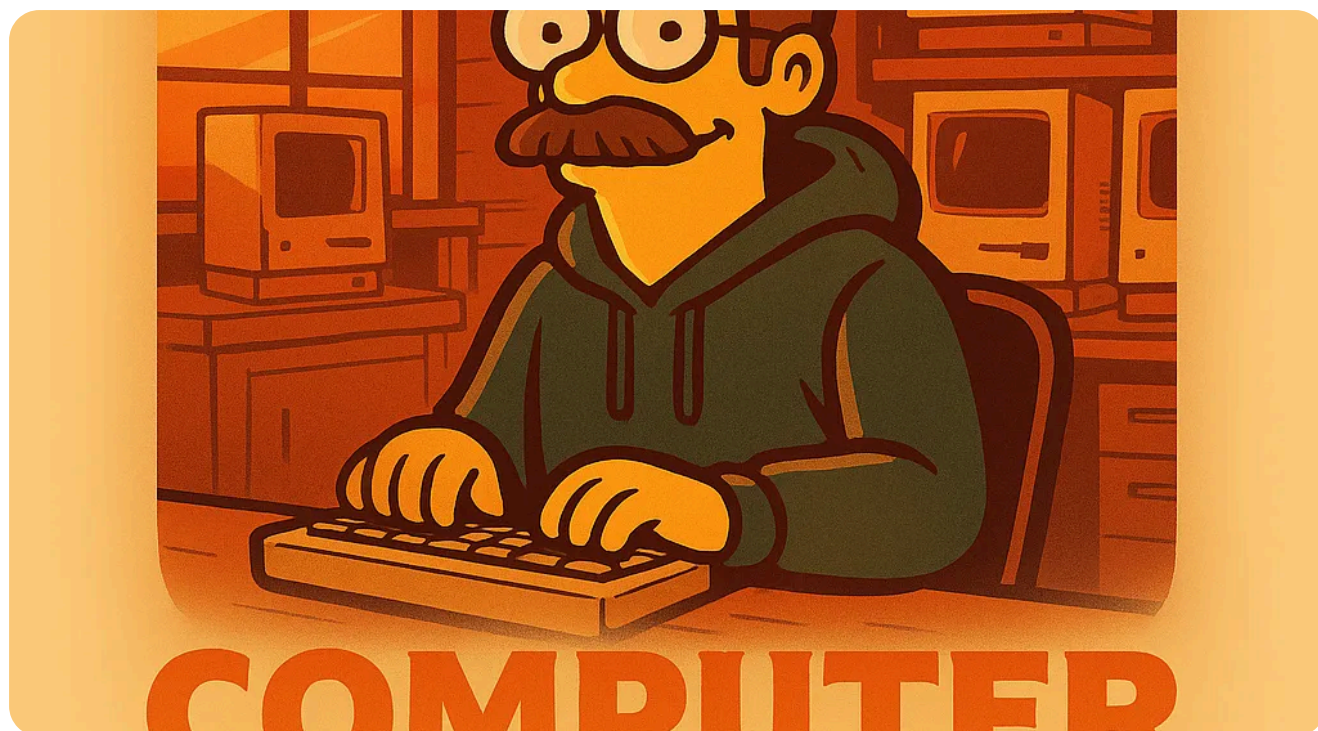




Sécurité

La sécurité

Couchard Roman

20 chapitres

SUPPORTS DE COURS

<https://cours.tsix.be/cours/la-securite>

Version 1 · 12/09/2026

PRÉSENTATION

Présentation du cours

Dans ce cours nous aborderons la sécurité informatique, et la gestion des mots de passe ainsi que la génération des mots de passe sûre.

Sommaire

- **Présentation du cours**
- 1 La sécurité informatique**
 - 1.1** Quels sont les points sensibles?
 - 1.2** Mes données sont-elles en sécurité ?
 - 1.3** Vocabulaire de sécurité informatique
- 2 Gérer vos mots de passe**
 - 2.1** Qu'est-ce qu'un mot de passe fort?
 - 2.2** Qu'est-ce qu'un générateur de mot de passe?
 - 2.3** Comment utiliser un gestionnaire de mots de passe
 - 2.4** Mise en pratique
- 3 La sécurité sur les réseaux**
 - 3.1** Les principaux risques?
 - 3.2** Mécanismes d'attaque courants
 - 3.3** Stratégies de protection efficaces
 - 3.4** Outils de protection
 - 3.5** Antivirus
- 4 Le VPN**
 - 4.1** Wifi repeater ou mesh?
- 5 Sur mobile**
- 6 QUIZZ**
 - 6.1** Réponse

CHAPITRE 1

La sécurité informatique

La sécurité informatique est essentielle pour protéger nos informations personnelles et professionnelles, un peu comme on verrouille notre maison. Elle utilise des outils simples pour empêcher les accès non autorisés à nos ordinateurs et données. Les principales menaces incluent les virus et les tentatives de vol d'informations. Pour se défendre, il est important d'avoir des mesures de base comme des mots de passe solides et de faire régulièrement des copies de sauvegarde de nos données. En résumé, c'est un ensemble de pratiques faciles à adopter pour garder nos informations en sécurité.



1.1 Quelques points sensibles de la sécurité informatique

Les portes d'entrée : Internet et vos appareils

Internet est la porte principale par laquelle les informations entrent et sortent de vos appareils. Si cette porte n'est pas bien sécurisée, des intrus peuvent s'y faufiler.

Conseils :

- **Installez un bon antivirus** : C'est comme un chien de garde pour votre ordinateur. Il surveille en permanence pour détecter les intrus et les bloquer. Des exemples populaires sont Avast, Kaspersky ou Norton.
- **Sécurisez votre Wi-Fi** : Assurez vous que votre réseau Wi-Fi est protégé par un mot de passe difficile à deviner. Évitez les noms communs ou les dates de naissance et préférez une combinaison aléatoire de lettres, chiffres et symboles. La plupart du temps le modem a un mots de passe propre que vous ne devez pas modifier.

Les Mots de passe

Les **mots de passe** sont les clés qui ouvrent l'accès à vos comptes en ligne. Si quelqu'un les obtient, il peut entrer et voler vos informations.

Conseils :

- **Utilisez des mots de passe complexes** : Pensez à une phrase que vous aimez et utilisez la première lettre de chaque mot, en ajoutant des chiffres et des symboles. Par exemple, "J'adore marcher sous la pluie!" pourrait devenir "J@mslp23!".
- **Changez vos mots de passe souvent** : C'est comme changer les serrures de votre maison régulièrement.
- Par-dessus tout, ne mettez pas le même mot de passe pour tous vos comptes. Au mieux, créez-en une variante.

Les fenêtres : Logiciels et applications

Les **logiciels et applications** sont comme les fenêtres de votre maison. Si elles ne sont pas bien fermées, quelqu'un peut passer par là pour entrer.

Conseils :

- **Mettez à jour vos logiciels** : Les créateurs de logiciels envoient régulièrement des "patches" ou des corrections pour réparer les brèches de sécurité. Sur un smartphone, vous pouvez généralement trouver ces mises à jour dans l'App Store pour iOS ou le Google Play Store pour Android. Sur un ordinateur, les mises à jour peuvent souvent être réglées pour s'installer automatiquement. Sinon passer par windows update directement depuis les paramètres du PC.

Les conversations : Communications en ligne

Quand vous **communiquez en ligne**, c'est comme si vous discutiez d'informations privées dans un lieu public. Si ces conversations ne sont pas sécurisées, quelqu'un pourrait écouter.

Conseils :

- **Faites attention aux emails suspects** : Ne cliquez pas sur des liens ou des pièces jointes dans des emails provenant de sources inconnues. Cela pourrait être une **cyberattaque** appelée phishing, où quelqu'un essaie de se faire passer pour une entreprise légitime pour voler vos informations.
- **Utilisez des services de messagerie sécurisés** : Des applications comme WhatsApp ou Signal chiffrent vos messages, ce qui signifie qu'ils les transforment en un code que seuls vous et votre destinataire pouvez comprendre.

Les invités : Qui a accès à vos informations

Faites attention à **qui vous laissez accéder à vos informations**. Sur les réseaux sociaux, vous ne voudriez pas que des inconnus voient vos photos ou connaissent vos plans de vacances.

Conseils :

- **Réglez vos paramètres de confidentialité** : Sur Facebook, par exemple, vous pouvez choisir qui peut voir vos publications, vos photos et vos informations de profil.
- **Éduquez vos proches** : Parlez de l'importance de la sécurité informatique avec votre famille et vos amis pour qu'ils ne deviennent pas involontairement une porte d'entrée pour les attaquants.

La maintenance : Mises à jour et sauvegardes

La **maintenance** est essentielle pour garder votre "maison" en sécurité. Cela inclut de s'assurer que tout est à jour et de faire des copies de vos informations importantes.

Conseils :

- **Sauvegardez vos données** : Cela signifie faire des copies de vos informations et les stocker en lieu sûr, comme sur un disque dur externe ou un service de cloud comme Google Drive ou iCloud, izzimi
- **Installez les mises à jour** : Lorsque votre téléphone ou votre ordinateur vous informe qu'une mise à jour est disponible, ne la repoussez pas. Prenez le temps de l'installer pour que vos "fenêtres et portes" restent bien sécurisées.

1.2 Mes données sont-elles en sécurité ?

Mises à jour de sécurité

- **Système d'exploitation** : Assurez-vous que votre système d'exploitation est toujours à jour.

- **Applications** : Les applications doivent également être mises à jour régulièrement pour corriger les vulnérabilités connues.

Logiciels de sécurité

- **Antivirus** : Un logiciel antivirus fiable peut détecter et neutraliser de nombreux types de malwares.
- **Firewall** : Un pare-feu aide à bloquer les accès non autorisés à votre ordinateur.
- Activer le pare-feu sur un ordinateur dépend du système d'exploitation que vous utilisez. Voici comment faire pour les systèmes les plus courants :
- Sur Windows 10 / 11 :

1. Ouvrir les paramètres du pare-feu :

Cliquez sur le menu Démarrer → tapez "Pare-feu" → cliquez sur "Pare-feu Windows Defender" (ou "Pare-feu Microsoft Defender").

2. Vérifier l'état :

Vous verrez trois types de réseaux : privé, public, et domaine.

Cliquez sur chacun d'eux pour vérifier ou activer le pare-feu.

3. Activer :

Dans chaque type de réseau, cochez "Activer le pare-feu Microsoft Defender".

4. Valider et fermer.

Pratiques de navigation sécurisée

- **Liens et pièces jointes suspects** : Évitez de cliquer sur des liens ou d'ouvrir des pièces jointes provenant de sources inconnues ou non fiables.
- **Sites sécurisés** : Privilégiez les sites web utilisant le protocole HTTPS pour des connexions sécurisées.

Comment ça marche le https?

HyperText Transfer Protocol Secure. C'est la version sécurisée du protocole HTTP, utilisé pour transférer des données entre votre navigateur et un site web.

À quoi sert HTTPS ?

Il sert à :

1. Crypter les échanges entre l'utilisateur et le site (vos mots de passe, données bancaires, etc.).

2. Vérifier l'identité du site web (certificat SSL/TLS)

3. Empêcher l'interception ou la modification des données par des pirates (attaque de type "man-in-the-middle").

HTTPS utilise des certificats numériques (SSL/TLS) pour établir une connexion chiffrée.

Avant l'échange de données, le navigateur vérifie l'authenticité du site via ce certificat.

Si tout est conforme, la connexion est sécurisée et un petit cadenas apparaît dans la barre d'adresse.

Pourquoi c'est important ?

Sans HTTPS, vos données peuvent être interceptées, surtout sur les réseaux Wi-Fi publics.

Google favorise les sites HTTPS dans les résultats de recherche.

Les navigateurs affichent maintenant des avertissements si un site n'utilise pas HTTPS.

Authentification forte

- **Mots de passe robustes** : Utilisez des mots de passe forts et uniques pour chaque compte.
- **Authentification à deux facteurs** : Activez l'authentification à deux facteurs lorsque c'est possible pour ajouter une couche de sécurité supplémentaire.

