir vous rejoindre mais aura besoin de vous pour acheter des billets de train ou d'avion. Vous allez payer mais un empêchement fera qu'il/elle ne viendra jamais. Cette arnaque durera aussi longtemps que vous penserez que tout cela est vraie relation.

Conseils :

Dès qu'une personne vous demande de l'argent soyez sur vos gardes. Si vous avez un doute dites-lui pour analyser sa réaction. Si la personne devient agressive par exemple, c'est certainement une arnaque.

Si vous avez déjà donné de l'argent à la personne. Signalez le profil de la personne et déposez plainte.

Reconnaître l'arnaque :

- Les arnaqueurs cherchent leurs victimes sur les réseaux sociaux (principalement Facebook) et sur les sites (ou applis) de rencontres. Ils utilisent également les mails et les forums.
- Un inconnu cherche à faire votre connaissance avec beaucoup d'enthousiasme.
- Les escrocs parlent très vite de leurs sentiments envers vous. Ils vous contactent via un autre moyen que le canal sur lequel vous avez fait votre rencontre.

- Lorsque vous essayez de planifier un rendez-vous, des excuses sont toujours évoquées. Ces problèmes pourront se résoudre avec votre aide, c'est-à-dire votre argent.
- Vérifiez l'authenticité du profil. Les arnaqueurs utilisent des faux comptes. Faites une recherche sur un moteur de recherche, si vous trouvez plusieurs fois la même photo de profil il s'agit certainement d'une arnaque.
- Si vous avez un doute, demandez des informations à votre nouveau contact. Contrôlez la véracité des réponses.
- Ne donnez pas votre argent, même si la personne insiste.

➢ Si vous avez fourni des données personnelles, il est possible que l'arnaqueur s'en serve pour une usurpation d'identité. Portez plainte à la police sans tarder. Si nécessaire, contactez également votre banque. Modifiez tous les codes et mots de passe que vous avez communiqués.

➢ Si vous avez donné de l'argent, signalez l'arnaque :

https://pointdecontact.belgique.be/meldpunt/fr/bienvenue

Vous ne récupérerez sans doute pas votre argent mais vous pouvez contacter votre banque.
Soyez doublement vigilant : en effet, les escrocs pourraient vous faire croire qu'il est possible d'obtenir un remboursement. Vous obtenez un lien sur lequel cliquer pour indiquer vos coordonnées. Ils vont en fait essayer de vous voler une seconde fois.

➢ Si vous avez transmis les coordonnées de votre carte de crédit, contactez immédiatement Card Stop (070 344 344).

Quelques conseils :

- Ne soyez pas aveuglés par de beaux profils et de belles paroles.
- Demandez suffisamment d'informations à votre nouveau contact.
- N'accordez pas trop vite votre confiance. Ne divulguez pas d'informations personnelles.
- Soyez vigilant avec les histoires « tristes ». En effet, les arnaqueurs essaieront de vous toucher sentimentalement pour parvenir à leurs fins.
- Si le profil de la personne à qui vous parlez semble trop parfait, c'est certainement que ce n'est pas réel.
- Il existe énormément de faux profils de légionnaires. Cette technique est beaucoup utilisée pour arnaquer des femmes.

Le Quishing

Vous recevez un mail avec un QR code. Celui-ci est supposé vous permettre de payer une facture, des frais de livraison, des frais de retard… Ce QR code vous enverra vers un site qui vous demandera d'encoder vos coordonnées bancaires ou qui installera un logiciel malveillant sur votre ordinateur.

Conseils :

Ne scannez pas le QR code sauf si vous êtes sûr qu'il est fiable.
Vérifiez l'adresse de l'expéditeur.
Vérifiez l'URL du QR Code en passant votre curseur par-dessus.

Vous avez scanné le QR Code ?

Envoyez une capture d'écran à suspect@safeonweb.be
Bloquez vos comptes via CardStop au 078/170.170
Déposez une plainte.

