

Parcours : DISCOVERY

Module : Naviguer en toute Sécurité

Projet 1 - Un peu plus de sécurité, on n'en a jamais assez !

1 - Introduction à la sécurité sur Internet

1/ Trois articles qui parlent de sécurité sur internet :

- Article 1 = [phonandroid](#) - **Restez anonyme et surfez en sécurité sur Internet grâce à un VPN**
- Article 2 = [cybermalveillance.gouv](#) - **Comment sécuriser ses achats sur Internet ?**
- Article 3 = [L'usine Digitale](#) - Microsoft lance un "copilote" pour la cybersécurité à base d'intelligence artificielle générative

2 - Créer des mots de passe forts

C'est fait.

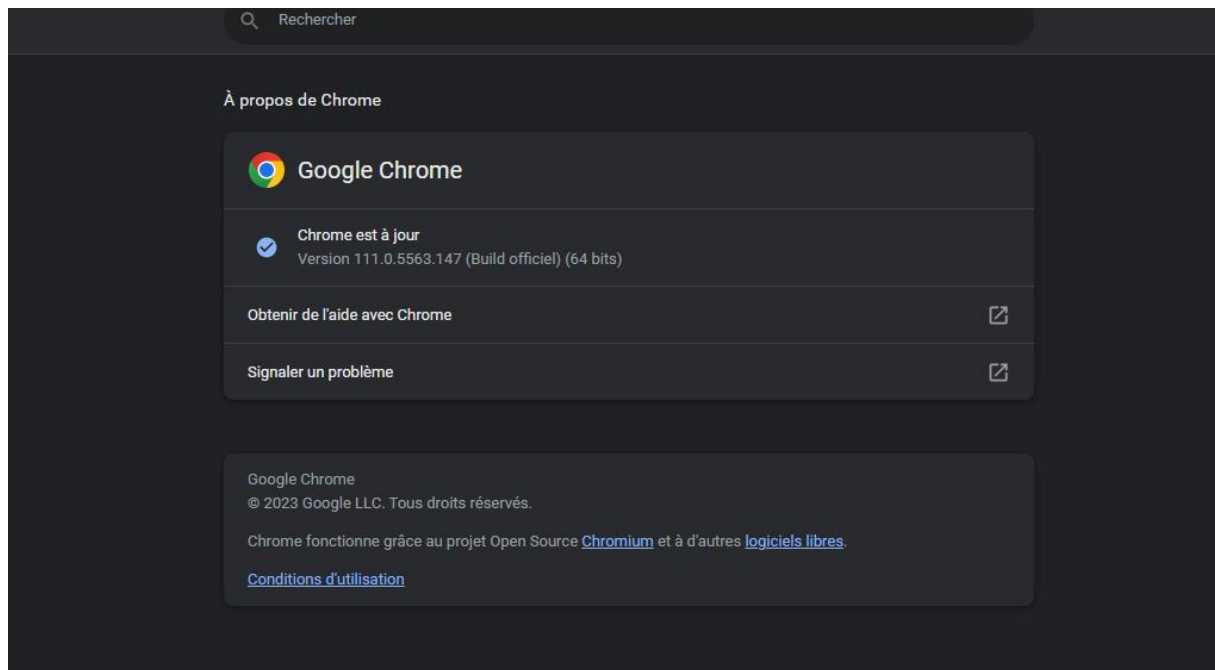
3 - Fonctionnalité de sécurité de votre navigateur

1/ Identifie les adresses internet qui te semblent provenir de sites web malveillants.

- [www.morvel.com](#) - malveillant
- [www.dccomics.com](#) - legit
- [www.ironman.com](#) - legit
- [www.fessebook.com](#) -malveillant
- [www.instagam.com](#) – malveillant

Les sites [www.morvel.com](#) ; [www.fessebook.com](#) ; [www.instagam.com](#) semblent malveillants car ils présentent des copies mal orthographiées des sites officiels : [www.marvel.com](#) ; [www.facebook.com](#) ; [www.instagram.com](#)

2/ Vérifier si mon navigateur est à jour :



Effectivement , j'utilise Chrome et il est à jour.

