Projet 3

1/introduction à la securité sur l'internet

1/en navigant sur le web ;consulte trois article qui parlent de securité sur l'internet pense à verifier la source des information et essaie de condulter des article recents pour que les information soient à jour saisir le nom du site et de l'article

Article 1 :ANSE Dix regle de bases

Aticle2 : economie gouv-comment assurer votre securité numerique

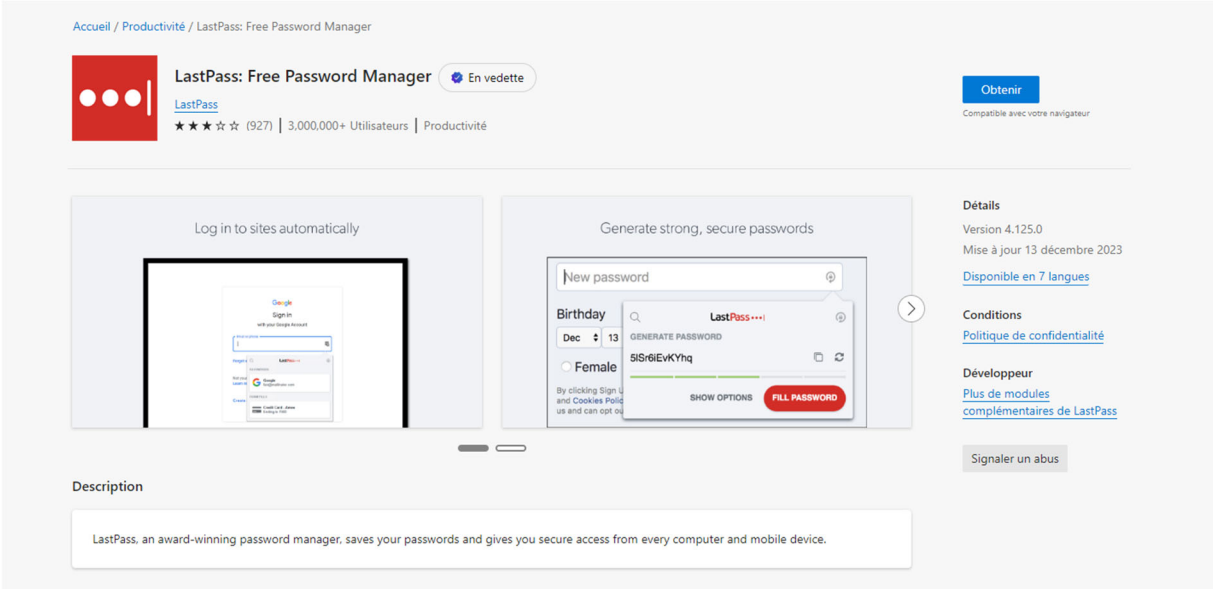
Aticle 3 :siteW –naviguer en toute sécurité sur internet

Article bonus : wikihow –comment surfer en securité sur internet

2/créer des mots de passe forts

LastPass est un gestionnaire de mots de passe freemium qui enregistre de manière sécurisée des mots de passe existants ou générés dans un compte privé du nuage du même nom. Disponible pour smartphones et module d'extension pour navigateur web, LastPass utilise la méthode de chiffrement AES-256.

Creation d'une compte last pass



3/la fonctionnalité de last pass

Avec LastPass, vous pouvez gérer vos mots de passe quel que soit l'endroit où vous vous trouvez. Les activités en ligne sont de plus en plus présentes dans nos vies : travail, loisirs, famille et amis... Dans ce tutoriel, découvrez comment utiliser LastPass, et comment simplifier et sécuriser votre vie numérique.

