



- + Parcours : DISCOVERY
- + Module : Naviguer en toute sécurité
- + Projet 1 - Un peu plus de sécurité, on n'en a jamais assez !

FANOMEZANJANAHARY Sitrakiniaina Elysa

1 - Introduction à la sécurité sur Internet :

La découverte de la sécurité sur internet

1/ Trois articles qui parlent de sécurité sur internet.

Article 1 : <https://www.lebigdata.fr/site-dangereux-a-eviter> Top des sites les plus dangereux à éviter en ligne.

Article 2 : <https://www.netcost-security.fr/mobilite/151010/naviguez-en-toute-securite-grace-a-la-derniere-mise-a-jour-de-mozilla-firefox/> Naviguez en toute sécurité grâce à la dernière mise à jour de Mozilla Firefox

Article 3 : <https://etp-bor.imfr.cgi.com/Alize/accueil/les-ministeres/lessentiel-de-lactualite/savez-vous-vraiment-assurer-votr.html?begin8783647c-c85d-45d9-a61f-69ee62995f08=20&end8783647c-c85d-45d9-a61f-69ee62995f08=29&pagesize8783647c-c85d-45d9-a61f-69ee62995f08=10&newsFullPagePicture=true&retrieveRightColumnContent=false&> Savez-vous vraiment assurer votre sécurité numérique sur internet ?

2 - Créer des mots de passe forts :

Utiliser un gestionnaire de mot de passe LastPass

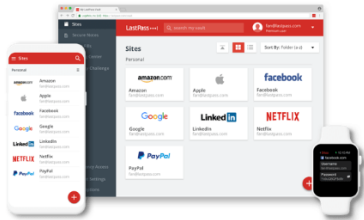
1/ Dans cet exercice, nous allons voir comment utiliser pour la première fois un gestionnaire de mot de passe nommé LastPass. Ce gestionnaire prend la forme d'une application web, accessible sur tous supports (PC, Mac, mobile). Il est simple à prendre en main et propose un niveau de sécurité optimal. Suis les étapes suivantes.

✓ Accède au site de LastPass

LastPass.....[®]

Un mot de passe. Zéro souci.

| LastPass s'occupe du reste.





Fonctionnalités Free

- ✓ Coffre-fort de mots de passe sécurisé ⓘ
- ✓ Accès sur un type d'appareils ⓘ

Créer un compte

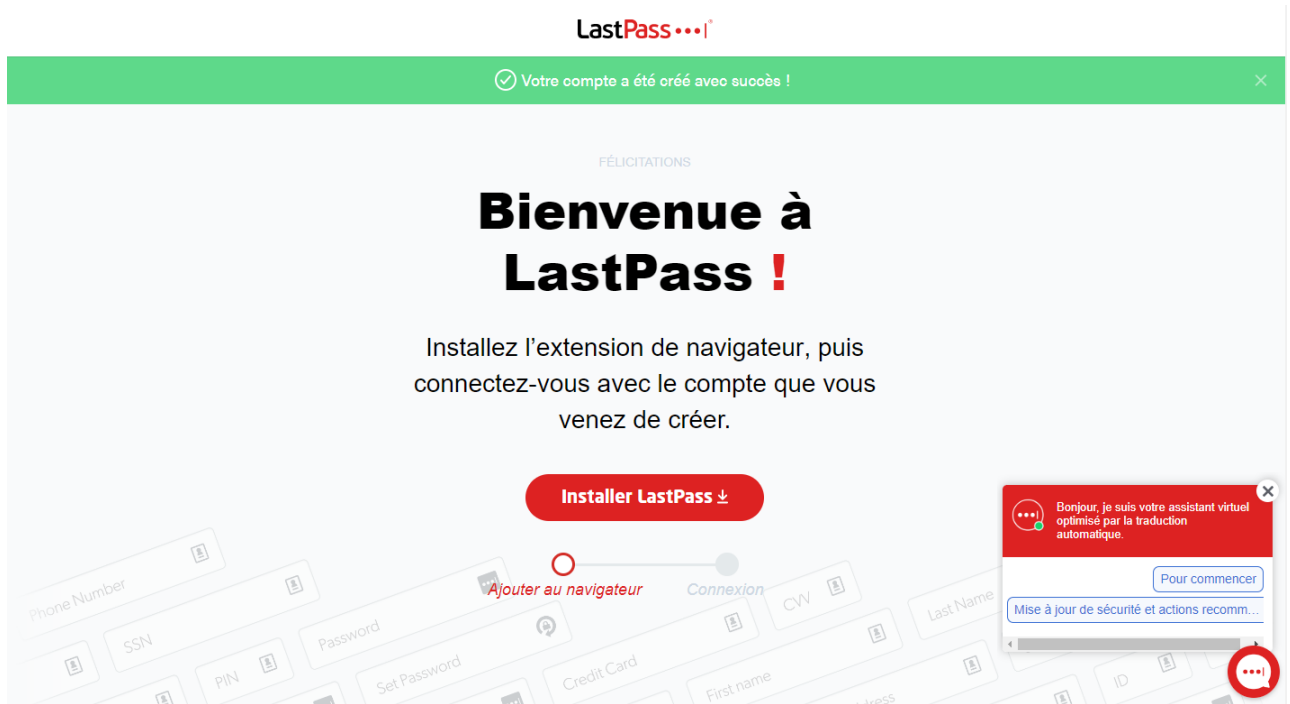
[ou Connexion](#)