L'authentification à deux facteurs (2FA) est une méthode de sécurité qui demande deux preuves d'identité pour accéder à un compte.

Exemple :

1. Mot de passe (1er facteur)

2. Code reçu par SMS ou via une appli (2e facteur)

L'objectif : rendre l'accès plus sûr, même si le mot de passe est volé.

Sauvegarde des données

- **Stratégie de sauvegarde** : Mettez en place une stratégie de sauvegarde régulière de vos données sur des supports externes ou dans le cloud.
- **Sauvegardes chiffrées** : Chiffrez vos sauvegardes pour protéger vos données en cas de vol du support de sauvegarde.

Sécurité physique

- **Accès physique** : Limitez l'accès physique à votre ordinateur pour éviter les vols ou l'utilisation non autorisée.
- **Verrouillage de l'écran** : Verrouillez votre écran lorsque vous vous absentez de votre ordinateur.

Prudence avec les périphériques externes

- **Clés USB/disques durs externes** : Soyez prudent lorsque vous connectez des périphériques externes, car ils peuvent être infectés par des malwares.

Surveillance du réseau

- **Réseau Wi-Fi sécurisé** : Assurez-vous que votre réseau Wi-Fi est sécurisé avec un mot de passe fort
- **VPN** : Utilisez un VPN lorsque vous vous connectez à des réseaux publics pour sécuriser votre trafic internet.
- Un VPN (Virtual Private Network), ou réseau privé virtuel, est un outil qui protège ta connexion Internet en chiffrant tes données et en masquant ton adresse IP

Sur smartphone (Android / iPhone) :

Il cache ta localisation réelle.

Il protège tes données sur les Wi-Fi publics.

Tu peux accéder à des contenus bloqués dans ta région (comme certains sites ou vidéos).

📱 Exemples d'apps VPN : NordVPN, ProtonVPN, Surfshark.

Sur Windows :

Même principe : il chiffre ta connexion et te rend anonyme en ligne.

Tu installes un logiciel VPN ou tu configures une connexion manuelle.

Très utile pour télétravail, sécurité, ou confidentialité.

1.3 Vocabulaire de la sécurité informatique :

Malware (programme malveillant)



Qu'est-ce qu'un logiciel malveillant ? | Akamai

Un **malware** est un **terme générique** qui désigne **tout logiciel malveillant conçu pour nuire à un système informatique ou à un utilisateur**.

Scénario précis : "crack" de logiciel

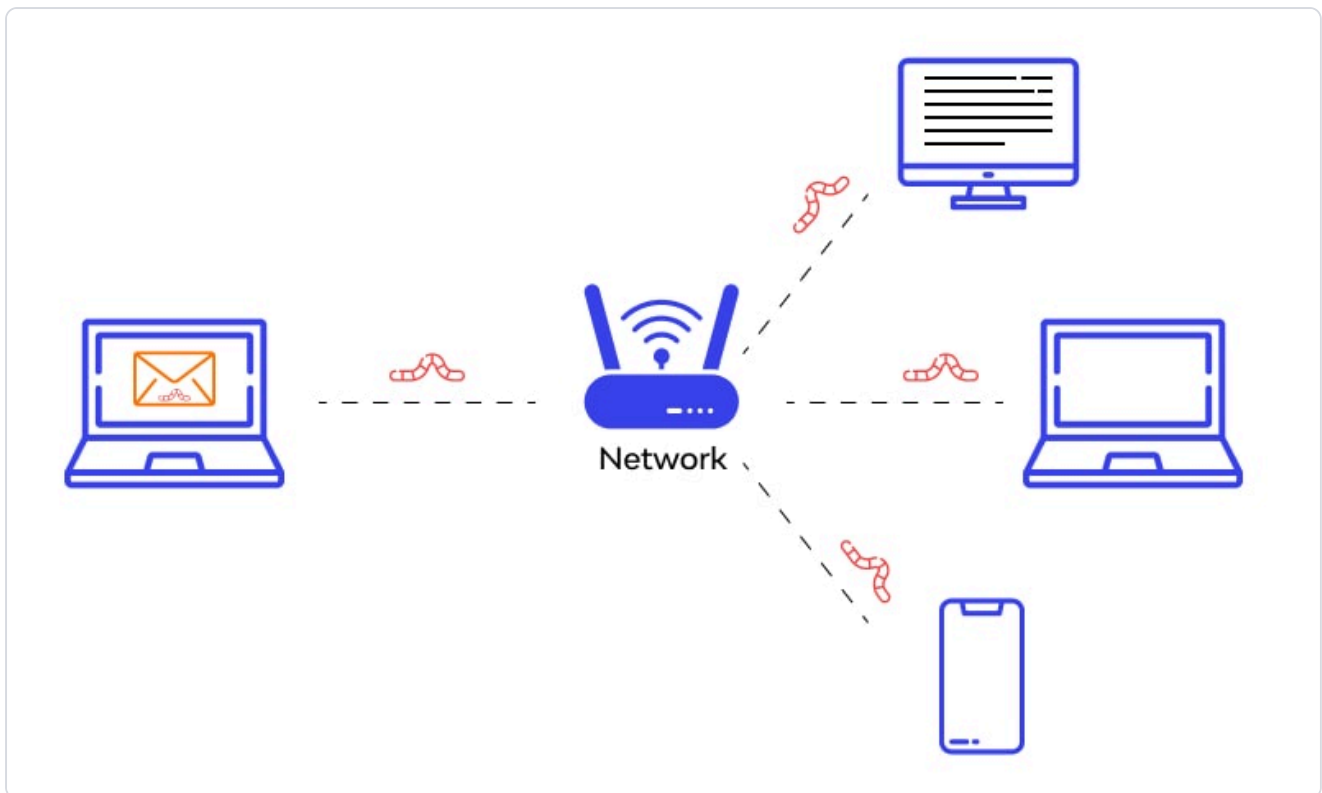
1. La victime cherche "Photoshop crack gratuit" et télécharge un fichier `Photoshop_2024_Crack.exe`.
2. Au double-clic, une fenêtre d'installation "normale" apparaît (pour rassurer).
3. En arrière-plan, le programme :
 - crée un dossier caché (ex. dans `AppData`),
 - ajoute une clé de démarrage automatique (pour se relancer au prochain allumage),
 - contacte un serveur distant (internet) pour télécharger un "module" supplémentaire.
4. Quelques heures/jours après :
 - les comptes (Google/Instagram) reçoivent des "tentatives de connexion",
 - le navigateur affiche des pubs,
 - l'ordinateur rame (processus inconnus).

➡ **C'est un malware** : un logiciel installé à l'insu de l'utilisateur pour nuire/voler/profiter.

Ver (Worm)

Un ver est un type de malware qui cherche à se répliquer lui-même pour contaminer d'autres systèmes informatiques.

Avec suffisamment de duplications, il peut entraver le fonctionnement d'un réseau d'entreprise.



Exemple concret :

Dans une entreprise, un employé reçoit un e-mail avec une pièce jointe appelée **"facture.docx"**.

Quand il ouvre le document :

1. Un ver informatique s'installe.
2. Le ver analyse automatiquement le réseau interne de l'entreprise.
3. Il cherche d'autres ordinateurs vulnérables.
4. Il se copie lui-même sur ces machines.

En quelques minutes :

- 50 ordinateurs sont infectés,
- le réseau devient extrêmement lent,
- certains serveurs ne répondent plus.

Le ver se propage **sans intervention humaine**, uniquement grâce au réseau.

Un exemple réel est **WannaCry**, qui a paralysé des hôpitaux en 2017.

Virus

Un virus est un malware qui se propage d'un ordinateur à l'autre, souvent en se greffant à un logiciel légitime.

Ce programme indésirable peut consommer les ressources de l'ordinateur, entraînant des lenteurs, des blocages ou des pertes de données.

Le terme "virus" a donné naissance au concept d'antivirus, bien que ces derniers soient en réalité des anti-malwares.

Exemple concret :

Un utilisateur télécharge un petit jeu sur Internet.

Le programme fonctionne normalement, mais il contient un virus caché.

Quand il est exécuté :

1. Le virus s'attache aux fichiers du système.
2. Il infecte aussi les fichiers que l'utilisateur envoie par e-mail.
3. Les personnes qui ouvrent ces fichiers infectés contaminent leur propre ordinateur.

Au fil du temps :

- l'ordinateur devient lent,
- certains fichiers disparaissent,
- le système plante.

Contrairement au ver, le virus a souvent besoin d'un **fichier hôte** pour se propager.

Cheval de Troie

Un cheval de Troie est un malware déguisé en programme ou document inoffensif (tel qu'un fichier PDF ou une image) pour s'implanter durablement sur un ordinateur.



Il a pour but, le plus souvent, de créer une "backdoor" ou porte dérobée, permettant à un attaquant de revenir espionner l'utilisateur ou de manipuler les données. Les chevaux de Troie sont également utilisés pour former des BotNets.

Exemple concret :

Un joueur télécharge un programme nommé "**Aimbot Fortnite.exe**" censé donner un avantage dans un jeu vidéo.

Quand il l'installe :

1. Le programme semble fonctionner.
2. Mais il installe en secret un **cheval de Troie**.
3. Ce Trojan ouvre une **backdoor** (porte dérobée).

Le pirate peut maintenant :

- accéder à l'ordinateur à distance,

- regarder l'écran,
- télécharger des fichiers,
- installer d'autres malwares.

L'utilisateur ne se rend compte de rien pendant des semaines.

Synonyme en anglais : Trojan.

BotNet



Un botnet est un réseau d'ordinateurs infectés par des chevaux de Troie, à l'insu de leurs propriétaires.

La gestion d'un tel réseau permet à un cybercriminel de réaliser des actions illégales comme la diffusion de malwares, l'envoi de spams ou le blocage de sites web.

Il existe même un marché noir où la puissance de calcul des botnets est vendue et achetée.

Exemple concret :

Un pirate infecte **20 000 ordinateurs** avec un cheval de Troie.

Chaque ordinateur infecté devient un **"bot"** (robot).

Ces machines attendent les ordres d'un serveur central appelé **Command & Control**.

Le pirate peut alors :

- envoyer des millions d'e-mails spam,
- lancer une attaque **DDoS** contre un site web,
- miner de la cryptomonnaie.

Les propriétaires des ordinateurs ne savent même pas que leur machine participe à ces attaques.

Cybercriminel

Un cybercriminel, ou pirate informatique, utilise les technologies numériques à des fins malhonnêtes, souvent pour s'enrichir aux dépens d'autrui.

Il se sert notamment de malwares pour mener à bien ses activités illicites.

Cookie

Scénario : session de connexion

Lorsque vous vous connectez à un site web (par exemple une plateforme scolaire), le serveur envoie à votre navigateur un **cookie de session**, c'est-à-dire un petit fichier contenant une valeur d'identification.

À chaque nouvelle page consultée, votre navigateur renvoie automatiquement ce cookie au site. Cela permet au serveur de **reconnaître l'utilisateur et de maintenir la session ouverte**, sans devoir saisir à nouveau son mot de passe.

Pourquoi c'est sensible

Les cookies peuvent contenir des informations importantes liées à la session d'un utilisateur. S'ils sont **volés par un attaquant**, celui-ci peut parfois les utiliser pour **se faire passer pour la victime** sur le site concerné. Cette technique est appelée **détournement de session (session hijacking)**.

Ainsi, même si un cookie n'est pas dangereux en soi, **il devient critique lorsqu'il permet d'identifier une session active**, ce qui explique son importance dans le domaine de la sécurité informatique.

Enregistreur de frappe (keylogger)

Un **keylogger** est un programme (ou parfois un appareil) qui **enregistre tout ce que tu tapes sur le clavier** : mots de passe, messages, identifiants, etc.