Avec LastPass, vous pouvez :

- créer, stocker et partager vos notes sécurisées et vos identifiants

- utiliser des notes sécurisées pour remplir automatiquement formulaires, données de connexion et de paiement
- créer différentes notes sécurisées en fonction de vos besoins

3/fonctionalité de la securité de votre navigateur

1/identifier les adresse internet qui te semble provenir d'une site malveillante

www.morvel.com; une deriv » du de www.marvel.com le site web officiel de l'univer marvel

www.fessebook.com un derivé de www.facebook.com le plus grand reseau social du monde

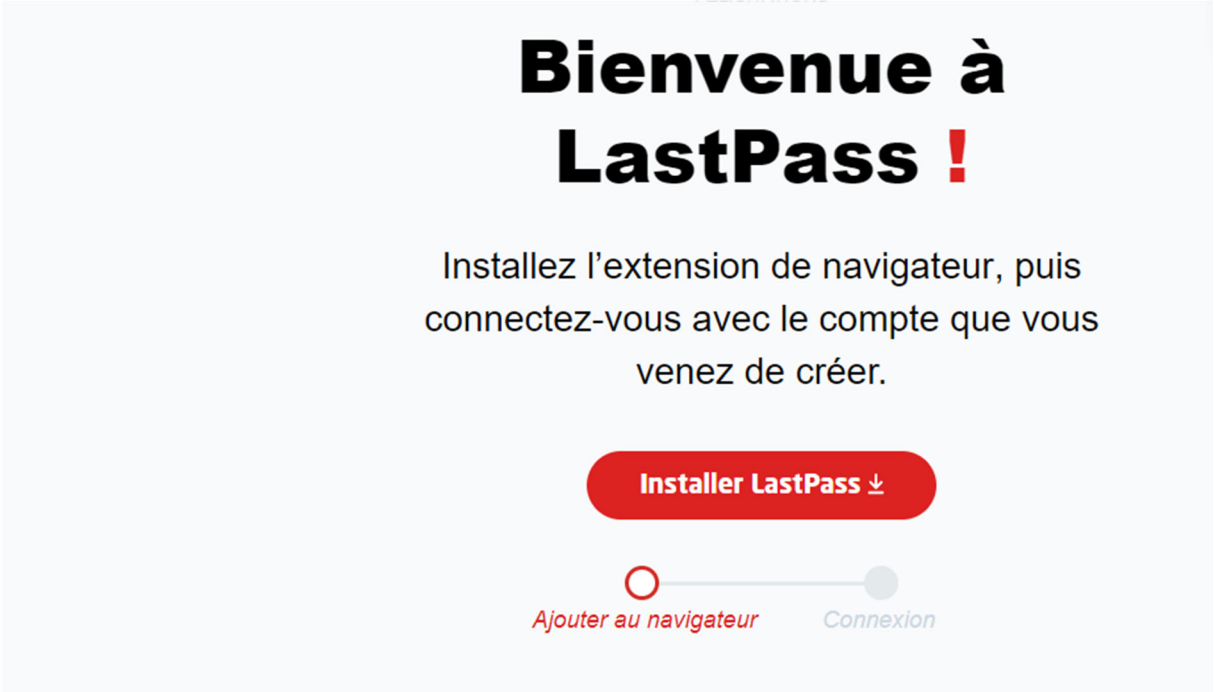
www.instagam.com le site dérivé de www.instagram.com un autre reseau social tres utiliser

les seul site qui semblaient etre cohérent sont donc

www.dccomics.com le site officiel de l'univers DC comic

www.ironman.com le site officiel d'une compétition internationnale le trianthlon (et non du super hero issus de l'univers)

2/ dans cet exercice nous allons verifier si les navigateur utiliser chrome et firefox dans notre exemple sont à jours pour ce faire suis les etapes suivantes suivante (case à cocher)



Pour firefox

4/eviter le spamet le phishing

1. dentifiez les spams :
   - Vérifiez l'adresse de l'expéditeur : La plupart des spams proviennent d'adresses email insensées ou incompréhensibles. Si vous ne savez pas si l'adresse email est légitime, vérifiez-la en la collant dans votre moteur de recherche.