La vente en seconde main

Vous publiez une annonce sur un site de seconde main. Une personne se manifeste et semble très intéressée par votre offre. Il vous demande de passer par un service de livraison pour récupérer son achat. Elle propose de payer via les moyens de paiements de cette entreprise. Il s'agit très certainement d'un faux acheteur qui souhaite utiliser un faux service de livraison pour obtenir vos informations bancaires personnelles.

Il propose en général de passer par un service de livraison connu. Il propose de régler le paiement via cette plateforme. Il vous demande quelques informations pour réaliser ce paiement (Nom, Prénom, n° de compte bancaire). Vous recevez alors un mail qui indique que vous avez reçu un paiement sur leur plateforme et que pour récupérer cet argent il faut créer un compte. Pour cela vous devez cliquer sur un lien. Lorsque vous cliquez sur ce lien, 2 possibilités :

Soit vous tombez sur un formulaire à remplir où on vous demande de renseigner vos coordonnées (Nom, Prénom, N° de téléphone, n° de compte bancaire). Vous remplissez le formulaire et vous recevez quelques instants plus tard un appel d'une personne qui prétendra travailler pour cette société et qui voudra vérifier votre identité. Pour cela vous devrez vous identifier à l'aide du digipass, et communiquer à la personne le code de réponse.

Soit vous arrivez sur une page où l'on vous demandera de procéder à une authentification bancaire. Vous devrez utiliser le digipass de votre banque, suivre les instructions et introduire le code réponse. Il s'agit d'un faux site. Vous communiquez en fait ces données à un escroc.

Conseils :

Lors d'une vente en seconde main, n'acceptez que les paiements par virement bancaires ou en espèces sur l'acheteur se déplace pour venir chercher son achat.

Consultez le profil de l'acheteur. Il est facile de repérer les faux comptes.

Lorsque vous recevez un mail d'un transporteur, vérifiez son adresse. S'il s'agit d'une adresse Gmail ou Hotmail par exemple, il ne s'agit pas d'une vraie adresse officielle de l'entreprise.

Ne donnez jamais vos coordonnées bancaires ou d'autres informations personnelles à une personne dont vous n'avez pas su vérifier l'identité.

Si vous êtes victime de ce type de fraude :

Faites bloquer votre carte bancaire.
Déposez une plainte.

Les faux concours sur Facebook

De faux concours et cadeaux circulent sur Facebook. Ces concours vous promettent des lots incroyables. Pour avoir une chance de gagner le concours ou de recevoir le cadeau, vous devez « liker » la publication et publier un commentaire.

Les cybercriminels vont alors vous contacter via Messenger. Il peut même arriver que ça soit la victime qui contacte l'escroc via Messenger en suivant simplement la procédure indiquée dans la publication.

Vous recevez un lien qui vous mènera vers un faux site Internet où on vous volera vos données bancaires. On vous dira par exemple que pour recevoir le lot il faut payer les frais de transport.

Que faire ?

Signalez la publication à Facebook. Cliquez sur les **3 petits points/ Signaler la page.**

Bloquez votre carte bancaire.
Transférez le message à suspect@safeonweb.be.
Contactez votre banque.

→ Quelques informations provenant de Facebook :
https://www.facebook.com/help/1674717642789671

