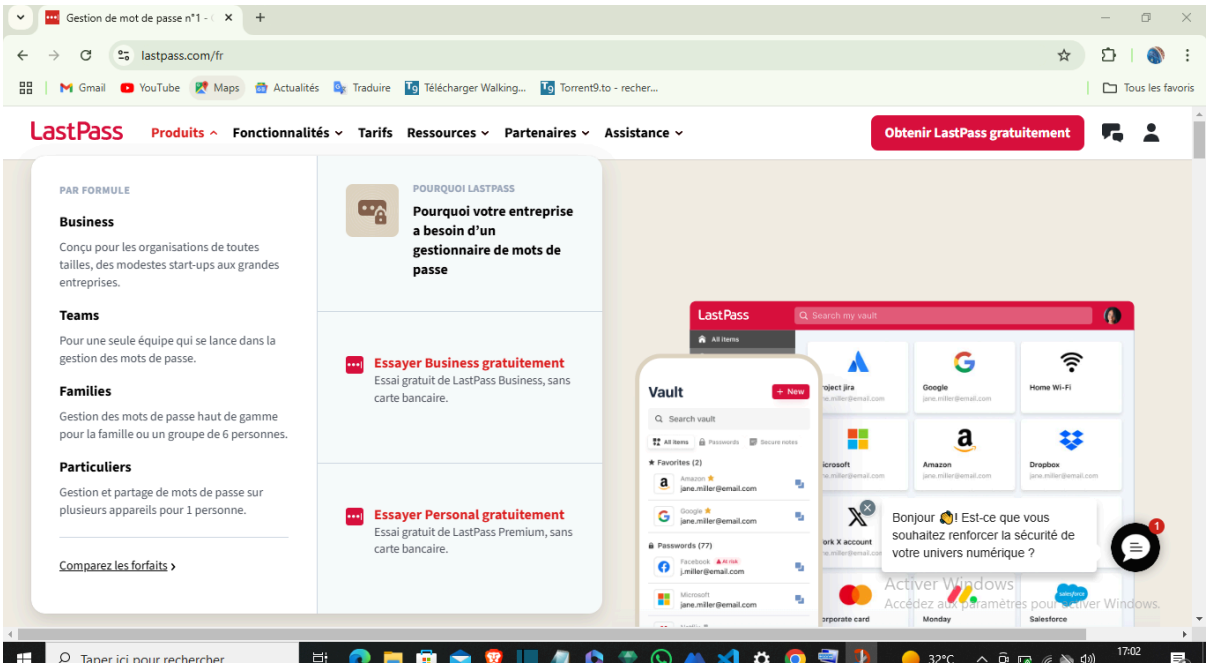
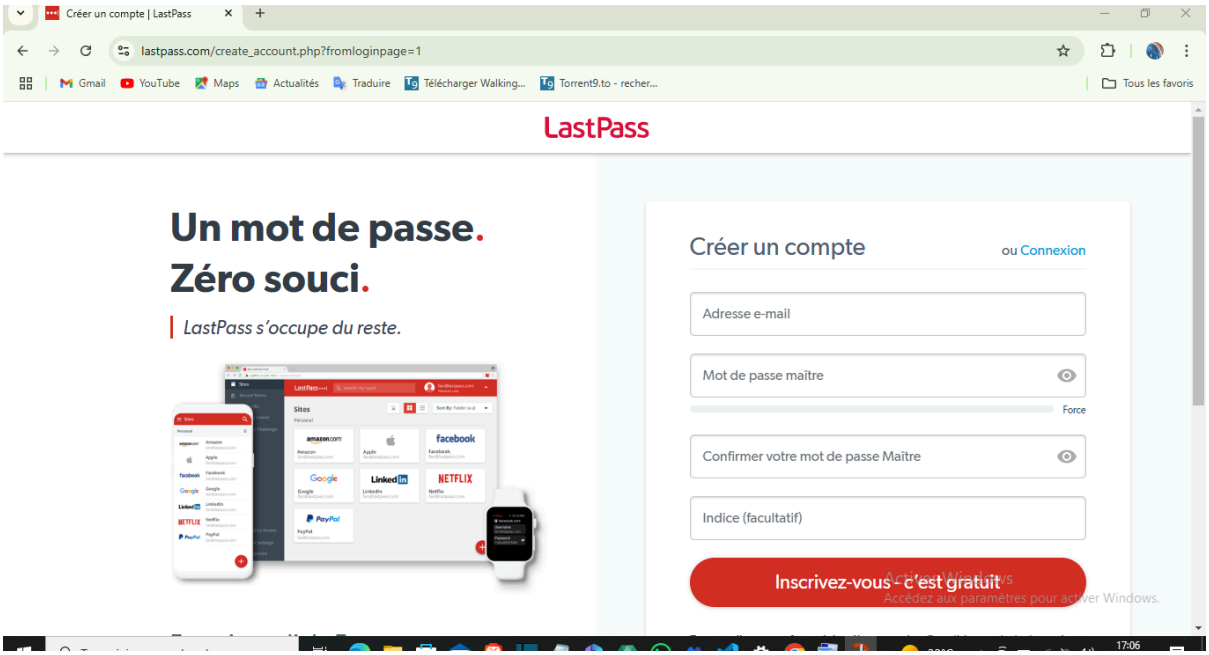
Parcours : DISCOVERY
Module : Naviguer en toute sécurité
Projet 1 : Un peu plus de sécurité sur internet