Il peut arriver de plusieurs façons :

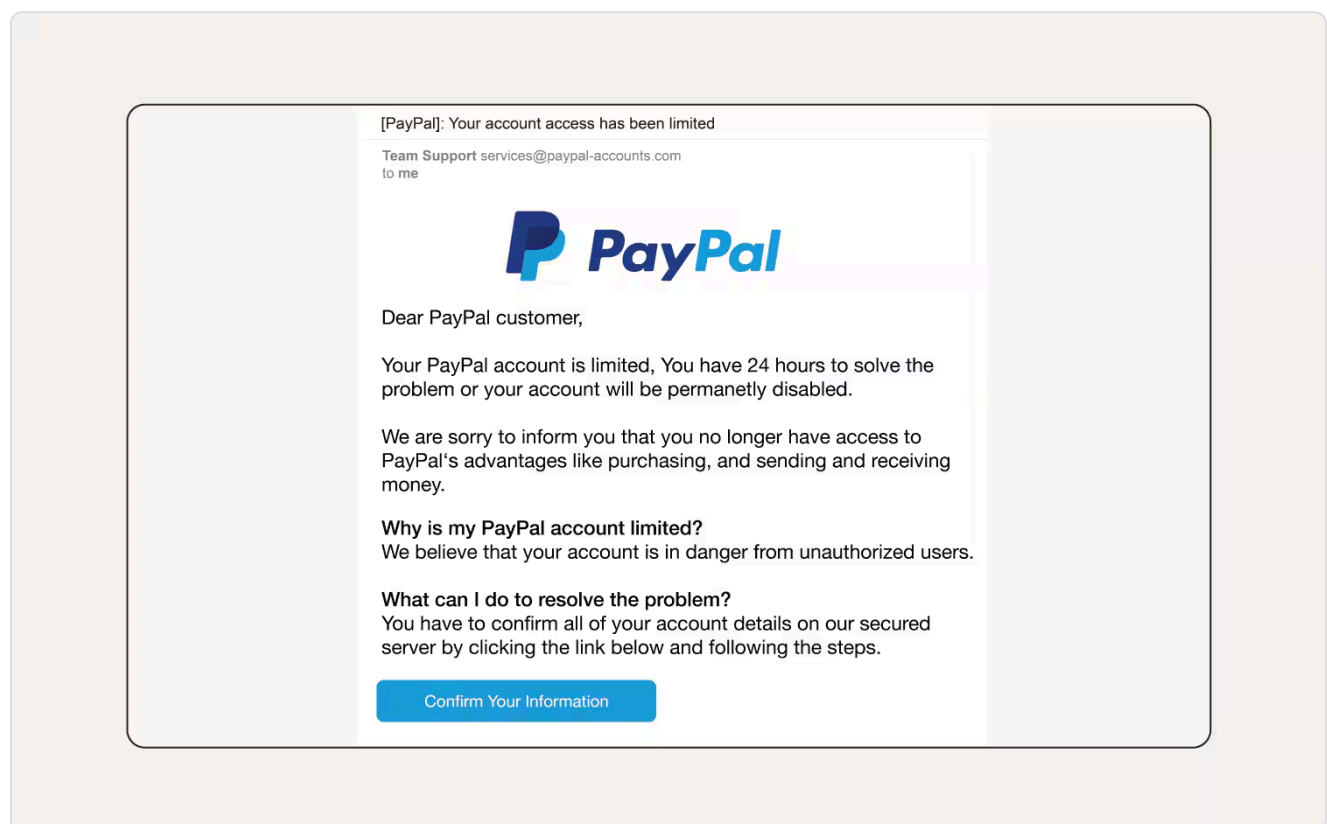
1. Dans un cheval de Troie (Trojan)

Un **cheval de Troie** est un logiciel malveillant caché dans un programme qui semble normal (jeu, logiciel gratuit...). Une fois installé, il peut contenir un **keylogger** qui enregistre les frappes au clavier.

2. Sur une clé USB

Un keylogger peut aussi être **installé via une clé USB infectée**. Il existe même des **keyloggers matériels** qui se branchent entre le clavier et l'ordinateur.

Phishing



Le phishing est une technique de fraude visant à dérober des données personnelles telles que l'état civil, les numéros de cartes bancaires, les identifiants et mots de passe.

Cette technique repose sur l'usurpation d'identité d'entités officielles, de services publics ou de marques reconnues pour provoquer chez la victime un état de panique ou d'euphorie, la désorientant et la poussant à divulguer ses informations personnelles.

Les outils utilisés incluent des sites web contrefaits, des e-mails ou SMS frauduleux, et des messages vocaux factices.

Synonymes : hameçonnage, harponnage.

Exemple : e-mail "votre compte sera fermé"

1. Tu reçois un mail "URGENCE : compte désactivé dans 24h".
2. Le mail contient :
 - logo,
 - ton prénom parfois,
 - un bouton "Confirmer".
3. Le bouton mène à un faux site copie conforme.
4. Tu saisis tes identifiants.
5. Le site les envoie au pirate **en temps réel**.
6. Le pirate se connecte aussitôt au vrai service.

Indices très concrets dans le mail :

- adresse expéditeur bizarre,
- lien qui ne correspond pas au domaine officiel,
- fautes ou tournures étranges,
- pression temporelle ("24h", "immédiat").

 **Le point clé** : tu donnes toi-même tes infos à l'attaquant.

Spyware (espionnage)



Un **spyware** est un logiciel espion qui **collecte des informations personnelles sur un utilisateur sans qu'il le sache**. Il peut accéder à des données sensibles comme les messages, les fichiers, les mots de passe ou l'activité sur Internet.

Exemple concret : Pegasus

Le spyware **Pegasus**, développé par l'entreprise NSO Group, a été au centre d'un scandale international révélé en 2021. Des enquêtes menées par plusieurs médias ont montré que ce logiciel avait été utilisé pour **espionner des journalistes, des militants et des responsables politiques**. Une fois installé sur un appareil, Pegasus pouvait accéder aux messages, aux emails, aux fichiers et même activer le micro ou la caméra.

➡ **Point clé** : un spyware sert à **espionner un utilisateur et à récupérer ses données personnelles de manière discrète**, souvent sans qu'il s'en rende compte.

Faillle Zero-Day (0-Day)

Une **faillle Zero-Day** est une vulnérabilité dans un logiciel **que l'éditeur ne connaît pas encore ou n'a pas encore corrigée**. Comme aucun correctif (patch) n'existe au moment de sa découverte, des attaquants peuvent l'exploiter avant que les développeurs aient le temps de la réparer.

Le terme **"Zero-Day"** signifie que les développeurs ont **zéro jour pour corriger la faille** lorsqu'elle devient connue.

Allusion à une série

La série Zero Day illustre bien ce type de menace : l'intrigue tourne autour d'une **cyberattaque massive exploitant des failles informatiques**, montrant comment des vulnérabilités inconnues peuvent provoquer des crises majeures.

Exemple réel dans les médias

En **2021**, plusieurs failles Zero-Day ont été découvertes dans le serveur de messagerie **Exchange** de Microsoft.

Des pirates les ont exploitées pour **s'introduire dans des milliers de serveurs d'entreprises et d'organisations dans le monde**, afin de voler des données ou installer des logiciels malveillants.

➡ **Point clé** : une faille Zero-Day est particulièrement dangereuse car **elle est exploitée avant qu'un correctif de sécurité soit disponible**.

Mot de passe

Un mot de passe fonctionne comme une clé donnant accès à un ordinateur, un fichier, etc.

Par exemple, si l'accès à un ordinateur est protégé par un mot de passe, il reste inaccessible à quiconque ne le connaît pas.

Il existe également des mots de passe pour restreindre l'utilisation d'une imprimante ou pour autoriser l'impression en couleur. Sans le mot de passe, l'impression se limitera au noir et blanc.

Étant donné que le mot de passe protège l'accès à une ressource, il fait souvent l'objet d'attaques.

Synonyme : Phrase de passe.

Une phrase de passe, composée de plusieurs mots séparés par des espaces, n'est pas nécessairement plus sécurisée qu'un mot de passe.

Vol d'identité

Le vol d'identité consiste à acquérir illégalement des informations d'identification d'une personne réelle : nom, prénom, date de naissance, adresse, numéro de téléphone, etc.

Ces données personnelles sont ensuite revendues sur le marché noir des cybercriminels.

En usurpant l'identité de leurs premières victimes, les fraudeurs peuvent monter des escroqueries ou commettre des fraudes ciblant d'autres victimes : particuliers, banques, organismes de crédit, assurances maladie, chômage, etc.

Le phishing est souvent utilisé pour récupérer des documents officiels d'une personne, tels qu'un extrait d'acte de naissance, une carte nationale d'identité ou une facture d'opérateur téléphonique mentionnant l'adresse de la victime.

Usurpation d'identité

Les escrocs utilisent souvent de fausses identités pour commettre leurs méfaits tout en restant anonymes. Ils peuvent créer de toutes pièces une fausse identité, mais préfèrent généralement usurper celle d'une personne réelle. Les cybercriminels procèdent de la même manière.

Imaginons un scénario simplifié mais réaliste : grâce au phishing, un cybercriminel obtient votre extrait d'acte de naissance et une copie de votre carte nationale d'identité, ainsi qu'une facture d'opérateur téléphonique indiquant votre adresse personnelle.

Avec ces documents, il peut solliciter plusieurs crédits en votre nom auprès de divers organismes de crédit.

Normalement, un établissement de crédit consciencieux vérifie l'authenticité de votre adresse et de votre identité (par envoi postal, etc.). Néanmoins, cette escroquerie reste efficace.

L'usurpation d'identité touche également les entités juridiques : entreprises privées, institutions publiques, etc.

Par exemple, un cybercriminel peut faire passer son site web pour celui d'une entreprise légitime afin de duper les internautes.

Authentification à Deux Facteurs (2FA)

L'authentification à deux facteurs est une méthode de sécurité qui requiert deux formes d'identification indépendantes pour accéder à un compte ou un système. C'est une couche de sécurité supplémentaire qui va au-delà du simple mot de passe.

Typiquement, la première forme d'identification est quelque chose que l'utilisateur sait, comme un mot de passe ou un code PIN. La seconde forme est généralement quelque chose que l'utilisateur possède, comme un smartphone (sur lequel un code temporaire peut être envoyé par SMS ou

généré par une application).

Dans certains cas, la 2FA peut aussi inclure quelque chose que l'utilisateur est, comme une empreinte digitale ou une autre forme de biométrie, pour ajouter encore plus de sécurité.

L'avantage de l'authentification à deux facteurs est qu'elle protège l'utilisateur contre le vol de mot de passe, car même si un attaquant obtient le mot de passe, il lui sera difficile d'accéder au compte sans la seconde forme d'identification.

Toutefois, il est important de noter que la 2FA n'est pas infaillible et peut être compromise par des attaques sophistiquées comme le phishing, où un attaquant pourrait tromper l'utilisateur pour obtenir les deux formes d'identification. Malgré cela, elle reste une des méthodes les plus efficaces pour sécuriser les accès en ligne.

CHAPITRE 2

Gérer vos mots de passe



Qui d'entre nous n'a jamais été confronté à la frustration d'oublier un mot de passe ? Ce moment désagréable où l'accès à un compte important est bloqué peut s'avérer stressant. Mais rassurez-vous, ces désagréments pourraient bien appartenir au passé. Dans ce chapitre, nous allons explorer des stratégies et des outils qui vous aideront à gérer efficacement vos mots de passe. Ainsi, avec quelques conseils simples et des pratiques sécuritaires, vous pourrez dire adieu à l'oubli de vos précieuses clés numériques.

2.1 Qu'est ce qu'un mot de passe fort?

Qu'est-ce qu'un mot de passe fort ?

Définition d'un mot de passe fort

Un mot de passe fort est une combinaison de caractères qui a pour but de sécuriser l'accès à un compte ou à des données. Il doit être difficile à deviner ou à casser par des attaquants, que ce soit par des tentatives manuelles (devinettes) ou automatisées (attaques par force brute ou à l'aide de logiciels spécialisés).