Conseils pour préserver la sécurité de votre compte

- **Ne cliquez pas sur les liens suspects** : si vous recevez un message suspect (e-mail, texto ou message sur les réseaux sociaux) dont l'expéditeur affirme être Facebook, ne cliquez sur aucune pièce jointe ni aucun lien. Vérifiez d'abord dans vos paramètres Facebook pour voir s'il provient réellement de Facebook.
- **Ne téléchargez pas de fichiers ni de logiciels provenant de personnes que vous ne connaissez pas** : soyez prudent·e lorsque vous installez des extensions de navigateur et des applications de tiers, surtout lorsqu'elles proposent des fonctionnalités qui semblent trop belles pour être vraies ou qu'elles vous demandent de vous connecter avec vos identifiants de réseaux sociaux pour pouvoir les utiliser.
- **Signalez sans y répondre les messages qui vous demandent les informations suivantes :**
  - Mot de passe
  - Numéro de sécurité sociale
  - Informations financières comme les numéros de carte de crédit
- **Renforcez votre sécurité en ligne :**
  - Activez l'authentification à deux facteurs pour ajouter une couche de sécurité supplémentaire à vos comptes sur Internet. L'authentification à deux facteurs est l'un des outils les plus efficaces pour lutter contre les tentatives de connexion suspectes à vos comptes.
  - Ne réutilisez jamais le même mot de passe sur plusieurs sites web.
  - Utilisez un logiciel antivirus de confiance. Il est primordial de garder ce logiciel à jour et d'analyser vos appareils régulièrement pour détecter les logiciels malveillants.
  - Activez les alertes de connexion afin de recevoir une notification dès qu'une tentative d'accès à votre compte est détectée. Pensez à examiner vos précédentes sessions pour vous assurer que vous reconnaissez bien les appareils ayant accès à votre compte.
  - Consultez l'outil Contrôle de la sécurité pour protéger votre compte.
  - Pour les entreprises : activez les notifications professionnelles afin de recevoir des alertes en cas de modifications dans votre compte Meta Business Manager. Pour en savoir plus, cliquez ici.

Si vous pensez que quelqu'un d'autre a accès à votre compte ou si vous ne parvenez pas à vous connecter, consultez cette page afin de suivre les étapes pour sécuriser votre compte.

Arnaques courantes

- **Arnaques liées à l'investissement** : les individus à l'origine de ce type d'arnaques peuvent faire miroiter des bénéfices irréalistes, en proposant notamment de faire fructifier une petite mise initiale (par exemple, transformer 100 € en 1 000 €) et ainsi vous demander de l'argent. Généralement, les escrocs disparaissent dès réception du paiement. Il convient de se méfier des types d'arnaques au faux investissement, notamment les arnaques au gain facile, les systèmes de Ponzi ou les propositions garantissant un enrichissement rapide.

- **Arnaques sentimentales** : les individus à l'origine de ce type d'arnaques envoient généralement des messages romantiques à des inconnu·es, en prétendant souvent être divorcé·es, veuf·ves ou malheureux·ses en ménage et à la recherche d'une relation. Ils ou elles peuvent prétendre avoir besoin d'argent ou de vos informations personnelles pour acheter un billet d'avion ou faire une demande de visa. Leur objectif étant de gagner votre confiance en premier lieu, ces escrocs peuvent discuter avec vous pendant plusieurs semaines avant de vous demander de l'argent.

- **Arnaques à l'emploi** : les individus à l'origine de ce type d'arnaques utilisent des offres d'emploi mensongères ou fictives pour tenter de vous extorquer des informations personnelles ou de l'argent. Méfiez-vous des offres d'emploi trop alléchantes ou qui requièrent un investissement initial avant même que votre candidature ne soit étudiée. Quand vous cliquez sur un lien dans une offre d'emploi, prenez garde aux sites web qui semblent ne pas avoir de rapport avec l'offre d'emploi originale ou qui vous demandent de fournir des informations sensibles (comme votre pièce d'identité officielle) mais n'utilisent pas la navigation sécurisée (https). Pour obtenir plus de conseils, consultez nos recommandations relatives à la recherche d'emploi sur Facebook.

- **Arnaques à la loterie** : les individus à l'origine de ce type d'arnaques peuvent utiliser des comptes ou des Pages usurpant l'identité quelqu'un que vous connaissez ou d'une organisation légitime (une agence gouvernementale, par exemple) afin de vous annoncer que vous faites partie des quelques gagnant·es d'une loterie dont vous pouvez recevoir le prix moyennant une avance de faible montant. Ces escrocs peuvent vous demander de fournir des informations personnelles, telles que votre adresse physique ou vos coordonnées bancaires, afin de « vérifier votre identité » avant de vous envoyer le prix.