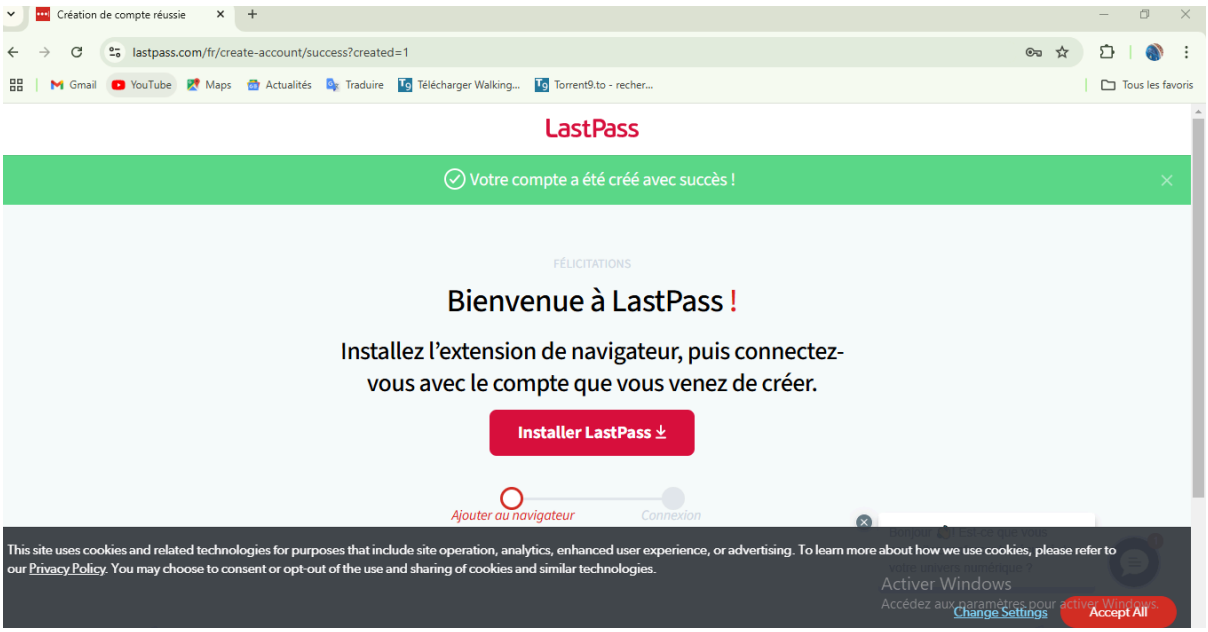
1-Introduction à la sécurité internet

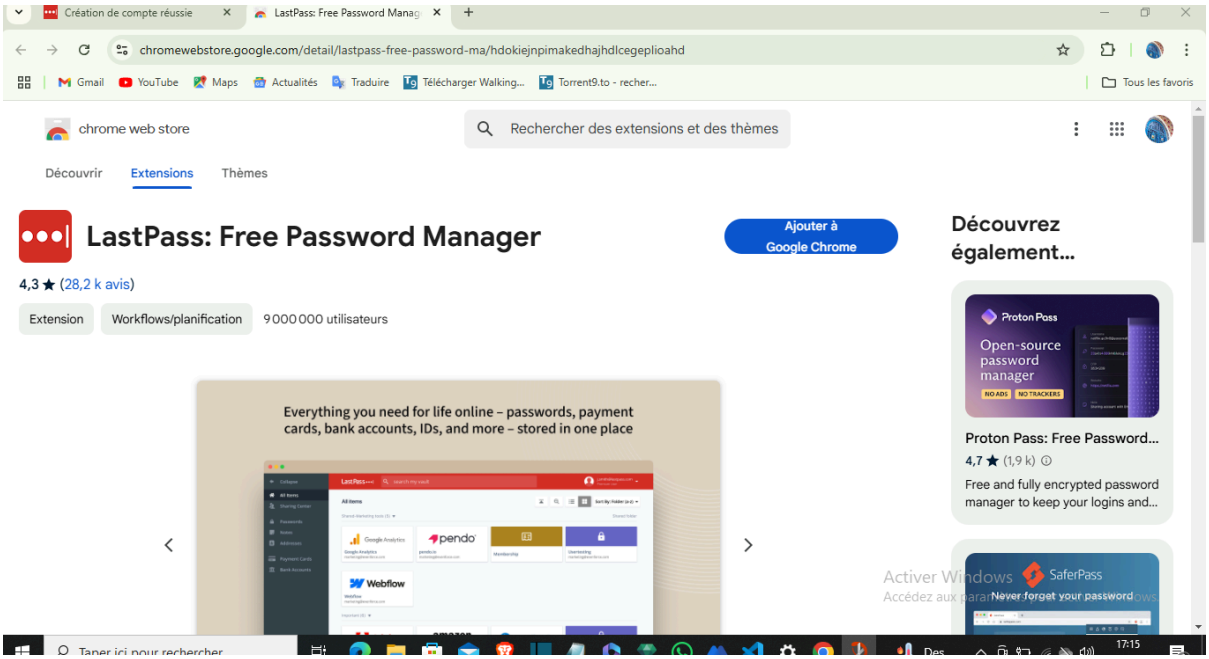
1- Article 1 Nom du site : https://www.cybermalveillance.gouv.fr/ ; Nom de l'article: Les 10 règles de base pour la sécurité numérique
Article 2 Nom du site : https://www.fortinet.com/; Nom de l'article : Qu'est-ce que la sécurité internet ?
Article 3 Nom du site : https://www.isagri.fr/ ; Nom de l'article : 11 règles pour naviguer sur Internet en sécurité