Composition d'un mot de passe fort

Pour être considéré comme fort, un mot de passe doit généralement répondre aux critères suivants :

- **Longueur** : Il doit être suffisamment long, généralement au moins 12 caractères, bien que 16 caractères ou plus soient recommandés pour une sécurité accrue.
- **Complexité** : Il doit inclure une combinaison de lettres majuscules et minuscules, de chiffres, et de symboles ou caractères spéciaux (comme !, @, #, etc.).
- **Unicité** : Il ne doit pas être facilement associable à l'utilisateur, comme l'utilisation de dates de naissance, noms d'animaux domestiques, ou d'autres informations personnelles facilement accessibles.

Pourquoi utiliser différents types de caractères

L'utilisation de différents types de caractères augmente le nombre de combinaisons possibles, ce qui rend le mot de passe plus difficile à deviner ou à pirater. Par exemple, un attaquant qui utilise une attaque par force brute (essayer toutes les combinaisons possibles) mettra beaucoup plus de temps à casser un mot de passe qui utilise un large éventail de caractères.

Durée de vie d'un mot de passe

La durée de vie d'un mot de passe fort dépend de plusieurs facteurs, notamment des directives de sécurité de l'organisation qui gère le compte et des pratiques de sécurité personnelles. Cependant, il est généralement recommandé de changer les mots de passe tous les 3 à 6 mois, ou immédiatement en cas de violation de données ou de soupçon que le mot de passe a été compromis.

Pourquoi avoir plusieurs mots de passe

Il est essentiel d'avoir des mots de passe différents pour chaque compte pour les raisons suivantes :

- **Réduire le risque de compromission multiple** : Si un attaquant obtient un mot de passe et que le même mot de passe est utilisé pour plusieurs comptes, il aura alors accès à tous ces comptes.
- **Sécurité spécifique au compte** : Certains comptes peuvent nécessiter un niveau de sécurité plus élevé en raison des informations sensibles qu'ils contiennent. Avoir des mots de passe uniques pour ces comptes renforce leur sécurité.
- **Gestion des violations de données** : En cas de fuite de données d'un service, seuls les comptes associés à ce service seront compromis, et non l'ensemble de vos comptes en ligne.

L'authentification à deux facteurs (2FA)

L'authentification à deux facteurs, souvent abrégée en 2FA, est une méthode de sécurité qui ajoute une couche supplémentaire de protection à l'habituel processus de connexion. Si vous utilisez uniquement un nom d'utilisateur et un mot de passe, c'est comme si vous aviez une seule serrure sur votre porte. Avec la 2FA, c'est comme si vous ajoutiez un verrou supplémentaire.

Comment fonctionne l'authentification à deux facteurs?

L'authentification à deux facteurs requiert deux types différents de preuves d'identité avant de vous donner accès à votre compte. Le premier facteur est généralement quelque chose que vous connaissez, comme votre mot de passe. Le deuxième facteur est quelque chose que vous possédez ou quelque chose que vous êtes, par exemple :

- **Quelque chose que vous possédez** : Un téléphone mobile sur lequel vous pouvez recevoir un code par SMS ou une application qui génère des codes de sécurité.
- **Quelque chose que vous êtes** : Utilisation de vos empreintes digitales, reconnaissance faciale ou autre biométrie.

Mise en place de l'authentification à deux facteurs

Pour activer la 2FA, vous devez généralement aller dans les paramètres de sécurité de votre compte en ligne. Voici les étapes générales, bien que les détails puissent varier selon le service :

1. **Connectez-vous à votre compte.**
2. **Recherchez une section comme 'Sécurité' ou 'Paramètres de connexion'.**
3. **Trouvez l'option pour activer l'authentification à deux facteurs ou la vérification en deux étapes.**
4. **Suivez les instructions** pour ajouter votre deuxième facteur, qui pourrait être un numéro de téléphone ou une application d'authentification comme Google Authenticator ou Authy.

Exemple concret

Prenons l'exemple de la mise en place de la 2FA sur un compte Google :

- Connectez-vous à votre compte Google.
- Allez dans "Sécurité" dans la barre latérale de navigation.
- Cliquez sur "Validation en deux étapes".
- Suivez les instructions pour ajouter votre téléphone comme deuxième étape.

Efficacité de l'authentification à deux facteurs

La 2FA est beaucoup plus sécurisée que la simple utilisation d'un mot de passe. Même si quelqu'un parvient à découvrir votre mot de passe, il lui sera difficile d'accéder à votre compte sans également avoir accès à votre deuxième facteur. Cela crée un obstacle significatif pour les attaquants, réduisant ainsi le risque de compromission de compte.

Points à considérer

- **Sécurité des messages SMS** : Recevoir un code par SMS n'est pas la méthode la plus sécurisée de 2FA en raison de techniques comme le "SIM swapping". Les applications d'authentification sont généralement plus sûres.
- **Gestion des accès** : Assurez-vous d'avoir une méthode de récupération en cas de perte de votre deuxième facteur, comme des codes de secours ou une adresse email de récupération.

2.2 Qu'est-ce qu'un générateur de mot de passe ?

Un **générateur de mot de passe** est un outil (site, application, extension ou gestionnaire de mots de passe) qui **crée automatiquement des mots de passe difficiles à deviner**.

Son objectif est de produire des mots de passe :

- **longs**
- **aléatoires**
- **riches en caractères variés**
- **uniques par compte**

Cela réduit fortement le risque d'attaque par **force brute** (tester beaucoup de combinaisons) ou par **dictionnaire** (tester des mots courants et variantes).

Comment ça fonctionne (plus précisément)

1) Génération "aléatoire" : hasard vs pseudo-hasard

Un bon générateur utilise un **générateur de nombres aléatoires cryptographiquement sûr** (souvent noté *CSPRNG*).

Ça veut dire :

- les valeurs produites sont **imprévisibles**

- même si on connaît beaucoup de mots de passe précédents, on ne peut pas “deviner” les suivants
- la génération est adaptée à la sécurité (contrairement à un hasard “simple” utilisé pour des jeux ou des simulations)

Exemple

Imaginons deux générateurs de mots de passe.

Générateur faible :

Il choisit les caractères dans un ordre simple comme dans l'alphabet :

abc123 , puis bcd234 , puis cde345 .

➡ On remarque un **schéma**. Un pirate peut donc deviner les prochains mots de passe.

Générateur sécurisé :

Il choisit chaque caractère **au hasard** parmi beaucoup de possibilités.

Exemples de mots de passe générés :

T8#kP4!mQ

zL7@rF2\$W

2) Construction du mot de passe : choix des caractères

Ensuite, l'outil **sélectionne des caractères** dans un ou plusieurs ensembles :

- minuscules : a-z
- majuscules : A-Z
- chiffres : 0-9
- symboles : !@#\$...

Deux points importants

- **Plus il y a de caractères possibles**, plus il y a de combinaisons → plus c'est difficile à casser.
- **La longueur** a souvent plus d'impact que “mettre un symbole”.

3) Options personnalisables (et pourquoi)

Les générateurs permettent souvent de régler :

✓ Longueur

- 12 caractères : bon niveau "standard"
- 16–20 : très solide
- 24+ : excellent (souvent inutilement long pour la plupart des usages, mais très robuste)

✓ Types de caractères

- Certains sites imposent : "1 majuscule, 1 chiffre, 1 symbole"
- Le générateur peut "forcer" ces contraintes pour que le mot de passe soit accepté

✓ Caractères ambigus

- Ex : 0 / 0 , 1 / 1 / I
- Utile si tu dois **l'écrire à la main** ou le communiquer oralement

Pourquoi ces mots de passe sont plus sûrs ?

1) Résistance à la force brute

Un pirate essaye des combinaisons automatiquement.

La difficulté dépend surtout de :

- **la longueur**
- **la variété de caractères**
- **le débit de tentative** (ça dépend du système attaqué)

Plus le mot de passe est long et aléatoire, plus le nombre de combinaisons explose.

2) Résistance aux attaques "humaines"

Les mots de passe inventés par des humains ont des patterns :

- mots + chiffres : azerty123
- dates : 2008 , 1999
- prénoms : amélie16

- substitutions classiques : a → @, o → 0

Les attaquants testent ces schémas en priorité.

Un générateur casse ce problème en produisant quelque chose comme :

vR7!qN2\$Lx9@pT

Exemples de générateurs

Intégrés à des gestionnaires de mots de passe

- Dashlane
- Bitwarden
- 1Password
- LastPass

Avantage : ils peuvent **générer + enregistrer automatiquement**.

En ligne (sites web)

Pratique, mais à utiliser avec prudence :

- éviter de générer un mot de passe pour un compte très sensible sur un site inconnu
- privilégier un gestionnaire reconnu ou un générateur "local" (dans ton navigateur/OS)

Comment utiliser un générateur correctement

1. Ouvre le générateur (ex : Dashlane)
2. Mets **16+ caractères** si possible
3. Active chiffres + symboles (si le site l'accepte)
4. Génère
5. Copie-colle dans le champ du site
6. **Enregistre dans le gestionnaire** (sinon tu vas le perdre)

🔴 Règle d'or : **un mot de passe différent par compte.**

Dashlane : ce que ça apporte en plus

Avec Dashlane (comme d'autres gestionnaires) tu as :

- **génération automatique** de mots de passe forts
 - **stockage chiffré** (les mots de passe sont gardés dans un "coffre-fort")
 - **remplissage automatique** pour éviter de retaper
 - alertes possibles si un mot de passe est :
 - réutilisé
 - trop faible
 - compromis lors d'une fuite de données (selon les fonctions)
-

À propos du "changement régulier" de mot de passe

Aujourd'hui, la recommandation la plus courante est plutôt :

✓ **changer si nécessaire**, par exemple :

- fuite de données
- suspicion de piratage
- mot de passe faible/réutilisé

Plutôt que de changer "tous les mois" (ça pousse souvent à choisir des mots de passe plus simples).

Erreurs fréquentes à éviter

- réutiliser le même mot de passe partout
- choisir un mot de passe "humain" (prénom, date, équipe...)
- stocker ses mots de passe dans un fichier non protégé
- envoyer un mot de passe par message non sécurisé

- ignorer l'activation de la **double authentification (2FA)** quand elle existe

2.3 Comment utiliser le gestionnaire de mots de passe de Google

Accéder au gestionnaire de mots de passe de Google

Le gestionnaire de mots de passe de Google est un service intégré à Google Chrome et à votre compte Google. Voici les étapes pour y accéder :

1. **Ouvrez Google Chrome** : Lancez le navigateur Google Chrome sur votre ordinateur, smartphone ou tablette.
2. **Connectez-vous à votre compte Google** : Cliquez sur le bouton de profil en haut à droite de Chrome et connectez-vous si ce n'est pas déjà fait.
3. **Accédez au gestionnaire de mots de passe** :
 - Sur ordinateur, vous pouvez cliquer sur votre photo de profil, puis sur la clé qui représente les mots de passe ou entrer `chrome://settings/passwords` dans la barre d'adresse.
 - Sur mobile, appuyez sur les trois points verticaux pour ouvrir le menu, allez dans "Paramètres", puis dans "Mots de passe".
4. **Consultez vos mots de passe** : Une fois dans la section mots de passe, vous verrez une liste de tous les sites pour lesquels vous avez enregistré des mots de passe. Vous pouvez les visualiser, les modifier ou les supprimer.

Avantages du gestionnaire de mots de passe de Google

- **Sécurité améliorée** : Google Chrome génère des mots de passe forts et uniques pour chaque site, ce qui réduit le risque de piratage de vos comptes.
- **Synchronisation** : Vos mots de passe sont synchronisés avec votre compte Google. Ainsi, peu importe l'appareil que vous utilisez, tant que vous êtes connecté à votre compte Google, vous aurez accès à vos mots de passe.
- **Remplissage automatique** : Google Chrome peut remplir automatiquement vos identifiants et mots de passe lorsque vous visitez un site web, ce qui vous fait gagner du temps.
- **Alerte de sécurité** : Google vous avertit si l'un de vos mots de passe a été compromis dans une violation de données connue.
- **Facilité d'utilisation** : L'interface est simple et intuitive, ce qui le rend accessible même pour les utilisateurs les moins expérimentés.

- **Gratuité** : Contrairement à certains gestionnaires de mots de passe tiers, celui de Google est entièrement gratuit.