- **Arnaques au prêt** : les individus à l'origine de ce type d'arnaques envoient des messages et partagent des publications proposant des prêts immédiats à un taux d'intérêt bas, moyennant une avance de faible montant. Après un paiement initial, ils peuvent demander plus d'argent pour fournir un prêt plus

important ou simplement mettre fin à la conversation et disparaître avec l'argent.

- **Arnaques aux dons** : les individus à l'origine de ce type d'arnaques peuvent utiliser des comptes en ligne prétendant représenter des organisations caritatives, des orphelinats ou des figures religieuses. Ils ou elles vous demandent ensuite de faire un don.

- **Arnaques à l'héritage** : les individus à l'origine de ce type d'arnaques déclarent être avocat·es ou représentant·es d'une autorité gouvernementale et vous contacter au sujet du patrimoine d'une personne décédée. Ces escrocs peuvent prétendre que l'héritage vous revient et vous demander de fournir des informations personnelles, telles que votre adresse physique ou vos coordonnées bancaires, pour que vous puissiez recevoir l'héritage en question.

- **Arnaques liées au commerce** : les individus à l'origine de ce type d'arnaques peuvent prétendre vendre des biens et des services en ligne, souvent à un prix trop beau pour être vrai, et essayer de vous convaincre que vous pouvez obtenir un meilleur prix si vous poursuivez la conversation sur un autre canal de communication, comme les e-mails ou des applications de discussion. Une fois que vous les avez payé·es, ils ou elles arrêtent de vous répondre, et vous ne recevez jamais les biens que vous avez achetés.Ces escrocs peuvent essayer de provoquer un sentiment d'urgence pour inciter les internautes à passer rapidement une commande, puis leur demander un paiement en cryptomonnaie.

    - **Remarque** : bien que l'achat d'articles éligibles via le paiement intégré sur Facebook et sur Instagram soit couvert par les politiques de protection des achats de Meta, Meta ne pratique pas de remboursement pour les transactions effectuées hors site entre particuliers. Voici quelques conseils en matière de sécurité des achats concernant le recours aux transactions entre particuliers dans le but d'acheter des articles via Facebook Marketplace, surtout si un article doit faire l'objet d'une expédition. Vous pouvez également en savoir plus sur la différence entre un achat avec paiement et une transaction locale.

- **Services d'abonnement payants** : les individus à l'origine de ce type d'arnaques peuvent proposer un accès à vie à des services d'abonnement convoités en échange d'un paiement unique et ne jamais livrer le produit.

Les bonnes pratiques

- Bien choisir ses mots de passe.

- Lorsque c'est proposé, choisissez l'authentification à 2 facteurs.

- Faire les mises à jour

- Faites des sauvegardes régulières de vos données.

- Sécurisez l'accès Wifi de votre domicile.

- Téléchargez des programmes sur les sites officiels des éditeurs.

- Être prudent avec les mails (les pièces jointes, les mails frauduleux…).

- Être vigilant lors des paiements sur Internet (vérifier https et présence du cademas).

- Séparez vos usage professionnels et personnels.

- Utilisez des adresses mail différentes pour vos pratiques (pro et autres).

- Faites attention à votre identité numérique, ne publiez pas d'informations personnelles. Décochez les cases qui autorisent à partager/ conserver vos informations lorsque vous remplissez des formulaires.

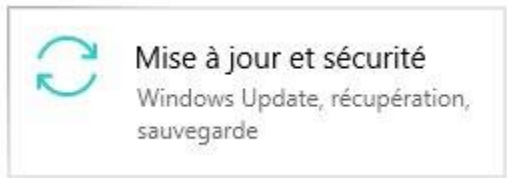
- Faites vos mises à jour régulièrement. Celles de votre système d'exploitation mais aussi celles de vos programmes et applications. Pensez à éteindre votre ordinateur tous les jours, en effet, les mises à jour sont généralement effectuées à l'extinction ou au démarrage de votre ordinateur.