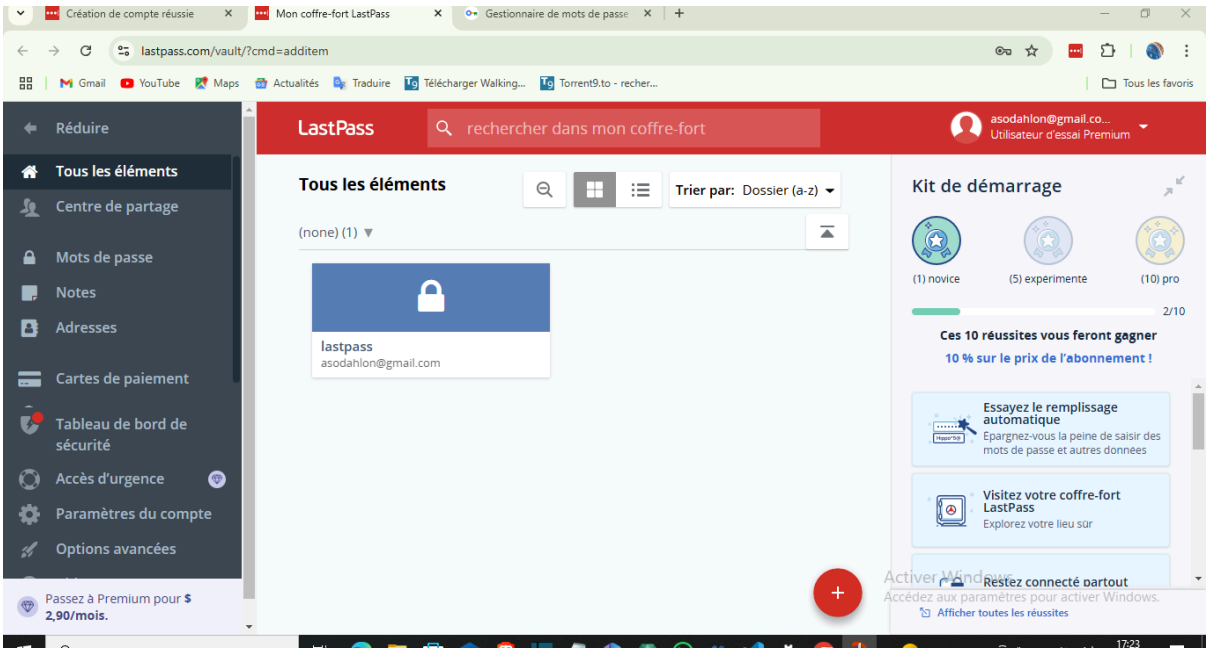
2- Créer des mots de passe forts




Créer un compte | LastPass
lastpass.com/create_account.php?fromloginpage=1
Gmail
YouTube
Maps
Actualités
Traduire
Télécharger Walking...
Torrent9.to - recher...
Tous les favoris
LastPass
Un mot de passe.
Zéro souci.
LastPass s'occupe du reste.
Créer un compte
ou Connexion
Adresse e-mail
Mot de passe maître
Force
Confirmer votre mot de passe Maître
Indice (facultatif)
Inscrivez-vous - c'est gratuit
Accédez aux paramètres pour activer Windows.


Création de compte réussie
lastpass.com/fr/create-account/success?created=1
Gmail
YouTube
Maps
Actualités
Traduire
Télécharger Walking...
Torrent9.to - recher...
Tous les favoris
LastPass
Votre compte a été créé avec succès !
FÉLICITATIONS
Bienvenue à LastPass !
Installez l'extension de navigateur, puis connectez-vous avec le compte que vous venez de créer.
Installer LastPass
Ajouter au navigateur
Connexion
This site uses cookies and related technologies for purposes that include site operation, analytics, enhanced user experience, or advertising. To learn more about how we use cookies, please refer to our Privacy Policy. You may choose to consent or opt-out of the use and sharing of cookies and similar technologies.
Change Settings
Accept All
Activer Windows
Accédez aux paramètres pour activer Windows.





3- Fonctionnalité de sécurité du navigateur

1- Les sites web qui semblent être malveillants sont :

● www.morvel.com, un dérivé de www.marvel.com, le site web officiel de l'univers Marvel

● www.fessebook.com, un dérivé de www.facebook.com, le plus grand réseau social du monde

● www.instagam.com, un dérivé de www.instagram.com, un autre réseau social très utilisé

Les seuls sites qui semblaient être cohérents sont donc :