En résumé, le gestionnaire de mots de passe de Google est un outil pratique et sécurisé pour stocker et gérer vos identifiants. Il offre une bonne base pour la gestion de mots de passe, surtout si vous utilisez déjà les services de Google.

2.4 Mise en pratique

Générer un mot de passe fort avec Dashlane

Pour générer un mot de passe fort avec Dashlane, suivez ces étapes :

1. **Ouvrez Dashlane** : Lancez l'application Dashlane sur votre appareil ou ouvrez l'extension de navigateur si vous l'utilisez.
 2. **Accédez au générateur de mots de passe** : Recherchez la fonctionnalité de générateur de mots de passe, souvent accessible via le menu principal ou une icône de génération de mots de passe.
 3. **Personnalisez votre mot de passe** : Sélectionnez les critères pour votre nouveau mot de passe, tels que la longueur, l'inclusion de chiffres, de symboles, de majuscules et de minuscules.
 4. **Générez le mot de passe** : Cliquez sur le bouton pour générer le mot de passe. Dashlane créera alors un mot de passe aléatoire qui respecte vos critères.
 5. **Utilisez ou enregistrez le mot de passe** : Utilisez le mot de passe généré pour votre compte en ligne ou laissez Dashlane l'enregistrer automatiquement pour vous.
-

Alternatives Gratuites à Dashlane

1. Bitwarden

- **Description** : Bitwarden est un gestionnaire de mots de passe open-source qui offre une version gratuite très complète. Il permet de stocker un nombre illimité de mots de passe, de les synchroniser sur plusieurs appareils et propose une extension de navigateur pour faciliter l'accès à vos comptes.
- **Exemple d'utilisation** :
 - Installation : Téléchargez l'application depuis le site officiel de Bitwarden ou via les magasins d'applications mobiles.
 - Création de compte : Inscrivez-vous avec une adresse e-mail et un mot de passe maître.

- Ajout de mots de passe : Importez vos mots de passe existants ou ajoutez-en de nouveaux manuellement.

2. LastPass (version gratuite)

- **Description** : LastPass propose une version gratuite qui permet de stocker des mots de passe et de les synchroniser entre appareils. Cependant, la version gratuite est limitée à un seul type d'appareil (soit mobile, soit ordinateur).
- **Exemple d'utilisation** :
 - Installation : Disponible sur les navigateurs, iOS et Android.
 - Fonctionnalités : Remplissage automatique des formulaires, générateur de mots de passe.

3. KeePass

- **Description** : KeePass est un gestionnaire de mots de passe open-source qui stocke les mots de passe localement sur votre appareil. Il est très sécurisé et offre de nombreuses fonctionnalités avancées.
- **Exemple d'utilisation** :
 - Installation : Téléchargez KeePass depuis le site officiel.
 - Fonctionnalités : Générateur de mots de passe, organisation par groupes, recherche de mots de passe.

4. NordPass (version gratuite)

- **Description** : NordPass propose une version gratuite qui inclut des fonctionnalités de base comme le stockage et l'organisation de mots de passe.
- **Exemple d'utilisation** :
 - Installation : Disponible pour Windows, macOS, Linux, Android, et iOS.
 - Fonctionnalités : Synchronisation sur plusieurs appareils, remplissage automatique des formulaires.

CHAPITRE 3

La sécurité sur les réseaux



Aujourd'hui, les réseaux sociaux font partie de notre quotidien. On les utilise pour **communiquer avec nos amis, partager des photos, suivre l'actualité ou regarder du contenu**. Des plateformes comme Instagram, TikTok, Snapchat ou Facebook sont utilisées chaque jour par des millions de personnes.

Mais cette utilisation a aussi un **côté moins visible** : elle peut présenter certains **risques pour la sécurité et la vie privée**. En effet, lorsque l'on publie des informations en ligne, on peut parfois **partager des données personnelles sans vraiment s'en rendre compte**.

Ces informations peuvent ensuite être utilisées par des personnes mal intentionnées pour **arnaquer, voler des données ou usurper une identité**.

C'est pourquoi il est important de **comprendre les risques liés aux réseaux sociaux** et de savoir **comment protéger ses informations**.

Dans cette partie du cours, nous allons notamment voir **les principaux risques**, comme **l'exposition des données personnelles et les différentes formes d'escroqueries en ligne**, ainsi que **les bonnes pratiques pour se protéger**

3.1 Identification des risques principaux

Exposition des données personnelles

L'exposition involontaire de données personnelles peut avoir des conséquences graves. Voici des exemples concrets de ce phénomène.

Quelles informations sont souvent exposées sans conscience ?

Anecdote réelle

En 2018, un incident impliquant Strava, une application de suivi d'activité physique, a révélé des emplacements de bases militaires secrètes. Les utilisateurs de l'application, y compris des militaires, utilisaient Strava pour enregistrer leurs parcours de jogging, révélant involontairement des itinéraires précis dans des zones sensibles.

Solution

Il est essentiel de vérifier les paramètres de confidentialité des applications utilisées et de désactiver le partage de localisation, surtout dans des contextes où la divulgation de votre localisation pourrait être sensible ou dangereuse.

Conséquences de l'exposition de données personnelles

Anecdote réelle

En 2017, Equifax, une des plus grandes agences de crédit aux États-Unis, a subi une violation de données affectant environ 143 millions de personnes. Des informations personnelles et financières sensibles ont été exposées, conduisant à des cas massifs de fraudes et d'usurpations d'identité.

Solution

Pour se protéger contre de telles expositions, il est recommandé d'utiliser des services de surveillance de crédit et d'activer les alertes de transaction sur tous les comptes financiers pour détecter rapidement toute activité suspecte.

Escroqueries et fraudes

Les escroqueries sur Internet sont diverses et affectent des millions de personnes chaque année.

Types d'escroqueries courantes

Anecdote réelle

En 2020, lors de la pandémie de COVID-19, des escrocs ont envoyé des emails de phishing se faisant passer pour des organisations de santé mondiale, demandant des dons pour le soi-disant "fonds de réponse au coronavirus". Beaucoup de personnes ont été trompées et ont envoyé de l'argent à ces faux fonds.

Solution

Il est crucial de vérifier la source de tout email ou message demandant des informations personnelles ou financières. Visitez toujours les sites web officiels en entrant l'URL directement dans votre navigateur au lieu de cliquer sur des liens dans des emails ou des messages.

Méthodes utilisées par les escrocs pour exploiter les utilisateurs

Anecdote réelle

En 2019, un homme âgé a été victime d'une escroquerie par téléphone où un escroc se faisant passer pour un agent de l'IRS (le service des impôts américain) a exigé un paiement immédiat pour de prétendus impôts en retard, menaçant de l'arrestation.

Solution

Apprenez à reconnaître les signes d'escroquerie par téléphone : les agences gouvernementales ne demandent jamais de paiements urgents par des moyens non traçables comme les cartes cadeaux ou les transferts en ligne. En cas de doute, raccrochez et appelez directement l'organisation concernée via un numéro officiel.

3.2 Mécanismes d'attaque courants

Hameçonnage (Phishing)

Reconnaître un email ou message de phishing

Le phishing est une technique utilisée par les cybercriminels pour obtenir des informations sensibles (comme des mots de passe ou des informations bancaires) en se faisant passer pour une source fiable. Voici comment reconnaître un email de phishing :

- **L'urgence** : Le message incite à agir rapidement, souvent avec des menaces de conséquences graves.
- **Fautes de grammaire et d'orthographe** : Les messages contiennent souvent des erreurs.

- **Adresses étranges** : L'adresse de l'expéditeur ne correspond pas à celle de l'organisation qu'elle prétend représenter.
- **Liens suspects** : Survolez les liens pour voir l'URL réelle avant de cliquer. Les liens peuvent sembler légitimes mais rediriger vers un site malveillant.

Exemple réel : En 2020, des utilisateurs ont reçu des emails prétendument de l'OMS, demandant des dons pour le COVID-19 via Bitcoin. Ces emails étaient des tentatives de phishing.

Précautions à prendre avec les liens et pièces jointes

- **Ne cliquez pas** sur les liens ou pièces jointes dans un email dont vous n'êtes pas sûr de la source.
- **Vérifiez l'URL** : Assurez-vous que l'URL est correcte et sécurisée (https, non http).
- **Utilisez des logiciels antivirus** : Assurez-vous que vos systèmes sont protégés par des logiciels de sécurité à jour.

Malware et ransomware via les réseaux sociaux

Diffusion de malware à travers des liens et applications malveillantes

Les réseaux sociaux peuvent être utilisés pour diffuser des malwares via des liens et des applications trompeuses. Ces liens peuvent apparaître dans des publications, des messages privés ou des publicités.

- **Applications trompeuses** : Méfiez-vous des applications qui demandent des permissions excessives ou qui semblent trop belles pour être vraies.

Signes d'une infection par malware et étapes à suivre en cas de compromission

Voici quelques signes que votre appareil pourrait être infecté par un malware :

- **Performance réduite** : Votre appareil est lent ou se bloque fréquemment.
- **Apparition de pop-ups** : Des fenêtres pop-up s'affichent régulièrement sans raison apparente.
- **Usage élevé de la bande passante** : Une utilisation anormale de données peut indiquer que le malware communique avec un serveur distant.

Étapes à suivre :

1. **Déconnectez votre appareil** du réseau pour empêcher la propagation du malware.
2. **Exécutez un logiciel antivirus** pour identifier et supprimer le malware.
3. **Changez vos mots de passe** après avoir nettoyé votre appareil.

Anecdote réelle : En 2017, le ransomware WannaCry a infecté des centaines de milliers d'ordinateurs dans le monde, cryptant les données et demandant une rançon pour les débloquent. La propagation a été stoppée lorsque un chercheur en sécurité a activé un "interrupteur d'arrêt" enregistré dans le code du malware.

3.3 Stratégies de protection efficaces

Réglages de confidentialité et de sécurité

Importance de comprendre et de configurer les paramètres de confidentialité

Les réglages de confidentialité dans les applications et sur les plateformes en ligne déterminent qui peut voir vos informations et dans quelles circonstances. Il est essentiel de comprendre ces paramètres pour pouvoir les configurer de manière à protéger vos données personnelles. Par exemple, sur les réseaux sociaux, vous devriez être en mesure de contrôler qui peut voir vos publications, vos photos, ou même votre profil. Prendre le temps de comprendre et de configurer ces paramètres peut grandement diminuer le risque d'exposition de vos informations personnelles.

Examen des permissions accordées aux applications tierces

Les applications tierces souvent demandent des permissions pour accéder à des informations sur votre appareil comme vos contacts, votre emplacement, ou même votre caméra. Il est crucial de réviser ces permissions avant de les accorder. Demandez-vous si l'application a vraiment besoin de ces informations pour fonctionner correctement. Si ce n'est pas le cas, il vaut mieux refuser l'accès pour minimiser les risques de fuites de données.

Configuration des paramètres de confidentialité sur Facebook

Facebook offre de multiples options pour personnaliser vos paramètres de confidentialité. Voici quelques exemples spécifiques :

1. Qui peut voir vos publications ?

Dans les paramètres de confidentialité, vous pouvez choisir qui peut voir vos nouvelles publications : tout le monde, seulement vos amis, des amis spécifiques, ou seulement vous. Il est recommandé de limiter l'accès à vos amis pour protéger votre vie privée.

2. Examen des tags avant publication :

Vous pouvez configurer Facebook pour examiner et approuver tout tag que quelqu'un essaie d'ajouter à vos photos ou publications avant qu'il ne devienne visible publiquement.

3. Contrôle des applications connectées :

Accédez à la section "Applications et sites web" dans les paramètres de Facebook pour voir quelles applications ont accès à vos données. Vous pouvez y révoquer des permissions qui ne

sont pas essentielles ou des applications que vous n'utilisez plus.