- Ne rechargez pas vos appareils sur les bornes de recharges publiques. Utilisez plutôt une batterie externe « power bank ».

- Méfiez-vous des clefs USB offertes ou trouvées. Elles peuvent contenir des programmes malveillants.
N'utilisez pas la saisie automatique dans les navigateurs Internet, surtout celles des cartes bancaires.

Les mises à jour :

Paramètres/Windows Update (ou Mise à jour et sécurité).



Les mises à jour permettent de profiter des dernières nouveauté apportées (fonctionnalités, design, ergonomie), mais elles permettent aussi de corriger les erreurs et de combler les failles de sécurité.

Tous les programmes peuvent contenir des failles. Cela les rend vulnérables. Les cybercriminels exploitent ces vulnérabilités pour endommager ou contrôler vos appareils. Lorsque vous faites vos mises à jour, vous corrigez ces failles. C'est donc extrêmement important.

La plupart des programmes proposent des mises à jour automatiques. C'est très pratique car vous serez certains de toujours avoir la dernière version et d'éviter ainsi les failles de sécurité.

Mettre à jour son navigateur :

N'oubliez pas que les **navigateurs Internet** sont également des programmes. Habituellement un navigateur se met à jour lors de sa fermeture ou de sa réouverture.

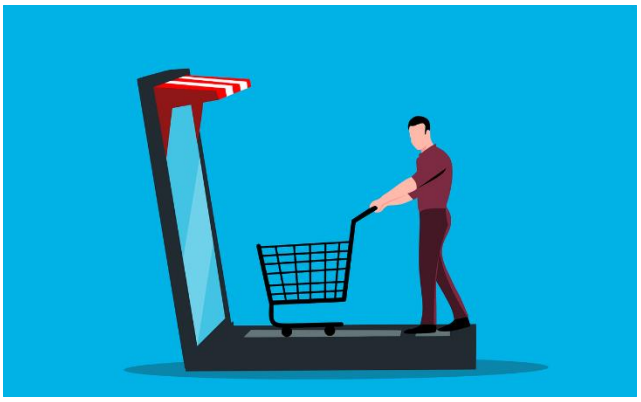
Il est probable que si votre navigateur n'est pas à jour vous en soyez averti lors de son ouverture. Par exemple, voici une fenêtre obtenue au démarrage du navigateur Vivaldi : je vais bien sûr cliquer sur le bouton **Installer la mise à jour**.

Néanmoins vous pouvez vous assurer d'utiliser la dernière version de votre navigateur en suivant cette procédure :

Google Chrome : cliquez sur les **paramètres** (3 petits point situés en haut à droite)/**Aide**.

Firefox : cliquez sur les paramètres, sur **Aide** et enfin sur **À propos de Firefox**. Une fenêtre apparaît avec les informations sur votre version : dans cet e xemple Firefox est à jour.

Acheter sur Internet



Lors d'achats sur Interent, vos données bancaires sont susceptibles d'être interceptées par des criminels directement sur votre ordinateur ou via les fichiers clients du site marchand.

Quelques conseils :

- Faites vos achat en utilisant uniquement des connexions sécurisées. N'utilisez pas de réseaux Wifi gratuits et ouverts à tous.
- Choisissez des sites fiables, connus, avec une grande renommée. Si vous avez un doute, effectuez des recherches.
- Vérifiez que le site respecte la réglementation en vigueur, certaines informations doivent être affichées :
  - Identité et activité professionnelle (et adresse physique)
  - Caractéristiques des biens et des services proposés
  - Les prix (+ les taxes et les frais de livraison)
  - Les modalités de paiement
  - Les modalités de retour
  - La durée de validité de l'offre, du prix indiqué (les conditions de vente).

- La zone de paiement doit être sécurisée avec le protocole https://. Les informations données sont cryptées et ne pourront ainsi pas être interceptées par un tiers.

- Assurez-vous de recevoir un mail de confirmation avec un récapitulatif de votre commande.