 
Force
 

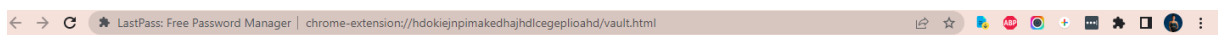
Inscrivez-vous - c'est gratuit

En remplissant ce formulaire, j'accepte les [Conditions générales](#) et la [Politique de confidentialité](#). Je souhaite recevoir des e-mails promotionnels, sauf si [je me désinscris](#).

- ✓ Crée un compte en remplissant le formulaire. Un conseil, on te demande de choisir un mot de passe maître. Pour rappel, ce mot de passe sera unique et te permettra d'accéder à tous tes comptes. Choisis donc un mot de passe avec un niveau de sécurité élevé et assure-toi de pouvoir le retrouver.
- ✓ Une fois la création du compte effectuée, tu arrives sur une page de validation qui propose le téléchargement de l'extension sur ton navigateur. Lance l'installation en effectuant un clic sur le bouton prévu à cet effet.



- ✓ Il te suffit de valider l'opération sur le Chrome Web Store en effectuant un clic sur le bouton "Ajouter à Chrome"
- ✓ Une fois installé, il te suffit d'accéder à cette extension et de t'y connecter
- ✓ En haut à droite du navigateur, clic sur le logo "Extensions"
- ✓ Épingler l'extension de LastPass avec l'icône
- ✓ Il ne te reste plus qu'à te connecter en effectuant un clic sur l'icône de l'extension et en saisissant ton identifiant et mot de passe



CONNEXION
OU [CRÉER UN COMPTE](#)

Adresse e-mail
Sitrakiniainaelysa7@gmail.com

Mot de passe maître
***** 👁

CONNEXION

[MOT DE PASSE OUBLIÉ ?](#)

[Options avancées](#)

3 - Fonctionnalité de sécurité de votre navigateur :


Identifier les éléments à observer pour naviguer sur le web en toute sécurité.

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

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 :



ERREUR
L'URL demandée n'a pas pu être trouvé

L'erreur suivante s'est produite en essayant d'accéder à l'URL : <https://192.168.10.254/sgerror.php?>

Il n'a pas été possible d'établir une connexion sécurisée avec 192.168.10.254

The system returned:

















(92) Protocol error (TLS code: X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT)


Self-signed SSL Certificate: /O=pfSense webConfigurator Self-Signed Certificate/CN=pfSense-6294ce71ba40d

Ce proxy et l'hôte distant n'ont pas pu négocier mutuellement une connexion sécurisée pour le traitement de votre requête. Il est possible que l'hôte distant ne supporte pas les connexions sécurisées, ou que le proxy n'est pas satisfait du certificat de sécurité de l'hôte distant.