Hygiène numérique

Importance des mots de passe forts et de l'authentification à deux facteurs

Un mot de passe fort est la première ligne de défense contre les accès non autorisés à vos comptes. Utilisez des mots de passe longs, avec une combinaison de lettres majuscules et minuscules, de chiffres et de symboles. Évitez d'utiliser le même mot de passe pour plusieurs sites ou applications. L'authentification à deux facteurs ajoute une couche supplémentaire de sécurité en requérant un deuxième facteur de vérification, généralement un code envoyé à votre téléphone ou généré par une application, pour accéder à votre compte.

Conseils pour une navigation sécurisée et consciente

La navigation sécurisée commence par la sensibilisation aux sites que vous visitez et aux informations que vous partagez en ligne. Utilisez toujours des connexions sécurisées (HTTPS) et soyez prudent avec les liens sur lesquels vous cliquez, surtout s'ils proviennent de sources inconnues ou suspectes. Installez des extensions de navigateur fiables qui peuvent bloquer les publicités intrusives et les trackers. De plus, assurez-vous que votre navigateur et votre système d'exploitation sont toujours à jour pour bénéficier des dernières protections de sécurité.

3.4 Outils de protection

Utilisation d'outils de sécurité numérique

Antivirus, anti-spyware, et autres outils de sécurité recommandés

Dans le domaine de la sécurité informatique, l'utilisation d'outils spécialisés est essentielle pour protéger vos appareils contre les menaces externes. Voici quelques-uns des outils les plus recommandés :

1. **Antivirus** : Un logiciel antivirus est essentiel pour détecter, bloquer et supprimer les logiciels malveillants. Des exemples populaires incluent Avast, Kaspersky, et Norton.
2. **Anti-spyware** : Ces outils sont spécifiquement conçus pour combattre les logiciels espions qui peuvent collecter des informations sur vous sans votre consentement. Malwarebytes est un exemple de tool efficace dans cette catégorie.
3. **Firewalls** : Un pare-feu aide à contrôler le trafic entrant et sortant de votre réseau, bloquant les accès non autorisés.

4. **Gestionnaires de mots de passe** : Ils stockent et organisent vos mots de passe pour vous aider à maintenir la sécurité de vos comptes. Des exemples incluent LastPass et 1Password.

Extensions de navigateur pour améliorer la sécurité

Les extensions de navigateur peuvent également jouer un rôle crucial dans la protection de votre activité en ligne. Voici quelques extensions recommandées :

- **HTTPS Everywhere** : Force le navigateur à utiliser des connexions sécurisées lorsque c'est possible, améliorant ainsi la sécurité de vos données.
- **uBlock Origin** : Un bloqueur de publicités qui peut également bloquer les trackers et les malwares connus.
- **Privacy Badger** : Bloque les trackers invisibles et améliore la confidentialité de vos activités en ligne.

3.5 Un antivirus est-il vraiment utile aujourd'hui ?

Oui, **un antivirus reste utile**, car il sert à **détecter, bloquer et supprimer les logiciels malveillants** (virus, ransomwares, spyware, etc.). Il analyse le système et les fichiers pour repérer des programmes dangereux et protéger les données de l'utilisateur.

Aujourd'hui, les ordinateurs ont déjà une protection intégrée (comme Microsoft Defender sur Windows), qui protège contre la plupart des menaces classiques : virus, malwares ou phishing.

👉 Donc pour un usage normal, **la protection intégrée peut déjà être suffisante**.

Comparaison des 5 leaders des antivirus

Bitdefender

Avantages

- Très **haut taux de détection des virus** dans les tests indépendants.
- Protection avancée contre les **ransomwares et le phishing**.
- Beaucoup de fonctionnalités (VPN, protection bancaire, optimisation système).
- Interface assez simple à utiliser.

Inconvénients

- Certaines options (VPN complet, outils avancés) sont **payantes**.
 - Peut être **un peu lourd pour l'ordinateur** sur certaines configurations.
-

Norton 360

Avantages

- Suite de sécurité **très complète** (VPN, gestionnaire de mots de passe, sauvegarde cloud).
- Très bon niveau de **détection des malwares**.
- Protection contre le **phishing et les arnaques en ligne**.

Inconvénients

- Peut être **cher** selon les abonnements.
 - Interface parfois **chargée et remplie d'options**.
-

McAfee Total Protection

Avantages

- Protège **plusieurs appareils** avec un seul abonnement.
- Bon système de **protection contre le vol d'identité**.
- Protection web efficace contre les sites dangereux.

Inconvénients

- Peut générer **de faux positifs** (fichiers sûrs détectés comme virus).
 - Interface parfois jugée **moins intuitive**.
-

Kaspersky Anti-Virus

Avantages

- Très **bonne détection des malwares**.
- Antivirus **rapide et léger** sur les performances.
- Bonne protection de la **webcam et du réseau domestique**.

Inconvénients

- Controverses politiques et restrictions dans certains pays.
 - Moins de fonctionnalités avancées dans la version de base.
-

Microsoft Defender

Avantages

- **Gratuit et intégré** dans Windows.
- Protection correcte contre les menaces courantes.
- Aucun logiciel supplémentaire à installer.

Inconvénients

- Moins de fonctionnalités avancées (VPN, gestion des identités...).
- Protection parfois **moins complète que les suites payantes**.

Antivirus	Point fort principal	Point faible principal
Bitdefender	Protection très performante	Options avancées payantes
Norton	Suite très complète	Prix élevé
McAfee	Protection multi-appareils	Faux positifs possibles
Kaspersky	Rapide et très efficace	Controverses géopolitiques
Defender	Gratuit et intégré	Moins complet

Bitdefender est-il plus efficace ?

Les tests de sécurité montrent que **Microsoft Defender et Bitdefender détectent tous les deux très bien les virus**, avec parfois **100 % de détection dans certains tests**.

Cependant, **Bitdefender offre généralement plus de fonctionnalités**, par exemple :

- protection contre les sites de phishing
- VPN intégré
- gestionnaire de mots de passe
- protection webcam ou micro
- détection avancée des menaces

C'est pour cela qu'il est souvent considéré comme **l'un des meilleurs antivirus du marché** par les tests indépendants.

CHAPITRE 4

Le VPN

Qu'est-ce qu'un VPN ?

Un **VPN** (Virtual Private Network) est un service qui permet de créer une connexion sécurisée et cryptée sur un réseau moins sécurisé, tel qu'Internet. Il agit comme un tunnel qui protège vos données en les cachant des regards indiscrets, y compris ceux des pirates informatiques, des fournisseurs d'accès Internet et même des gouvernements.

Fonctionnement d'un VPN

1. **Cryptage des Données** : Lors de la connexion à un VPN, vos données sont cryptées, rendant toute information envoyée ou reçue illisible pour quiconque tenterait de l'intercepter.
2. **Adresse IP Masquée** : Un VPN masque votre adresse IP réelle en la remplaçant par celle du serveur VPN, ce qui permet de cacher votre localisation géographique et de naviguer anonymement sur Internet.
3. **Accès à du Contenu Restreint** : En vous connectant à un serveur VPN situé dans un autre pays, vous pouvez accéder à du contenu qui pourrait être restreint ou censuré dans votre région.

Utilité d'un VPN

Sécurité et Confidentialité

- **Protection des Données Personnelles** : Un VPN protège vos informations personnelles, telles que les mots de passe et les numéros de carte de crédit, contre les cyberattaques.
- **Navigation Anonyme** : Il vous permet de naviguer sur le web sans laisser de traces, protégeant ainsi votre vie privée en ligne.

Accès à Internet Sans Restrictions

- **Contourner la Censure** : Dans certains pays, l'accès à certains sites web est limité. Un VPN vous permet de contourner ces restrictions en vous connectant à un serveur dans un pays où le contenu est accessible.
- **Accéder à des Contenus Géographiquement Limités** : Vous pouvez par exemple regarder des séries ou des films disponibles uniquement dans certaines régions en vous connectant à un serveur de cette région.

Sécurité sur les Réseaux Wi-Fi Publics

- **Protection sur les Réseaux Non Sécurisés** : L'utilisation d'un VPN sur un réseau Wi-Fi public protège vos données des interceptions par des tiers malveillants qui pourraient exploiter la faible sécurité de ces réseaux.

Sécurité des VPN sur les Réseaux Publics

L'utilisation d'un **VPN** sur des réseaux Wi-Fi publics est fortement recommandée pour sécuriser vos données. Cependant, bien que les VPN offrent une protection significative, ils ne sont pas infailibles.

Avantages de l'utilisation d'un VPN sur les Réseaux Publics

1. **Cryptage des Données** : Un VPN crypte vos données, empêchant les pirates d'intercepter et de lire vos informations sensibles.
2. **Protection contre l'Espionnage** : Sur un réseau public, il est facile pour des attaquants de surveiller le trafic. Un VPN masque votre trafic, rendant difficile pour quiconque de suivre vos activités en ligne.

Limites et Risques Potentiels

1. **VPN Compromis** : Si le fournisseur de VPN est compromis, vos données pourraient être à risque. Il est crucial de choisir un fournisseur de VPN réputé et fiable.
2. **Vulnérabilités Logicielles** : Comme tout logiciel, les applications VPN peuvent avoir des failles de sécurité. Il est important de maintenir votre logiciel VPN à jour pour bénéficier des derniers correctifs de sécurité.
3. **Faux Sentiment de Sécurité** : Un VPN ne protège pas contre toutes les menaces. Par exemple, si vous téléchargez un fichier malveillant ou visitez un site web frauduleux, un VPN ne pourra pas vous protéger.
4. **Fuites DNS et IP** : Parfois, des fuites peuvent se produire, exposant votre adresse IP ou vos requêtes DNS. Utilisez des outils en ligne pour vérifier que votre VPN ne présente pas de fuites.

Bonnes Pratiques

- **Choisir un VPN Fiable** : Optez pour des fournisseurs de VPN qui ont une bonne réputation et qui offrent des politiques de non-conservation des logs.
- **Activer le Kill Switch** : Cette fonctionnalité coupe automatiquement votre connexion Internet si le VPN se déconnecte, empêchant ainsi l'exposition de vos données.

Choisir un VPN : Fiabilité et Options Gratuites ou Payantes

Critères de Sélection d'un VPN Fiable

Pour choisir un VPN fiable, il est important de prendre en compte plusieurs critères :

1. **Politique de Non-conservation des Logs** : Assurez-vous que le VPN ne conserve pas de journaux de vos activités en ligne. Cela garantit votre anonymat.
2. **Protocole de Sécurité** : Optez pour un VPN qui utilise des protocoles de sécurité robustes comme OpenVPN ou WireGuard.
3. **Vitesse de Connexion** : Un bon VPN doit offrir des vitesses de connexion rapides pour éviter les ralentissements lors de la navigation ou du streaming.
4. **Couverture Géographique** : Vérifiez que le VPN dispose de serveurs dans les pays où vous souhaitez accéder à des contenus spécifiques.
5. **Support Client** : Un service client réactif est essentiel en cas de problèmes techniques.

VPN Payants Recommandés

Les VPN payants sont souvent plus fiables et offrent plus de fonctionnalités que les versions gratuites. Voici quelques options populaires :

- **NordVPN** : Connu pour sa sécurité robuste et sa large couverture de serveurs.
- **ExpressVPN** : Offre des vitesses rapides et une excellente protection de la vie privée.
- **CyberGhost** : Facile à utiliser, avec une bonne politique de non-conservation des logs.

VPN Gratuits

Il existe des VPN gratuits, mais ils ont souvent des limitations :

- **ProtonVPN** : Offre une option gratuite sans limitation de bande passante, mais avec un choix limité de serveurs.
- **Windscribe** : Propose un plan gratuit avec une limite de données mensuelle, mais avec une bonne sécurité.
- **TunnelBear** : Facile à utiliser, mais limité à 500 Mo de données par mois dans la version gratuite.

Avantages et Inconvénients des VPN Gratuits

- **Avantages** : Pas de coût initial, idéal pour un usage occasionnel ou pour tester le service.

- **Inconvénients** : Limitations en termes de bande passante, de vitesse, et de choix de serveurs. Certains VPN gratuits peuvent également vendre vos données à des tiers pour compenser le manque de revenus.