- Ne gardez pas en mémoire vos données bancaires lors du paiement, décochez systématiquement cette case.

Utilisez un mot de passe fort.

Pour vous aider, vous pouvez utiliser cet outil :

https://www.cecbelgique.be/themes/achats-sur-internet/faites-le-webshop-check

- Pour en savoir plus sur les achats en ligne, consultez le site :

  https://www.cecbelgique.be/themes/achats-sur-internet

- Si vous souhaitez savoir depuis quand existe un site Internet, utilisez cet outil :

  Pour les sites avec une extension .be :

  https://www.dnsbelgium.be/fr

  Pour les sites avec une extension .eu :

  https://eurid.eu/fr/

  Pour tous les autres :

  https://www.whois.com/

- Si vous êtes victime d'une arnaque, signalez-le sur ce site :

  https://meldpunt.belgie.be/meldpunt/fr/bienvenue

  Habitudes des escrocs :

  Utiliser un site Internet qui ressemble très fort à un site connu, pour mettre les personnes en confiance. On a le sentiment de faire ses achats sur un site fiable. Lorsque vous aurez fait votre achat, le site disparaîtra.

L'authentification

L'authentification permet de vérifier l'identité d'une personne et d'autoriser l'accès à cette personne pour qu'elle puisse :

Accéder à ses mails.

Accéder à Windows sur son ordinateur.

Accédrer à ses fichiers stockés sur un cloud.

Accèder à son compte sur un service de e-commerce.

…

Authentification unique : l'utilisateur doit procéder à une seule authentification pour accèder à quelque chose.

Il existe différents facteurs d'authentification :

Mots de passe

Carte à puce

Données biométriques (empreinte digitale, iris, reconnaissance faciale…).

…

Il existe 2 grandes familles de protocoles d'authentification :

Simple : un seul facteur d'authentification entre en jeu. Par exemple, indiquer son identifiant et son mot de passe.

Forte : il faut au minimum fournir 2 facteurs d'authentification. Par exemple, un facteur de connaissance (mot de passe) cumulée à un facteur de « possession » (un code reçu sur votre smartphone par exemple).

Créer des mots de passe forts

Il est primordial d'utiliser des mots de passe efficaces et sûrs. Les robots conçus pour décrypter les mots de passe sont de plus en plus perfectionnés, il est donc évident que vous devez absolument ne jamais utiliser un mot de passe courant ou qui comporte des informations personnelles (dans ce cas, il n'est même pas utile d'utiliser un programme pour tenter de trouver votre mot de passe).

Quelques conseils pour créer des mots de passe efficaces :

- Choisissez un mot de passe de minimum 12 caractères. Évitez d'utiliser des mots du dictionnaire. Utilisez des majuscules, des minuscules, des chiffres et des caractères spéciaux si le site le permet.

- Utilisez un mot de passe différent pour chacun de vos comptes. Si l'un de vos comptes est piraté, le cybercriminel essaiera immédiatement de s'attaquer à vos autres comptes. Si vous avez utilisé un mot de passe identique (ou même similaire) il pourra prendre possession de tous vos comptes. Vous pouvez apr contre garder la même base et modifier la fin selon le compte.

- Surtout ne pas utiliser de données personnelles pour élaborer votre mot de passe comme par exemple le nom de votre chien suivi de votre année de naissance, les prénoms de vos proches. Évitez également les expressions courantes et les caractères identiques qui se suivent.

- Ne partagez jamais vos mots de passe.

- Ne les conservez pas sur un post-it ou dans un carnet. Évitez également de les noter dans un fichier sur votre ordinateur ! Si vous voulez vraiment une trace écrite, cachez-là dans un endroit sûr.

- Pour vos comptes sensibles (professionnels, qui détiennent des données sensibles, bancaires,…) modifiez votre mot de passe régulièrement.

- Si vous souhaitez savoir si vous avez été victime d'une fuite de données, vous pouvez utiliser le site **https://monitor.firefox.com/**. En saisissant votre adresse mail vous pourrez voir les fuites de données remontant jusqu'à 2007.