- Regardez le type d'informations demandées : Les entreprises légitimes ne vous demandent pas des informations personnelles par email de manière inattendue.
- Restez sur vos gardes si le message semble urgent : Les spammeurs utilisent souvent des mots comme "urgent" pour vous inciter à agir rapidement.
- Vérifiez si votre nom est présent dans l'email : Les entreprises légitimes vous adressent correctement par votre nom.
- Vérifiez la grammaire et l'orthographe : Les fautes d'orthographe peuvent être un indicateur de spam.

2. Évitez d'ouvrir les pièces jointes :
- Si vous recevez un email d'un expéditeur inconnu avec une pièce jointe, évitez de l'ouvrir. Elle pourrait contenir un programme malveillant.

3. Utilisez des outils de filtrage :
- Configurez des filtres dans votre logiciel de messagerie pour rediriger les messages suspects vers le dossier spam.
- Utilisez des extensions pour votre navigateur internet ou votre logiciel de messagerie pour signaler les spams.

4. Soyez vigilant :
- N'installez que des logiciels provenant de sources fiables.
- Ne préenregistrez jamais vos informations sur des formulaires en ligne.

En suivant ces conseils, vous pourrez mieux protéger votre ordinateur contre les spams et les attaques de phishing.

5/comment eviter le logiciel malveillant

2. pplémentaires.

3. McAfee : Un excellent scanner pour la suppression totale des logiciels malveillants et des virus[1].

En plus de ces solutions, voici quelques conseils généraux pour protéger votre ordinateur contre les logiciels malveillants :

- Adoptez une attitude vigilante : Soyez prudent lorsque vous naviguez sur Internet et évitez de cliquer sur des liens suspects.

- Installez un outil de détection de sites web malveillants (comme WOT) pour vous avertir des sites potentiellement dangereux
    - Copilot
    - La meilleure solution de protection contre les logiciels malveillants dépend de vos besoins spécifiques et de votre environnement informatique. Cependant, voici quelques options populaires en 2024

2. Bitdefender : Il offre une protection avancée contre les malwares avec de nombreuses fonctionnalités supplémentaires.

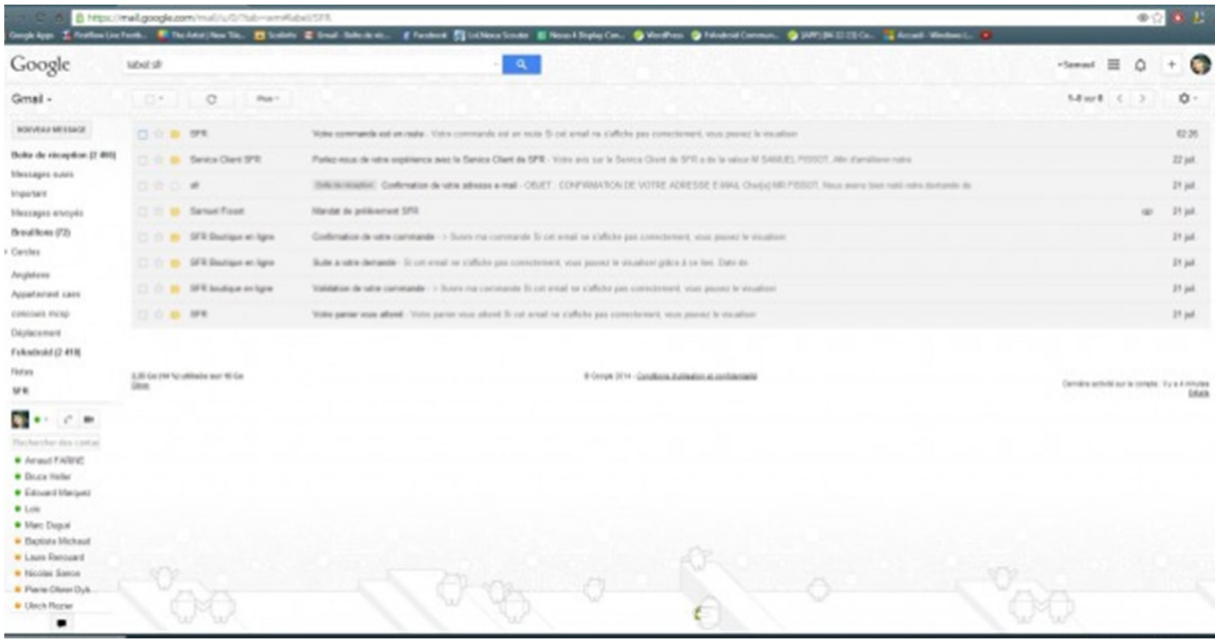
Norton **:** taux de détection de malware de 100 % et suppression immédiate de tous les fichiers malveillants. Il est simple, rapide, et facile à utiliser, et a plus de fonctionnalités que la plupart de ses concurrents, dont un pare-feu, une protection web, un réseau virtuel privé (VPN), un gestionnaire de mots de passe, le contrôle parental, la surveillance du dark web et bien plus encore