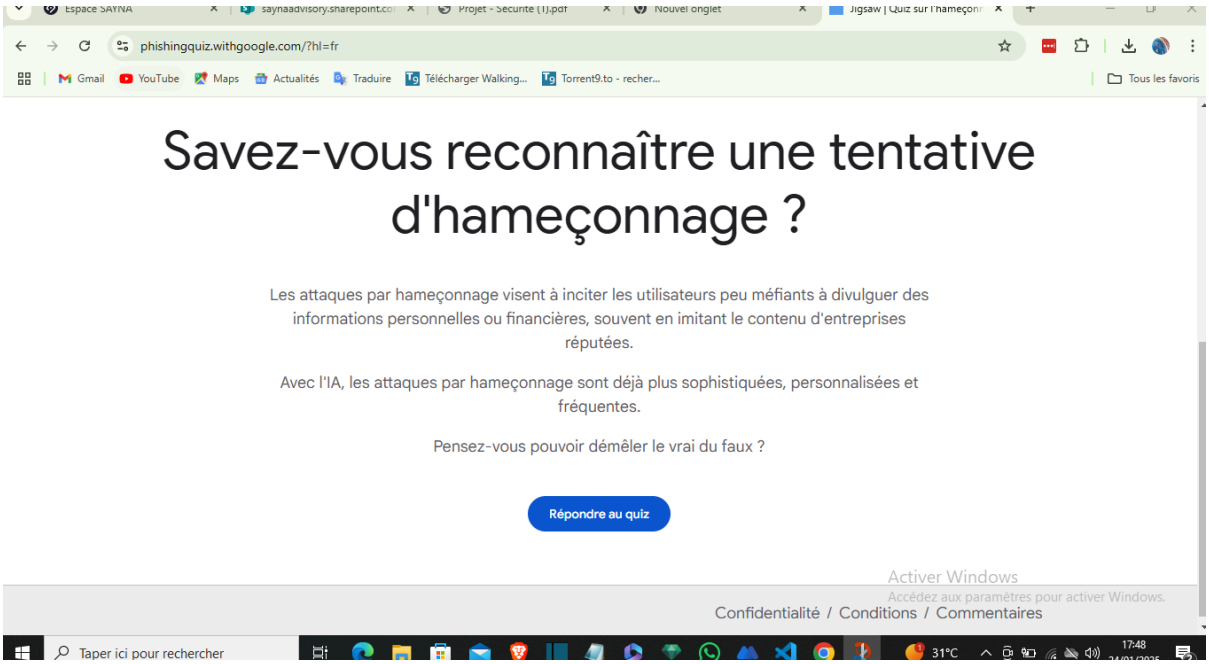
● www.dccomics.com, le site officiel de l'univers DC Comics

● www.ironman.com, le site officiel d'une compétition internationale de triathlon (et non du super-héros issu de l'univers Marvel)

2/

4 - Éviter le spam et le phishing Objectif : Reconnaître plus facilement les messages frauduleux