- N'enregistrez pas vos mots de passe sur le navigateur Internet que vous utilisez.

- Si retenir tous ces mots de passe est trop compliqué, utilisez un gestionnaire de mots de passe :

Exemple : le programme KeePass. Cependant, pensez à faire une copie de vos mots de passe ailleurs car si votre ordinateur plante vous perdez l'ensemble de vos mots de passe. Vous pouvez également utiliser un service cloud de gestionnaire de mot de passe (Dashlane, 1Password, bitwarden…).

- Activez la double authentification dès que possible.

Les cookies

Les cookies sont associés aux sites Web. Ils sont stockés sur votre ordinateur et ils permettent au site d'enregister des informations sur l'utilisateur et de récupérer ces infos lors d'une visite ultérieure.

Il arrive que certains sites revendent et partagent ces infos stockées à des régies publicitaires. Elles sont ainsi capables de tracer les sites que vous visitez en lisant ces fichiers et de vous proposer des publicités ciblées.

Pour éviter d'être tracé il faut bloquer les cookies ou installer un bloqueur de publicité.

Notez que si vous refusez l'utilisation des cookies, vous ne pourrez plus utiliser pleinement certaines fonctionnalités des sites que vous visitez.

Une solution est aussi d'utiliser la navigation privée, car elle limite les traces de navigation, y compris les cookies.

Source de ce qui suit : https://www.blogdumoderateur.com/fin-cookies-tiers-impact-collecte-de-donnees/

les cookies se divisent en deux typologies principales, le cookie first party et le cookie third party :

Cookie first party : ce type de cookie est dédié aux services et aux analytics, avec quatre usages principaux. Il assure le service d'un site, son bon fonctionnement aux yeux de l'utilisateur, grâce au « cookie strictement nécessaire » ; il permet de stocker les préférences de navigation, comme vos identifiants de connexion par exemple,

grâce au cookie de fonctionnalité ; il donne des informations de mesures et d'analytics ; il permet la personnalisation du site visité en fonction des habitudes de l'utilisateur.

Cookie third party : aussi appelé cookie tiers, il a deux usages principaux liés à la publicité. Ainsi, il permet de cibler et recibler les annonces publicitaires pour l'internaute, tout comme la mesure de la performance média.

La décision de Google de mettre fin aux cookies tiers en 2024 va donc toucher de nombreux acteurs d'Internet. Cependant, les deux experts se veulent rassurants. Dans un premier temps, Benoit Le Bras a tenu à rappeler que « Google est le dernier à supprimer les cookies tiers ». En effet, les navigateurs Safari et Firefox l'ont fait dès 2018. « Cette ère du cookieless existe déjà et concerne 40 % du trafic Internet »

Télécharger des fichiers sur Internet

Losque vous souhaitez télécharger un logiciel, faites le uniquement sur le site de l'éditeur.

N'ouvrez jamais une pièce jointe provenant d'un mail si vous en connaissez pas l'expéditeur, ou si vous nêtes pas sûr de ce dont il s'agit.

Les formats de fichier les plus utilisés pour les programmes malveillants :

.PDF .DOC .XLS

Pourquoi ?

Car ce sont les formats les plus connus, ils n'ont pas l'air d'être malveillants.

.EXE est également beaucoup utilisé par les pirates.

Évitez également de télécharger des logiciels craqués. En plsu d'être illégal, les pirates les utilisent parfois pour installer un code malveillant.

Réseaux sociaux

Quelles informations peuvent être collectées sur les réseaux sociaux ?

Informations de profil.
Les traces de nos activités (ce qu'on like, nos commentaires, nos partages…).
Notre géolocalisation.

Conseils :

Activer la double authentification.

Lire et personnaliser les paramètres de confidentialité.

Ne pas partager d'informations personnelles.

Ne jamais publier quelque chose qu'on pourrait regretter plus tard.

Protéger son image et sa réputation.

Table des matières