Votre administrateur proxy est elijaona@sincro.org.

Générée le Wed, 05 Apr 2023 06:20:28 GMT par sincro_proxy (squad/4.15)


← → ↺ ⚠ Non sécurisé | <https://192.168.10.254/sgerror.php?>                 En pause ⋮



Votre connexion n'est pas privée

Des individus malveillants tentent peut-être de subtiliser vos informations personnelles sur le site **192.168.10.254** (mots de passe, messages ou numéros de carte de crédit, par exemple). [En savoir plus](#)

NET::ERR_CERT_AUTHORITY_INVALID

 Pour bénéficier du niveau de sécurité le plus élevé de Chrome, [activez la protection renforcée](#)

Paramètres avancés

Revenir en lieu sûr

www.instagram.com : un dérivé de www.instagram.com





Se connecter

OU

 Se connecter avec Facebook

Mot de passe oublié ?

Vous n'avez pas de compte ? Inscrivez-vous

Téléchargez l'application.

DISPONIBLE SUR



Obtenir sur

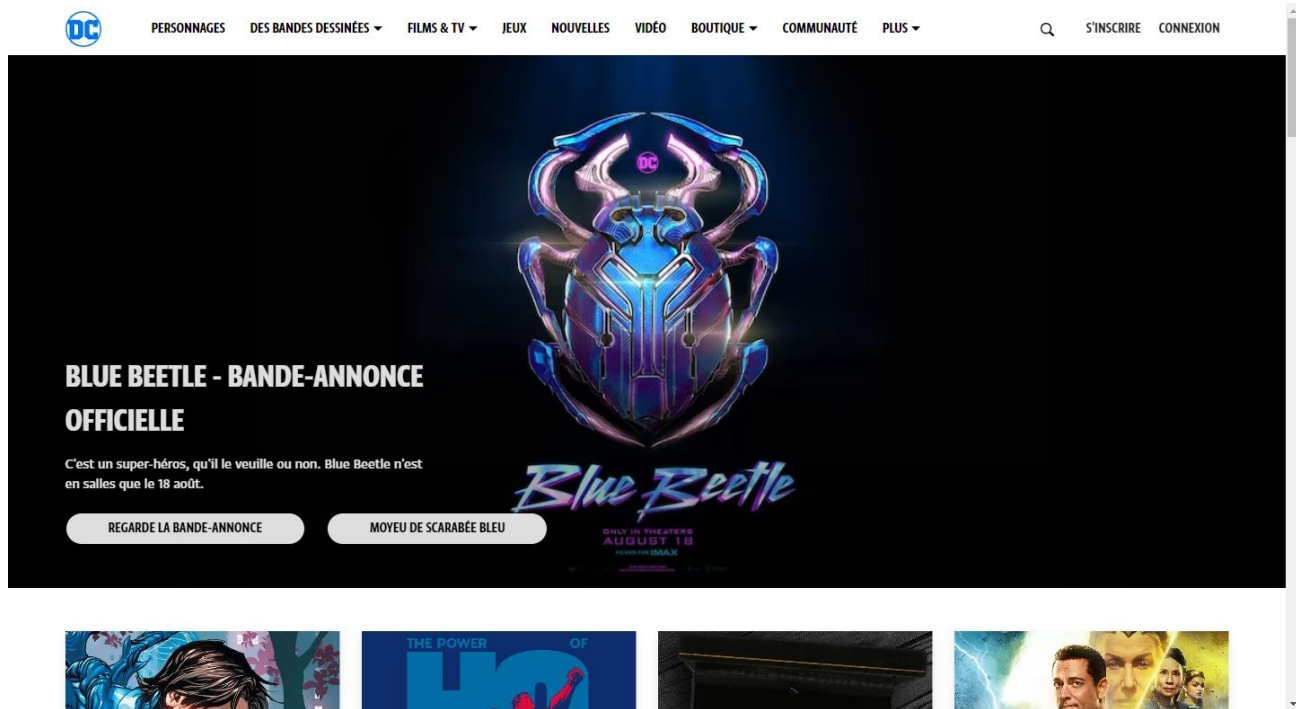


[Meta](#) [À propos](#) [Blog](#) [Emplois](#) [Aide](#) [API](#) [Confidentialité](#) [Conditions](#) [Comptes principaux](#) [Lieux](#) [Instagram Lite](#) [Importation des contacts et non-utilisateurs](#) [Meta Verified](#)

Français  © 2023 Instagram par Meta

Les sites qui semblaient être cohérents sont:

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

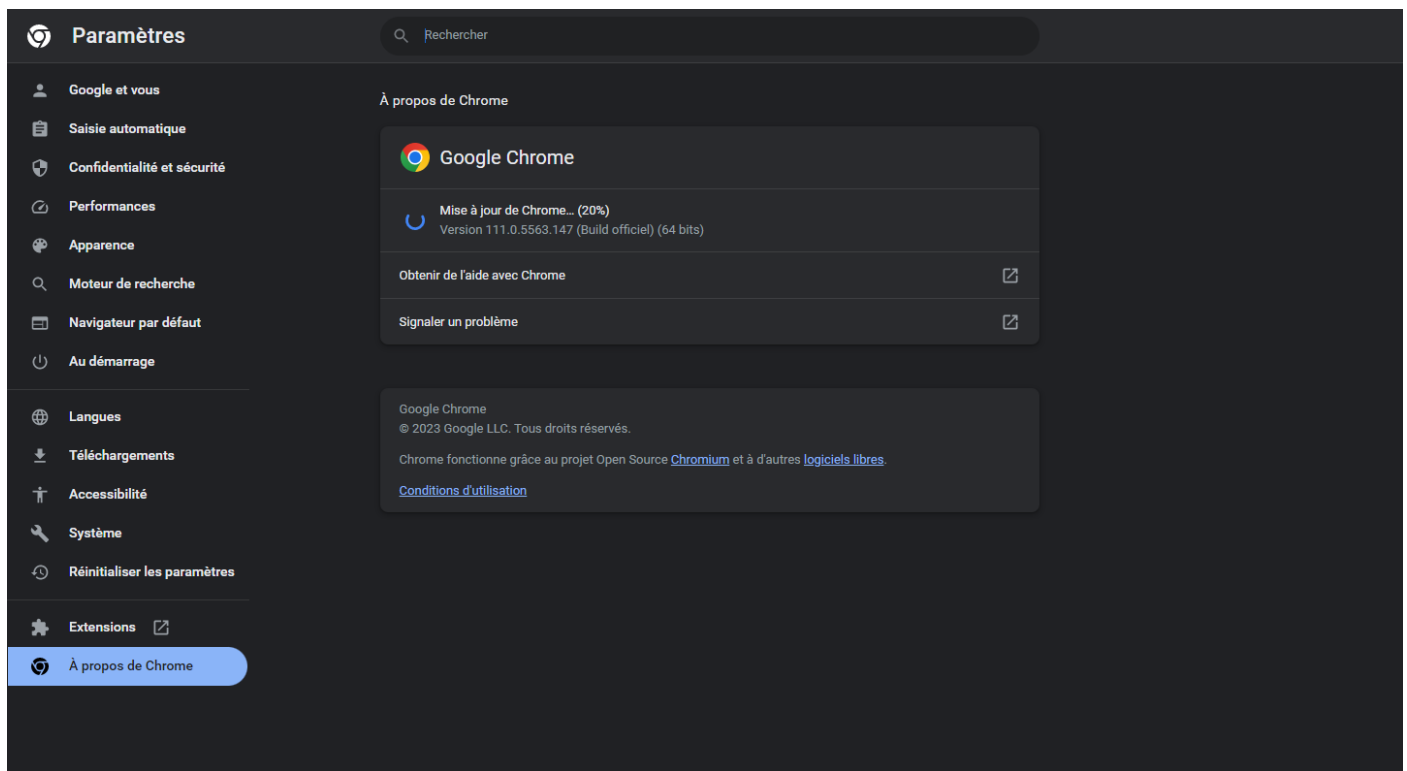


www.ironman.com : le site officiel d'une compétition internationale de triathlon



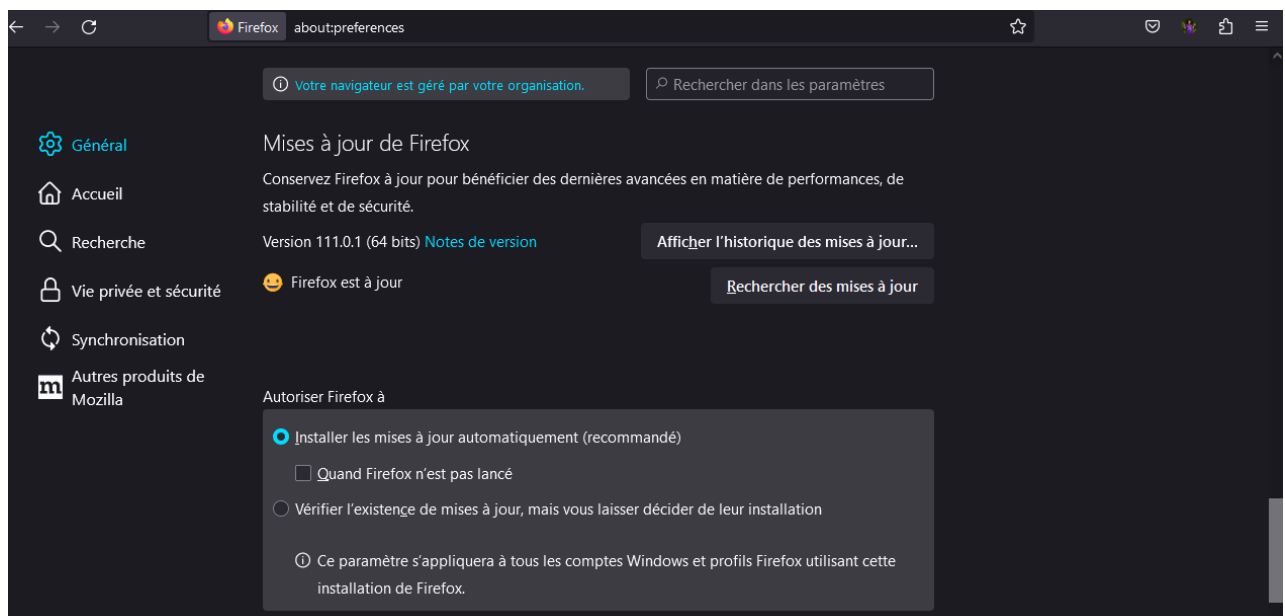
2/ Dans cet exercice, nous allons vérifier si les navigateurs utilisés, Chrome et Firefox dans notre exemple, sont à jour. Pour ce faire, suis les étapes suivantes.

- Pour Chrome
 - ✓ Ouvre le menu du navigateur et accède aux "Paramètres"
 - ✓ Clic sur la rubrique "A propos de Chrome"
 - ✓ Si tu constates le message "Chrome est à jour", c'est Ok



Il se met à jour automatique.