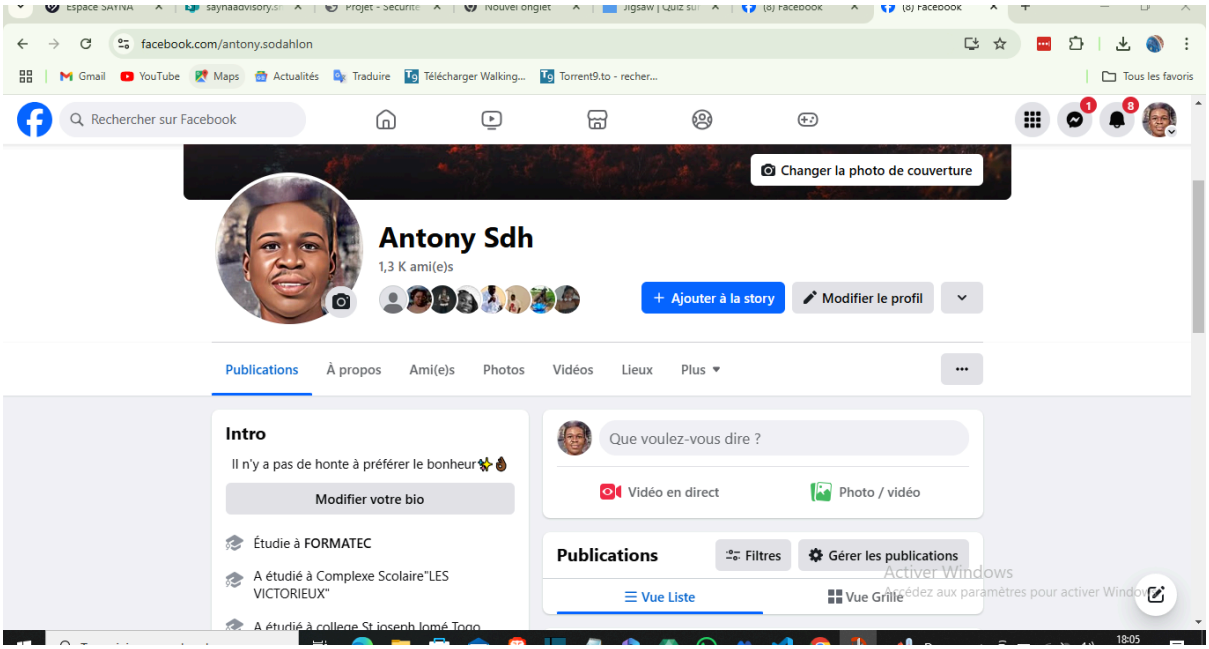
1/

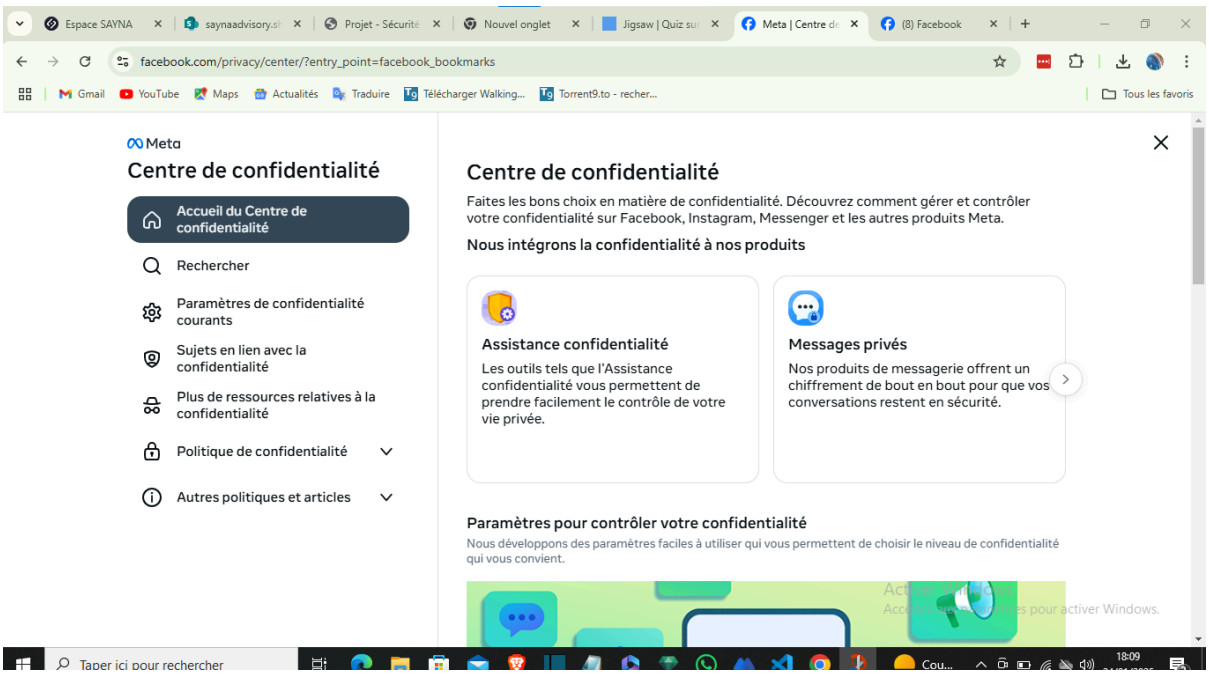


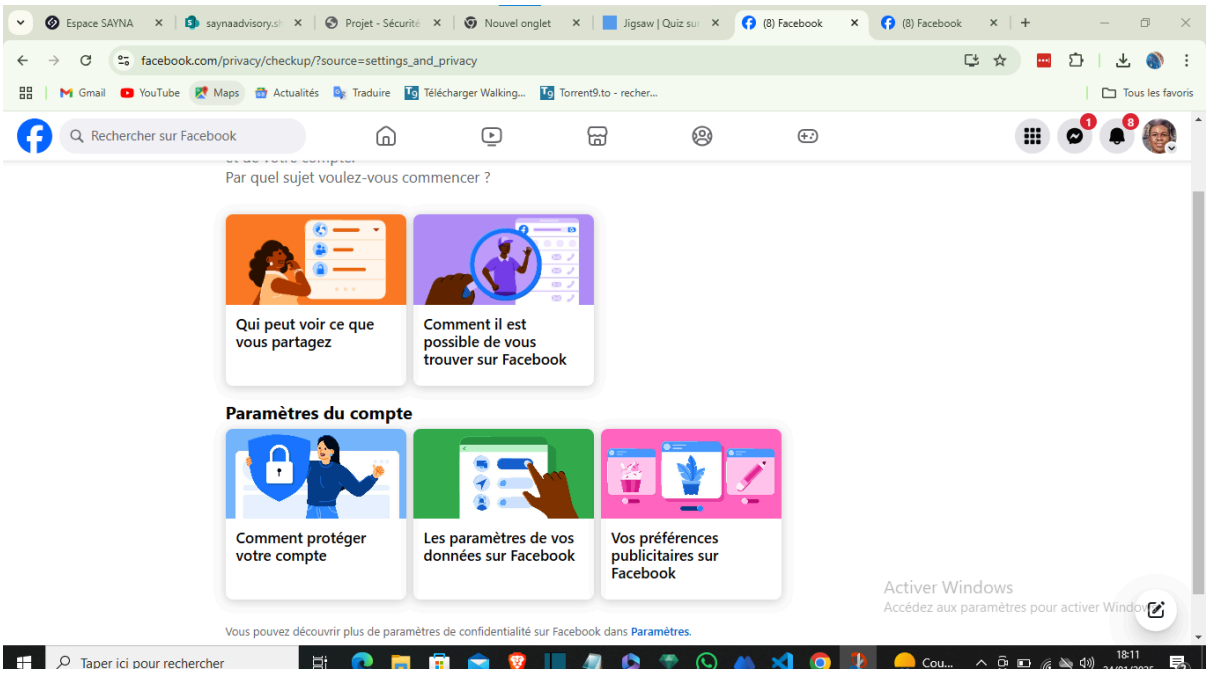
5 - Comment éviter les logiciels malveillants
sécuriser L'ordinateur et identifier les liens suspects

● Site n°1
○ Indicateur de sécurité ■ HTTPS
○ Analyse Google
■ Aucun contenu suspect ●
Site n°2
○ Indicateur de sécurité
■ Not secure ○
Analyse Google
■ Aucun contenu suspect
● Site n°3
○ Indicateur de sécurité
■ Not secure
○ Analyse Google
■ Vérifier un URL en particulier (analyse trop générale)

8 - Principes de base de la confidentialité des médias sociaux


facebook.com/antony.sodahlon
Rechercher sur Facebook
Changer la photo de couverture
Antony Sdh
1,3 K ami(e)s
Ajouter à la story
Modifier le profil
Publications
À propos
Ami(e)s
Photos
Vidéos
Lieux
Plus
Intro
Il n'y a pas de honte à préférer le bonheur
Modifier votre bio