4 - Éviter le spam et le phishing



5 - Comment éviter les logiciels malveillants

● Site n°1

○ Indicateur de sécurité :

■ HTTPS

o Analyse Google :

■ Aucun contenu suspect

● Site n°2

o Indicateur de sécurité :

■ Not secure

o Analyse Google :

■ Aucun contenu suspect

● Site n°3

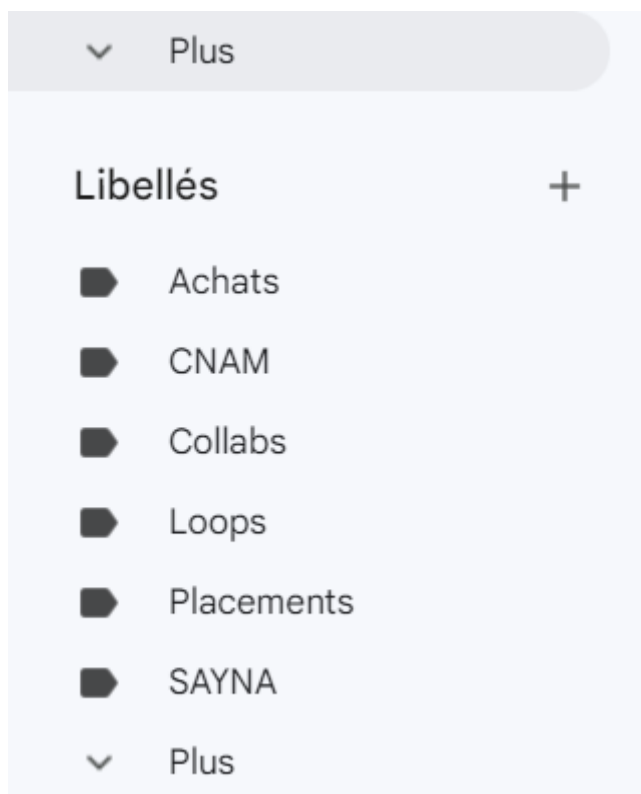
o Indicateur de sécurité :

■ Not secure

o Analyse Google :


■ Vérifier un URL en particulier

6 - Achats en ligne sécurisés



8 - Principes de base de la confidentialité des médias sociaux

● Confidentialité

Votre activité	Qui peut voir vos futures publications ?	Public	Modifier
	Examinez toutes les publications et tous les contenus dans lesquels vous êtes identifié(e)	Utiliser l'historique d'activité	
	Limiter l'audience des publications que vous avez ouvertes aux amis de vos amis ou au public ?	Limiter l'audience des anciennes publications	
	Qui peut voir les personnes, Pages et listes que vous suivez ?	Moi uniquement	Modifier
Comment les autres peuvent vous trouver et vous contacter	Qui peut vous envoyer des invitations ?	Tout le monde	Modifier
	Qui peut voir votre liste d'amis ? <small>Rappel : vos amis peuvent paramétrer qui peut voir avec qui ils sont amis sur leur propre journal. Si des personnes peuvent voir ces informations sur un autre journal, elles le peuvent également sur le Fil, la recherche et ailleurs sur Facebook. Si vous définissez ce paramètre sur Moi uniquement, nul autre que vous ne pourra voir votre liste d'amis sur votre journal. Les autres personnes ne verront que vos amis communs.</small>	Moi uniquement	Modifier
	Qui peut vous trouver à l'aide de l'adresse e-mail que vous avez fournie ?	Moi uniquement	Modifier
	Qui peut vous trouver à l'aide du numéro de téléphone que vous avez fourni ? Ceci concerne les personnes qui ne peuvent pas voir votre numéro de téléphone sur votre profil. <div>  Moi uniquement ▼ </div>	Fermer	
	Voulez-vous que les moteurs de recherche en dehors de Facebook affichent un lien vers votre profil ?	Oui	Modifier

● Publications publiques

Filtres et outils des publications publiques

Qui peut me suivre

Vos followers voient vos publications, reels, stories et mini-audios dans le Fil. Vos amis suivent vos publications, reels, stories et mini-audios par défaut, mais vous pouvez aussi autoriser quiconque ne faisant pas partie de vos amis à suivre vos publications, reels, stories et mini-audios publics. Utilisez ce paramètre pour choisir qui peut vous suivre.