- Pour Firefox
 - ✓ Ouvre le menu du navigateur et accède aux “Paramètres”
 - ✓ Dans la rubrique “Général”, fais défiler jusqu’à voir la section “Mise à jour de Firefox (astuce : tu peux également saisir dans la barre de recherche (2) “mises à jour” pour tomber directement dessus)

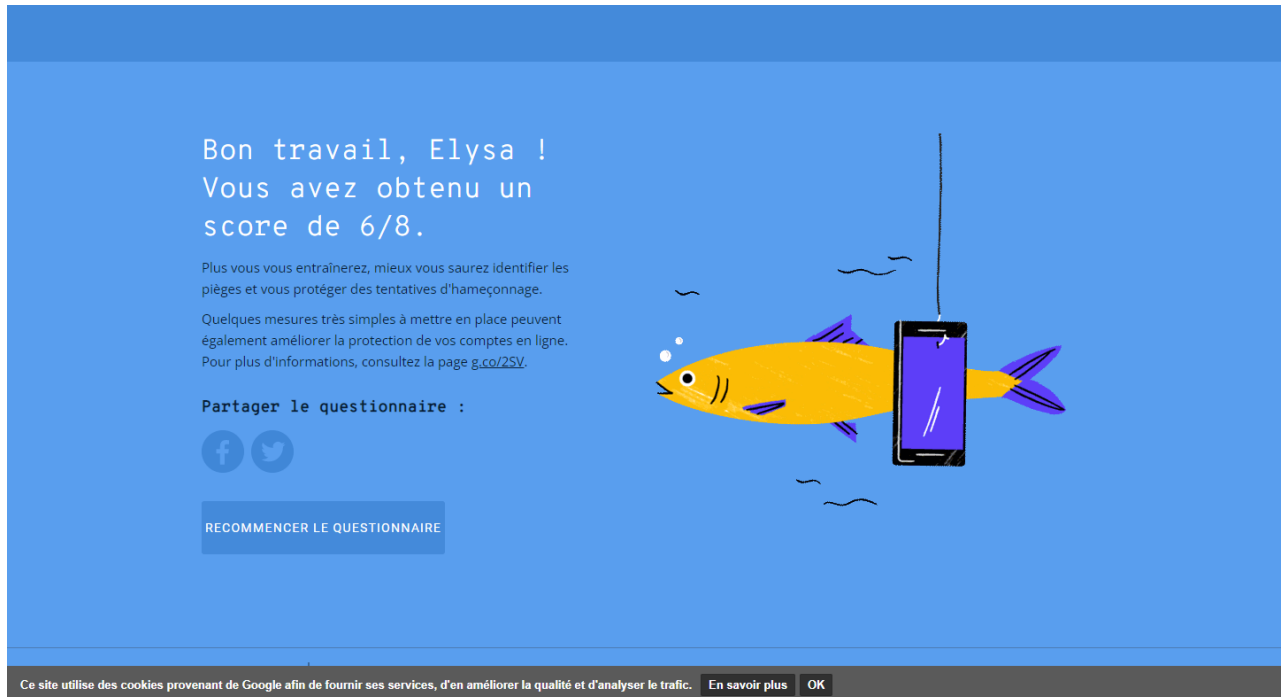


- ✓ Vérifie que les paramètres sélectionnés sont identiques que sur la photo

4 - Éviter le spam et le phishing

Reconnaître plus facilement les messages frauduleux

1/ Dans cet exercice, on va exercer ta capacité à déceler les erreurs dans les messages cachant une action malveillante en arrière-plan.



5 - Comment éviter les logiciels malveillants :

Sécuriser votre ordinateur et identifier les liens suspects

3/ Lors de la navigation sur le web, il arrive d'avoir des doutes sur la sécurité de certains sites. Comme tu as pu le voir précédemment, le premier de niveau de vigilance à avoir se trouve dans la barre d'adresse des navigateurs web. La plupart affichent des indicateurs de sécurité pour donner une information sur la protection d'un site internet.

Site n°1 :

o Indicateur de sécurité

■ HTTPS 

État du site selon la navigation sécurisée

Grâce à la fonctionnalité de navigation sécurisée offerte par Google, des milliards d'URL sont analysés chaque jour afin de détecter les sites Web suspects. Nous découvrons ainsi des milliers de nouveaux sites douteux tous les jours, parmi lesquels figurent de nombreux sites Web légitimes ayant été infectés. Nous signalons ensuite ces sites par des avertissements dans la recherche Google et dans les navigateurs Web. Vous pouvez effectuer une recherche pour savoir si un site Web en particulier présente un danger.