Étudie à FORMATEC
A étudié à Complexe Scolaire"LES VICTORIEUX"
Que voulez-vous dire ?
Vidéo en direct
Photo / vidéo
Publications
Filtres
Gérer les publications
Vue Liste
Vue Grille


facebook.com/privacy/center/?entry_point=facebook_bookmarks
Meta
Centre de confidentialité
Accueil du Centre de confidentialité
Rechercher
Paramètres de confidentialité courants
Sujets en lien avec la confidentialité
Plus de ressources relatives à la confidentialité
Politique de confidentialité
Autres politiques et articles
Centre de confidentialité
Faites les bons choix en matière de confidentialité. Découvrez comment gérer et contrôler votre confidentialité sur Facebook, Instagram, Messenger et les autres produits Meta.
Nous intégrons la confidentialité à nos produits
Assistance confidentialité
Les outils tels que l'Assistance confidentialité vous permettent de prendre facilement le contrôle de votre vie privée.
Messages privés
Nos produits de messagerie offrent un chiffrement de bout en bout pour que vos conversations restent en sécurité.
Paramètres pour contrôler votre confidentialité
Nous développons des paramètres faciles à utiliser qui vous permettent de choisir le niveau de confidentialité qui vous convient.



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

Exercice 1 : Vérification de la sécurité des connexions Internet
But : S'assurer que les appareils sont connectés de manière sécurisée à Internet.
Méthode :
1. Vérifie que les réseaux Wi-Fi utilisés sont protégés par un mot de passe.
2. Assure-toi que l'option "Connexion automatique" aux réseaux publics est désactivée.
3. Teste la fonctionnalité VPN (réseau privé virtuel) et assure-toi qu'elle fonctionne correctement.
4. Confirme que les sites web visités utilisent HTTPS.