Chaque fois que vous créez ou publiez un reel, une story ou un mini-audio, vous choisissez l'audience avec qui vous voulez les partager.

Ce paramètre ne s'applique pas aux personnes qui vous suivent sur Marketplace et dans les groupes d'achat et de vente. Vous pouvez gérer ces paramètres sur Marketplace.

[En savoir plus](#)

Publique

Commentaires des publications publiques

Choose who is allowed to comment on your public posts. People tagged in your public posts and their friends may still be able to comment. [En savoir plus](#)

Vous pouvez mettre à jour cette option sur chaque publication sans affecter les paramètres de votre compte.

Amis

Notifications de publications publiques

Vous pouvez recevoir des notifications lorsque des personnes qui ne font pas partie de vos amis commencent à vous suivre et partagent, aiment ou commentent vos publications publiques.

Amis et leurs amis

Informations de profil publiques

Gérez qui peut aimer ou commenter vos informations de profil qui sont toujours publiques, y compris vos photos de profil, vidéos de profil, photos de couverture, photos à la une et les mises à jour de votre courte bio.

Amis

9 - Que faire si votre ordinateur est infecté par un virus

1 / Test de vulnérabilité de l'ordinateur portable

1. Installer un logiciel antivirus et un pare-feu sur votre ordinateur portable.
2. Utiliser un outil de numérisation de vulnérabilité pour trouver les vulnérabilités connues de votre système d'exploitation et des logiciels installés.
3. Essayer d'ouvrir une pièce jointe suspecte dans un e-mail ou de télécharger un fichier d'un site web non fiable. Si le logiciel antivirus ne détecte pas la menace, l'ordinateur est vulnérable à une attaque de phishing ou de malware.

4. Essayer de se connecter à des réseaux Wi-Fi publics non sécurisés. Si on peut nous connecter sans entrer de mot de passe, l'ordinateur est vulnérable à une attaque de l'homme du milieu.
5. Essayer d'installer des logiciels malveillants à partir d'un site Web de téléchargement non fiable. Si le pare-feu n'avertit pas, l'ordinateur est vulnérable à une attaque d'installation de logiciels malveillants.

2 / Installation et utilisation d'un antivirus + antimalware sur un ordinateur Windows

Télécharger un logiciel antivirus et antimalware gratuit, tel que Avast Free Antivirus ou Malwarebytes Anti-Malware.

Ouvrir le fichier d'installation téléchargé et suivre les instructions pour installer le logiciel.

Une fois l'installation terminée, exécuter une analyse complète du système pour détecter tout virus, malware ou programme potentiellement indésirable (PUP).

Si des menaces sont détectées, suivez les instructions de suppression fournies par le logiciel antivirus et antimalware pour nettoyer votre système.

Configurer le logiciel pour qu'il s'exécute en arrière-plan en continu, pour que toutes les futures menaces soient détectées et supprimées rapidement.

Planifier des analyses régulières pour vous assurer que votre système est toujours protégé contre les menaces les plus récentes.

Assurez-vous que le logiciel est régulièrement mis à jour pour bénéficier des dernières fonctionnalités de sécurité et des définitions de virus les plus récentes.

Si on rencontre des problèmes avec le logiciel, contacter le support technique pour obtenir de l'aide.

Il est important de noter que l'installation et l'utilisation d'un logiciel antivirus et antimalware ne suffisent pas à garantir une protection complète contre toutes les menaces de sécurité. Il est également recommandé d'adopter de bonnes pratiques de sécurité, telles que la mise à jour régulière de vos logiciels, la configuration de mots de passe forts et uniques, et l'utilisation d'un pare-feu pour bloquer les attaques réseau.