VPN avec Antivirus

Certains fournisseurs de VPN intègrent également des fonctionnalités antivirus pour offrir une protection complète. Voici quelques options :

- **NordVPN avec Nord Security** : En plus de son service VPN, NordVPN propose des outils de sécurité supplémentaires comme un bloqueur de publicités et de logiciels malveillants.
- **Avast SecureLine VPN** : Bien que principalement un antivirus, Avast offre également un service VPN intégré pour protéger votre navigation.
- **Bitdefender Premium VPN** : Proposé par Bitdefender, un leader dans le domaine des antivirus, il offre une protection VPN en complément de ses solutions antivirus.

Avantages des VPN avec Antivirus

- **Protection Complète** : Combiner un VPN avec un antivirus offre une sécurité renforcée contre les menaces en ligne et les logiciels malveillants.
- **Gestion Simplifiée** : Avoir un seul fournisseur pour la sécurité et la confidentialité en ligne peut simplifier la gestion des abonnements et des mises à jour.

Inconvénients Potentiels

- **Coût Élevé** : Ces solutions combinées peuvent être plus coûteuses que d'acheter séparément un VPN et un antivirus.
- **Performance** : L'ajout de fonctionnalités antivirus à un VPN peut parfois ralentir la connexion en raison des processus supplémentaires de vérification.

4.1 Wifi repeater ou mesh?

Qu'est-ce qu'un répéteur Wi-Fi ?

Un répéteur Wi-Fi, aussi appelé amplificateur de signal ou extender, est un dispositif qui capte le signal Wi-Fi existant de votre routeur principal et le retransmet pour étendre la couverture du réseau. Il est particulièrement utile dans les grandes maisons ou les espaces où le signal Wi-Fi est faible.

Exemple de fonctionnement :

- **Maison à deux étages** : Si votre routeur est situé au rez-de-chaussée et que le signal est faible à l'étage, un répéteur placé à mi-chemin peut améliorer la couverture à l'étage.

Système Wi-Fi Mesh : Un Réseau Sans Perte de Puissance

Un système Wi-Fi Mesh est conçu pour offrir une couverture Wi-Fi homogène et performante dans toute votre maison ou votre bureau, sans les pertes de puissance souvent associées aux répéteurs traditionnels. Voici comment cela fonctionne :

Création d'un Réseau Unifié

- **Nœuds Interconnectés** : Un système Mesh est composé de plusieurs nœuds (ou unités) qui sont placés stratégiquement dans votre espace. Chaque nœud communique avec les autres pour créer un **réseau maillé**. Contrairement aux répéteurs, qui simplement retransmettent le signal du routeur principal, les nœuds Mesh partagent les données entre eux, ce qui permet de maintenir une connexion stable et rapide.

Avantages du Système Mesh

- **Pas de Perte de Puissance** : Chaque nœud du système Mesh dispose de sa propre connexion avec les autres nœuds, ce qui signifie que le signal ne faiblit pas à mesure qu'il est transmis d'un nœud à l'autre. Cela contraste avec les répéteurs qui peuvent réduire la bande passante disponible en réutilisant le même canal pour recevoir et transmettre des données.
- **Réseau Unique** : Avec un système Mesh, vous n'avez qu'un seul nom de réseau (SSID) et un seul mot de passe pour toute votre maison. Cela signifie que vos appareils se connectent automatiquement au nœud le plus proche et le plus performant, sans interruption de service lorsque vous vous déplacez.
- **Optimisation Dynamique** : Les systèmes Mesh utilisent des technologies avancées pour optimiser automatiquement le chemin de transmission des données. Par exemple, si un nœud devient surchargé, le système peut rediriger le trafic vers un autre nœud pour maintenir une performance optimale.

Installation et Gestion

- **Installation Facile** : Les systèmes Mesh sont souvent accompagnés d'applications mobiles intuitives qui facilitent l'installation et la gestion du réseau. Vous pouvez facilement ajouter ou déplacer des nœuds pour adapter le réseau à vos besoins en constante évolution.
- **Gestion Simplifiée** : Grâce à l'application, vous pouvez surveiller l'activité du réseau, gérer les appareils connectés, et même configurer des paramètres avancés comme le contrôle parental ou les priorités de bande passante.

En résumé, un système Wi-Fi Mesh est idéal pour ceux qui cherchent une solution fiable et performante pour couvrir de grandes surfaces sans compromis sur la vitesse ou la stabilité du réseau.

Exemple de fonctionnement :

- **Grand espace ouvert** : Dans un grand bureau ou une maison de plusieurs étages, des nœuds Mesh peuvent être placés à différents endroits pour assurer une couverture Wi-Fi homogène partout.

Différences principales

- **Structure** : Les répéteurs fonctionnent en captant et retransmettant le signal, tandis que les systèmes Mesh créent un réseau maillé où chaque nœud communique avec les autres.
- **Performance** : Les systèmes Mesh offrent généralement une meilleure performance et une couverture plus homogène, car ils optimisent automatiquement le chemin de transmission des données.
- **Installation** : Les systèmes Mesh sont souvent plus faciles à installer et à gérer via des applications mobiles.

Coût et budget

- **Répéteurs Wi-Fi** : En général, les répéteurs sont moins chers, avec des prix commençant autour de 20-50 euros pour les modèles de base.
- **Systèmes Mesh** : Les systèmes Mesh sont plus coûteux, avec des prix variant de 150 à 500 euros ou plus, selon le nombre de nœuds et les fonctionnalités.

Utilité et nécessité

- **Utilité** : Si vous avez des zones mortes ou une couverture Wi-Fi inégale, un répéteur ou un système Mesh peut être très utile pour améliorer votre expérience Internet.
- **Nécessité** : La nécessité dépend de la taille de votre espace et de vos besoins en connectivité. Pour une petite maison ou un appartement, un bon routeur peut suffire. Pour les grandes maisons ou les bureaux, un système Mesh est souvent recommandé pour une couverture optimale.

1. TP-Link Deco

TP-Link est une marque bien établie dans le domaine des réseaux, et sa gamme Deco est particulièrement appréciée pour sa facilité d'utilisation et sa connectivité fiable.

- **TP-Link Deco M5** : Un modèle populaire offrant une couverture solide et des fonctionnalités de sécurité avancées. Il est idéal pour les maisons de taille moyenne.

- **TP-Link Deco X60** : Un modèle plus avancé qui prend en charge le Wi-Fi 6, offrant des vitesses plus rapides et une meilleure gestion des appareils connectés simultanément.
- **TP-Link Deco P9** : Combine le Wi-Fi Mesh avec la technologie Powerline, ce qui est utile dans les maisons où le signal Wi-Fi peut être obstrué par des murs épais.

2. Huawei

Huawei propose également des solutions Mesh performantes, comme le Huawei Mesh X3 Pro.

- **Huawei Mesh X3 Pro** : Ce modèle offre une couverture étendue et des vitesses élevées, idéal pour les grandes maisons ou les bureaux. Il est compatible avec le Wi-Fi 6, ce qui assure une connectivité rapide et stable.

3. Netgear Orbi

Netgear est une autre marque de confiance dans le domaine des réseaux, connue pour ses systèmes Mesh haut de gamme.

- **Netgear Orbi RBK50** : Un système Mesh puissant qui offre une couverture exceptionnelle et des vitesses rapides, adapté aux grandes maisons.
- **Netgear Orbi WiFi 6 (RBK852)** : Un modèle premium qui utilise le Wi-Fi 6 pour offrir des performances optimales, même dans les environnements les plus exigeants.

4. Google Nest Wifi

Google Nest Wifi est reconnu pour son design élégant et son intégration facile avec d'autres appareils Google.

- **Google Nest Wifi** : Offre une couverture étendue et une gestion simplifiée via l'application Google Home. Chaque point d'accès Nest Wifi peut également fonctionner comme un haut-parleur intelligent avec Google Assistant intégré.

CHAPITRE 5

Sur mobile

Les smartphones et les tablettes sont devenus des outils indispensables dans notre quotidien, mais ils sont également vulnérables à divers types de menaces sécuritaires. Nous explorerons les points sur lesquels il faut porter une attention particulière pour protéger efficacement vos appareils mobiles.

Les risques de sécurité sur les appareils mobiles

Les applications malveillantes

Les applications sont souvent la porte d'entrée pour de nombreux types de menaces. Il est crucial de vérifier la source de chaque application avant de la télécharger et de s'assurer qu'elle provient d'un éditeur fiable. Les magasins d'applications officiels comme Google Play Store ou Apple App Store ont des mesures de sécurité, mais ne sont pas infailibles.

Anecdote 1 : L'application de cryptomonnaie trompeuse

Scénario : En 2021, des utilisateurs de Google Play Store ont été victimes d'une application se faisant passer pour un portefeuille de cryptomonnaies légitime. Cette application, qui imitait l'interface d'une application populaire, demandait aux utilisateurs de transférer leurs cryptomonnaies pour bénéficier d'une prétendue sécurité améliorée. Les fonds transférés étaient en réalité envoyés directement aux comptes des escrocs. L'application a été retirée après que des utilisateurs aient rapporté des pertes significatives.

Anecdote 2 : L'application de lampe torche intrusive

Scénario : Une application de lampe torche téléchargée des millions de fois sur Android et iOS a été découverte collectant et envoyant des données GPS, des listes de contacts et même des contenus de messages textes à un serveur distant. L'application, bien qu'offrant simplement une fonction de lampe torche, utilisait ces données pour des campagnes de publicité ciblée sans le consentement explicite des utilisateurs. Suite à des enquêtes, l'application a été supprimée des deux plateformes.

Anecdote 3 : Jeux pour enfants avec publicités abusives

Scénario : Des parents ont rapporté que leurs enfants étaient exposés à des publicités inappropriées via des jeux populaires pour enfants disponibles sur l'Apple App Store. Ces jeux, bien que gratuits, montraient des publicités trompeuses qui poussaient les enfants à effectuer des

achats in-app sans le consentement de leurs parents. Après de nombreuses plaintes, les développeurs ont dû modifier leur stratégie de monétisation et réduire la fréquence des publicités.

Anecdote 4 : L'application de fitness vendant des données

Scénario : Une application de suivi de fitness très téléchargée a été prise en flagrant délit de vente de données d'utilisateurs à des compagnies d'assurance et des annonceurs sans en informer clairement ses utilisateurs. L'application analysait les activités physiques et les habitudes de sommeil, et ces données étaient utilisées pour ajuster les tarifs des assurances ou cibler des publicités. Après un scandale médiatique, l'application a dû changer ses pratiques de confidentialité et informer explicitement les utilisateurs de l'utilisation de leurs données.

Les mises à jour de sécurité

Les systèmes d'exploitation des appareils mobiles, comme Android et iOS, sont régulièrement mis à jour pour corriger des failles de sécurité. Ignorer ces mises à jour peut laisser votre appareil vulnérable à des attaques. Il est donc essentiel de configurer vos appareils pour qu'ils se mettent à jour automatiquement ou de vérifier régulièrement les mises à jour disponibles.

Les connexions réseau non sécurisées

Les connexions Wi-Fi publiques et non sécurisées peuvent être des vecteurs d'attaques. Utiliser un réseau non sécurisé peut permettre à des hackers de s'introduire dans votre appareil ou d'intercepter vos données. Il est recommandé d'utiliser des réseaux sécurisés et, si nécessaire, d'utiliser un VPN (Virtual Private Network) pour chiffrer vos communications.

La perte ou le vol d'appareils

Les appareils mobiles sont particulièrement susceptibles d'être perdus ou volés. Il est important de mettre en place des mesures telles que le verrouillage par code PIN, le chiffrement des données et des fonctionnalités de localisation et de suppression à distance pour minimiser les risques en cas de perte ou de vol.

Bonnes pratiques de sécurité sur mobile

Utilisation de mots de passe forts et de l'authentification à deux facteurs

Pour chaque application et service utilisé sur votre appareil mobile, il est conseillé d'utiliser des mots de passe forts et uniques. L'authentification à deux facteurs peut également ajouter une couche de sécurité supplémentaire, rendant plus difficile l'accès non autorisé à vos comptes.