Exercice 2 : Mise à jour des logiciels et applications
But : S'assurer que tous les logiciels et applications sont à jour pour éviter les vulnérabilités.
Méthode :
1. Vérifie les mises à jour du système d'exploitation (Windows, macOS, iOS, Android, etc.).
2. Assure-toi que toutes les applications installées sont à jour.
3. Active les mises à jour automatiques pour les applications et le système d'exploitation.

Exercice 3 : Sécurité des mots de passe
But : S'assurer que les utilisateurs utilisent des mots de passe forts et sécurisés.
Méthode :
1. Utilise un gestionnaire de mots de passe pour générer et stocker des mots de passe sécurisés.
2. Vérifie que les mots de passe sont composés d'au moins 12 caractères, incluant des lettres majuscules, des lettres minuscules, des chiffres et des symboles spéciaux.
3. Assure-toi que l'authentification à deux facteurs (2FA) est activée pour les comptes importants.

Exercice 4 : Sécurité des données personnelles
But : S'assurer que les données personnelles sont protégées sur les appareils.
Méthode :
1. Vérifie que le chiffrement du disque dur ou de l'appareil est activé (BitLocker pour Windows, FileVault pour macOS).
2. Assure-toi que les sauvegardes de données sont chiffrées et stockées de manière sécurisée.
3. Limite les permissions des applications pour accéder aux données personnelles (contacts, photos, localisation, etc.).

Exercice 5 : Protection contre les logiciels malveillants
But : S'assurer que les appareils sont protégés contre les virus et les logiciels malveillants.
Méthode :
1. Installe et mets à jour régulièrement un logiciel antivirus.
2. Effectue des analyses régulières de l'appareil pour détecter les menaces potentielles.
3. Sensibilise les utilisateurs à ne pas télécharger et installer des applications de sources non fiables.

2-

Exercice pour Installer et Utiliser un Antivirus et un Antimalware

Objectif :
Assurer que tous les appareils (PC, téléphone, etc.) soient protégés contre les virus et logiciels malveillants.

Matériel nécessaire :
- Ordinateur (PC ou Mac)
- Téléphone (Android ou iOS)
- Connexion Internet
- Logiciel antivirus et antimalware (ex : Avast, Norton, Malwarebytes, etc.)

Étapes pour PC :

1. **Téléchargement et Installation :**
   - Visitez le site officiel de votre logiciel antivirus/antimalware.
   - Téléchargez le fichier d'installation pour votre système d'exploitation.
   - Exécutez le fichier téléchargé et suivez les instructions à l'écran pour installer le logiciel.

2. **Mise à jour et Analyse Initiale :**
   - Ouvrez le logiciel installé.
   - Assurez-vous qu'il est mis à jour avec les dernières définitions de virus.
   - Lancez une analyse complète du système pour détecter et supprimer les menaces potentielles.

3. **Planification des Analyses :**

- Configurez le logiciel pour effectuer des analyses automatiques régulières (quotidiennes ou hebdomadaires).
- Vérifiez que les mises à jour automatiques des définitions de virus sont activées.

4. **Sensibilisation à la Sécurité :**
- Évitez de télécharger des fichiers de sources inconnues.
- Ne cliquez pas sur les liens suspects dans les emails ou les messages instantanés.

Étapes pour Téléphone (Android et iOS) :

1. **Téléchargement et Installation :**
- Accédez à l'App Store (iOS) ou au Google Play Store (Android).
- Recherchez un logiciel antivirus/antimalware fiable.
- Téléchargez et installez l'application.

2. **Mise à jour et Analyse Initiale :**
- Ouvrez l'application installée.
- Assurez-vous qu'elle est mise à jour avec les dernières définitions de virus.
- Lancez une analyse complète de l'appareil pour détecter et supprimer les menaces potentielles.

3. **Planification des Analyses :**
- Configurez l'application pour effectuer des analyses automatiques régulières.
- Vérifiez que les mises à jour automatiques des définitions de virus sont activées.

4. **Sensibilisation à la Sécurité :**
- Évitez de télécharger des applications de sources non vérifiées.
- Ne cliquez pas sur les liens suspects dans les SMS ou les messages instantanés.