6/Acaht en ligne securiser

Dans cette escercice on va t'aider à créer un registre des achat comme tu as pu le voir dans le cours ce registre a pour but de conserver les information relation à tes achats en ligne

1creer un dossier sur ta messagerie electronique

2 créer un dossier sur ton espace de stockage personnel (en local ou sur le cloud)



7/comprendre un navigateur

1. Sur votre ordinateur, ouvrez Chrome.
2. En haut à droite, cliquez sur Plus ⋮ › Paramètres ⚙.
3. Cliquez sur **Confidentialité et sécurité** › **Cookies tiers**.
    - Conseil : Si vous faites partie du groupe de test de la fonctionnalité Protection contre le suivi, sélectionnez plutôt Protection contre le suivi.
4. Cliquez sur Voir toutes les données et autorisations des sites › Effacer toutes les données.

5. Pour confirmer la suppression, cliquez sur Supprimer

8/les principe de base de la confidentialité des media sociaux

Plus tot dans le cours tu as déjà été méné a utiliser ce reseau social en partageant une publication dans cet exercice on va montrer le reglage des paramètre de confidentialitépour facebook suis les etape suivantes

Connecter à ton compte facebook

Une fois sur la page d'acceuil ouvre le menu facebook puis effectuer un clic sur paramètre

Ce sont des onglet confidentiels et publication publique qui nous interssent accède à confidentialité e clic sur le premier rubrique

Cette rubrique resume les grandes ligne de la confidetialité sur facbook

1. Cliquez sur votre photo de profil en haut à droite de Facebook.
2. Cliquez sur Paramètres et confidentialité, puis sur Paramètres.
3. Cliquez sur Sécurité et connexion.
4. Sous Facebook Protect, cliquez sur Démarrer.
5. Sur l'écran d'accueil, cliquez sur Suivant.
6. Sur l'écran qui indique les avantages de Facebook Protect, cliquez sur Suivant.
7. Nous vérifierons si votre compte présente des failles et vous suggérerons des corrections pour renforcer la sécurité de votre compte lorsque vous activez Facebook Protect. Parmi les corrections courantes, nous vous suggérons de choisir un mot de passe plus fort ou d'activer l'authentification à deux facteurs.
8. Cliquez sur Corriger maintenant et suivez les instructions qui apparaissent à l'écran pour finaliser l'activation de Facebook Protect.

9/que faire si votre ordinateur est infecter par un virus

1. Changer d'antivirus ou le mettre à jour. Si votre antivirus actuel n'a pas pu empêcher l'infiltration du malware, il se peut qu'il ne soit pas assez performant.
2. Procéder à une mise en quarantaine des fichiers infectés. Lorsque le scan est fini, vous pouvez procéder à une mise en quarantaine des fichiers infectés.
3. Réinstallation du système. Si les virus sont trop nombreux et que le système est trop endommagé, il peut être nécessaire de réinstaller le système d'exploitation