Vérifier l'état du site



État actuel

✓ Aucun contenu suspect détecté

Informations sur le site

Ces informations ont été mises à jour pour la dernière fois le 5 avr. 2023.

La sécurité d'un site peut évoluer. Vérifiez régulièrement s'il y a des changements.

o Analyse Google

■ Aucun contenu suspect

Site n°2 :

○ Indicateur de sécurité

■ HTTPS 

Etat du site selon la navigation sécurisée

Grâce à la fonctionnalité de navigation sécurisée offerte par Google, des milliards d'URL sont analysées chaque jour afin de détecter les sites Web suspects. Nous découvrons ainsi des milliers de nouveaux sites douteux tous les jours, parmi lesquels figurent de nombreux sites Web légitimes ayant été infectés. Nous signalons ensuite ces sites par des avertissements dans la recherche Google et dans les navigateurs Web. Vous pouvez effectuer une recherche pour savoir si un site Web en particulier présente un danger.

Vérifier l'état du site



État actuel

✓ Aucun contenu suspect détecté

Informations sur le site

Ces informations ont été mises à jour pour la dernière fois le 5 avr. 2023.

La sécurité d'un site peut évoluer. Vérifiez régulièrement s'il y a des changements.

○ Analyse Google

■ Aucun contenu suspect

Site n°3

○ Indicateur de sécurité

■ Not Secure

État du site selon la navigation sécurisée

Grâce à la fonctionnalité de navigation sécurisée offerte par Google, des milliards d'URL sont analysées chaque jour afin de détecter les sites Web suspects. Nous découvrons ainsi des milliers de nouveaux sites douteux tous les jours, parmi lesquels figurent de nombreux sites Web légitimes ayant été infectés. Nous signalons ensuite ces sites par des avertissements dans la recherche Google et dans les navigateurs Web. Vous pouvez effectuer une recherche pour savoir si un site Web en particulier présente un danger.

Vérifier l'état du site



État actuel

Vérifier une URL en particulier

Il est difficile d'indiquer un simple niveau de sécurité pour les sites comme <http://www.baidu.com/>, qui comportent énormément de contenu. Des sites généralement considérés comme étant fiables présentent parfois du contenu suspect (par exemple, dans les blogs ou les commentaires). Pour obtenir des informations plus détaillées sur la sécurité, vérifiez un annuaire ou une page Web spécifiques.

○ Analyse Google

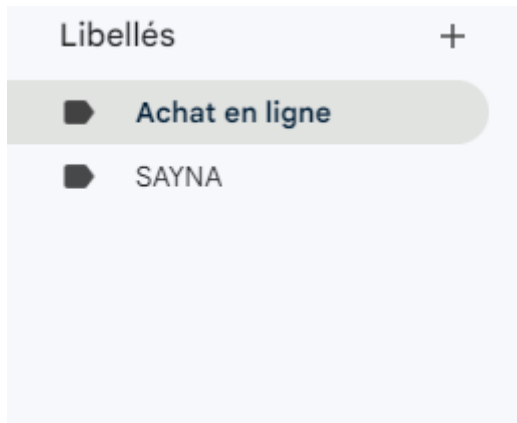
■ Vérifier un URL en particulier (analyse trop générale)

6 - Achats en ligne sécurisés Objectif :