Prudence avec les permissions des applications

Soyez vigilant quant aux permissions que vous accordez aux applications. Certaines applications peuvent demander l'accès à des données sensibles, comme vos contacts ou votre localisation. Assurez-vous que ces demandes sont légitimes et nécessaires pour le fonctionnement de l'application.

Précautions à prendre avec l'Assistant Google et le microphone sur mobile

L'utilisation de l'Assistant Google et du microphone sur les appareils mobiles offre de nombreux avantages en termes de commodité et d'accessibilité. Cependant, ces technologies soulèvent également des questions de confidentialité et de sécurité. Voici quelques points essentiels à surveiller :

1. Accès au microphone

Gestion des permissions

- **Vérifiez les permissions** : Assurez-vous que seules les applications de confiance ont accès au microphone. Sur Android et iOS, vous pouvez vérifier et modifier les permissions d'accès au microphone dans les paramètres de l'appareil.
- **Désactivez l'accès inutile** : Si une application n'a pas besoin d'accéder au microphone pour fonctionner correctement, il est préférable de lui retirer cette permission.

Surveillance de l'activité

- **Indicateurs visuels** : Surveillez les indicateurs visuels qui montrent lorsque le microphone est actif. Certaines interfaces utilisateur affichent une icône de microphone en haut de l'écran lorsque celui-ci est en cours d'utilisation.

2. Utilisation de l'Assistant Google

Contrôle des données partagées

- **Réviser l'historique des interactions** : Dans les paramètres de l'Assistant Google, vous pouvez examiner et supprimer l'historique de vos interactions vocales. Cela peut aider à limiter la quantité de données stockées.
- **Paramètres de confidentialité** : Configurez les paramètres de confidentialité de l'Assistant Google pour limiter le partage et l'utilisation des données collectées. Vous pouvez désactiver certaines fonctionnalités de personnalisation pour réduire le profilage basé sur vos données.

Sensibilité à l'activation

- **Ajustez la sensibilité à l'activation** : Réduisez les déclenchements accidentels de l'Assistant Google en ajustant la sensibilité de l'option "Ok Google" dans les paramètres de l'Assistant.

3. Sécurité des données audio

Revue régulière

- **Check up de sécurité** : Faites des check up réguliers de la sécurité de votre appareil pour identifier et corriger les vulnérabilités potentielles liées à l'utilisation du microphone et de l'Assistant Google.

4. Sensibilisation à l'environnement

Attention aux environnements sensibles

- **Prudence dans les lieux publics** : Soyez conscient de votre environnement lorsque vous utilisez l'Assistant Google ou le microphone. Évitez de divulguer des informations sensibles vocalement lorsque vous êtes dans des lieux publics ou potentiellement non sécurisés.

Une gestion prudente des permissions, une configuration adéquate de la confidentialité et une sensibilisation aux risques environnementaux sont essentielles pour sécuriser vos interactions vocales sur les appareils mobiles.

Temu et Shein

Ces plateformes présentent des dangers à la fois sur le plan physique, en raison des produits qu'elles vendent, et sur le plan numérique, concernant la sécurité des données personnelles.

Risques Physiques des Produits

Produits Non Conformes aux Normes de Sécurité

Conformité insuffisante : Selon des enquêtes menées par des associations de consommateurs comme Test Achats, près de 70% des produits vendus sur Temu et Shein ne respectent pas les normes de sécurité européennes. Cela signifie que ces produits peuvent poser des risques graves pour la santé et la sécurité des consommateurs.

- **Appareils électriques** : Parmi les 54 chargeurs USB testés, la plupart étaient non conformes, présentant des risques de surchauffe, d'électrocution, ou même d'incendie. Ces appareils peuvent être dangereux à utiliser, en particulier dans des environnements domestiques où la sécurité est primordiale.

- **Jouets pour enfants** : De nombreux jouets contiennent des petites pièces qui peuvent se détacher facilement, posant un risque d'étouffement pour les jeunes enfants. De plus, ces jouets ne respectent souvent aucune norme de sécurité, ce qui les rend particulièrement dangereux.
- **Substances toxiques** : Des tests ont révélé que certains vêtements et accessoires contiennent des niveaux de produits chimiques dangereux, tels que les phtalates, le plomb et le cadmium, qui dépassent jusqu'à 600 fois les limites légales. Ces substances peuvent avoir des effets néfastes sur la santé, notamment des irritations cutanées ou des problèmes plus graves à long terme.

Risques Numériques liés à l'Application

Collecte Excessive de Données Personnelles

Accès aux données : Temu, en particulier, est critiquée pour ses demandes d'accès excessives à vos informations personnelles, telles que vos contacts, votre localisation et votre historique de navigation. Cette collecte massive de données peut être utilisée à des fins de marketing agressif ou, pire encore, tomber entre les mains de cybercriminels.

Conséquences Financières et Comportementales

Mécanismes de consommation impulsive : Le modèle économique de ces applications repose souvent sur la gamification, incitant les utilisateurs à effectuer des achats impulsifs. Ce comportement peut entraîner des problèmes de gestion budgétaire, car les consommateurs peuvent être amenés à dépenser plus qu'ils ne le souhaitent ou ne le peuvent.

Recommandations pour Limiter les Risques

Précautions à Prendre avec les Produits

- **Évitez les produits sensibles** : Il est fortement déconseillé d'acheter des chargeurs, des produits de beauté (tels que le maquillage), des jouets pour jeunes enfants ou des bijoux bon marché qui touchent la peau. Ces articles présentent un risque accru en raison de leur non-conformité aux normes de sécurité.
- **Lavez les vêtements avant utilisation** : Avant de porter un vêtement acheté sur ces plateformes, lavez-le impérativement pour éliminer un maximum de résidus chimiques potentiellement dangereux.

Sécurisation de l'Application

- **Limitez les accès de l'application** : Ne donnez pas à l'application l'accès à vos contacts, votre micro ou d'autres informations sensibles. Privilégiez les paiements via des services tiers sécurisés, tels que PayPal ou des cartes virtuelles, pour protéger vos informations financières.

Mise en Garde et Actions Réglementaires

Enquêtes de l'Union Européenne : L'Union Européenne a ouvert des enquêtes pour forcer Temu et Shein à respecter les règles de sécurité et de protection des consommateurs. Ces actions visent à garantir que les produits vendus respectent les normes de sécurité et que les pratiques de collecte de données soient conformes aux réglementations en vigueur.

CHAPITRE 6

QUIZZ

N°	Question	Options
1	Qu'est-ce qu'une "porte d'entrée" en sécurité informatique ?	A) Un point faible par lequel les attaquants peuvent pénétrer dans un système. B) Un sas de sécurité physique dans un data center. C) Un protocole qui permet l'accès sécurisé à un réseau.
2	À quoi sert un antivirus ?	A) À gérer les mises à jour des applications. B) À nettoyer et à accélérer l'ordinateur. C) À détecter et à supprimer les logiciels malveillants.
3	Qu'est-ce qu'un mot de passe complexe et fort ?	A) Un mot de passe avec une signification personnelle. B) Un mot de passe qui inclut une variété de caractères et est difficile à deviner. C) Un mot de passe qui est utilisé pour plusieurs comptes.
4	Est-il utile d'avoir plusieurs mots de passe et de les changer régulièrement ?	A) Il est recommandé de ne jamais changer de mot de passe pour éviter de les oublier. B) Non, il est plus pratique d'utiliser le même mot de passe partout. C) Oui, cela réduit le risque de compromission de plusieurs comptes.
5	Pourquoi est-il important de mettre à jour ses logiciels ?	A) Les mises à jour sont principalement esthétiques. B) Les mises à jour ajoutent souvent de nouvelles fonctionnalités utiles. C) Les mises à jour corrigent les failles de sécurité et protègent contre les nouvelles menaces.
6	Qu'est-ce que la maintenance informatique et de données ?	A) La mise à jour des sites web et des contenus en ligne. B) L'organisation et la sauvegarde régulières des données. C) Le remplacement périodique des composants matériels.
7	Qu'est-ce qu'un malware ?	A) Un outil de maintenance système. B) Un logiciel conçu pour protéger contre les virus. C) Un logiciel malveillant destiné à endommager ou à exploiter des systèmes.
8	Qu'est-ce qu'un ver informatique ?	A) Un type de logiciel antivirus. B) Un outil de diagnostic réseau. C) Un programme qui se duplique lui-même pour se propager à d'autres ordinateurs.
9	Qu'est-ce qu'une authentification à deux facteurs (2FA) ?	A) Une nouvelle technologie qui double la force de cryptage. B) Un système qui demande deux formes d'identification avant d'accorder l'accès. C) Une méthode qui nécessite deux mots de passe différents.

N°	Question	Options
10	Qu'est-ce qu'un virus informatique ?	A) Un logiciel utilisé pour nettoyer l'ordinateur. B) Un type de malware qui s'attache à des fichiers et se propage à d'autres systèmes. C) Un programme qui aide à maintenir la santé du système.
11	Qu'est-ce qu'un cheval de Troie ?	A) Un jeu vidéo populaire sur les stratégies de guerre. B) Un outil utilisé pour renforcer la sécurité d'un réseau. C) Un programme qui semble légitime mais qui contient un code malveillant.
12	Qu'est-ce que le phishing ?	A) Une méthode pour sécuriser les communications par email. B) Une technique de pêche numérique. C) Une tentative d'obtenir des informations sensibles en se faisant passer pour une entité de confiance.
13	Qu'est-ce qu'un spyware ?	A) Un outil de surveillance pour les parents. B) Un programme qui aide à espionner les concurrents. C) Un logiciel qui collecte des informations sur un utilisateur sans son consentement.
14	Que signifie chiffrer et déchiffrer des données ?	A) Compresser et décompresser des fichiers pour économiser de l'espace. B) Organiser et désorganiser des informations. C) Convertir des données en un format sécurisé pour la transmission et les reconvertir en format original.
15	Qu'est-ce que l'authentification à deux facteurs (2FA) ?	A) Une méthode qui utilise deux mots de passe différents. B) Un système qui demande deux formes d'identification avant d'accorder l'accès. C) Une nouvelle technologie qui double la force de cryptage.
16	Qu'est-ce qu'un gestionnaire de mots de passe ? Qu'est-ce qu'un générateur de mot de passe ?	A) Un gestionnaire enregistre les mots de passe oubliés, et un générateur aide à les récupérer. B) Un gestionnaire aide à stocker de manière sécurisée les mots de passe, tandis qu'un générateur en crée de nouveaux et complexes. C) Un gestionnaire surveille la force des mots de passe existants, et un générateur envoie des rappels de changement.

6.1 Réponse

Réponses du quizz

N°	Réponse
1	A) Un point faible par lequel les attaquants peuvent pénétrer dans un système.

N°	Réponse
2	C) À détecter et à supprimer les logiciels malveillants.
3	B) Un mot de passe qui inclut une variété de caractères et est difficile à deviner.
4	C) Oui, cela réduit le risque de compromission de plusieurs comptes.
5	C) Les mises à jour corrigent les failles de sécurité et protègent contre les nouvelles menaces.
6	B) L'organisation et la sauvegarde régulières des données.
7	C) Un logiciel malveillant destiné à endommager ou à exploiter des systèmes.
8	C) Un programme qui se duplique lui-même pour se propager à d'autres ordinateurs.
9	B) Un système qui demande deux formes d'identification avant d'accorder l'accès.
10	B) Un type de malware qui s'attache à des fichiers et se propage à d'autres systèmes.
11	C) Un programme qui semble légitime mais qui contient un code malveillant.
12	C) Une tentative d'obtenir des informations sensibles en se faisant passer pour une entité de confiance.
13	C) Un logiciel qui collecte des informations sur un utilisateur sans son consentement.
14	C) Convertir des données en un format sécurisé pour la transmission et les reconvertir en format original.
15	B) Un système qui demande deux formes d'identification avant d'accorder l'accès.
16	B) Un gestionnaire aide à stocker de manière sécurisée les mots de passe, tandis qu'un générateur en crée de nouveaux et complexes.