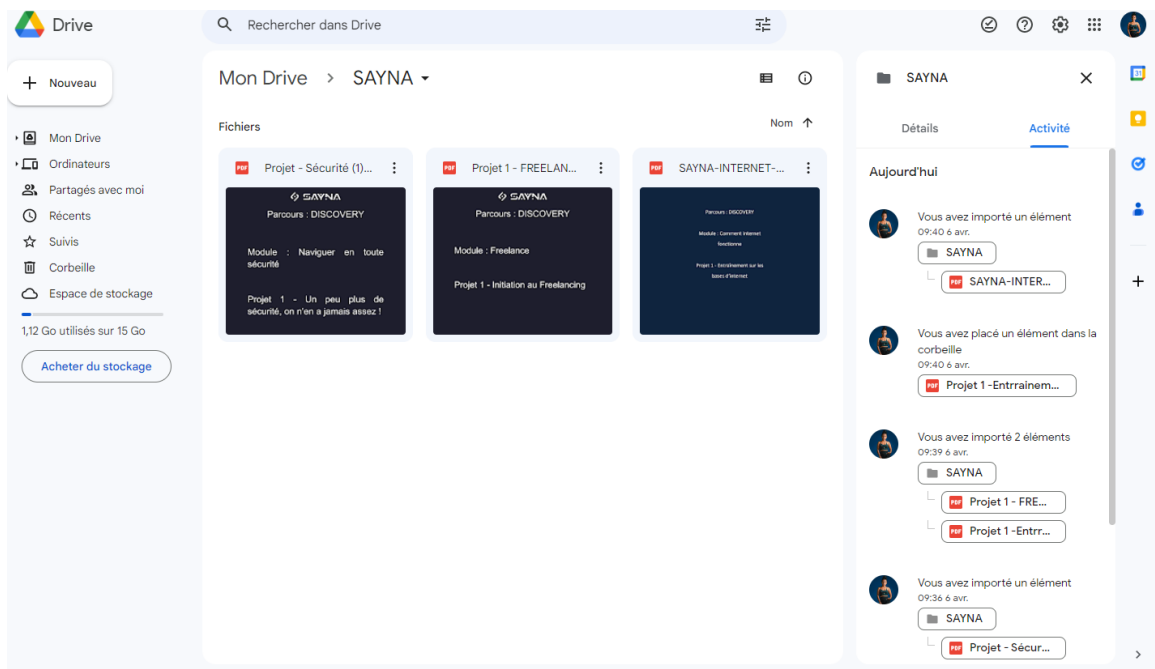
créer un registre des achats effectués sur internet

1/ Dans cet exercice, on va t'aider à créer un registre des achats. Comme tu as pu le voir dans le cours, ce registre a pour but de conserver les informations relatives à tes achats en ligne. Très pratique lorsque tu fais face à un litige, un problème sur ta commande ou tout simplement pour faire le bilan de tes dépenses du mois. Deux possibilités s'offrent à toi pour organiser ce registre :

1. Créer un dossier sur ta messagerie électronique



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



La première est la plus pratique à utiliser et la plus facile à mettre en place. Nous prendrons pour exemple la messagerie de Google (les autres messageries fonctionnent sensiblement de la même manière).

Suis les étapes suivantes pour créer un registre des achats sur ta messagerie électronique.

- ✓ Pour commencer, accède à ta messagerie électronique. Pour rappel, tu peux y accéder rapidement en ouvrant un nouvel onglet (dans la barre des favoris ou via le raccourci)

- ✓ Sur la page d'accueil de ta messagerie, tu trouveras sur la gauche les libellés initialement prévus (boîte de réception, messages envoyés, etc.)
- ✓ C'est dans cette partie que tu vas créer ta rubrique des achats. Pour ce faire, clic sur "Plus" et va tout en bas des libellés. Pour créer un libellé rapidement il te suffit d'effectuer un clic sur "Créer un libellé" et de le nommer "ACHATS" (pour notre exercice)
- ✓ Effectuer un clic sur le bouton "Créer" pour valider l'opération
- ✓ Tu peux également gérer les libellés en effectuant un clic sur "Gérer les libellés"(1). Sur cette page, tu peux gérer l'affichage des libellés initiaux (2) et gérer les libellés personnels (3)
- ✓ Tu as maintenant un libellé pour stocker tous tes messages électroniques relatifs aux achats effectués sur internet : confirmation de l'achat, détail de la commande, modalités de livraison.

7 - Comprendre le suivi du navigateur

Exercice présent sur la gestion des cookies et l'utilisation de la navigation privée

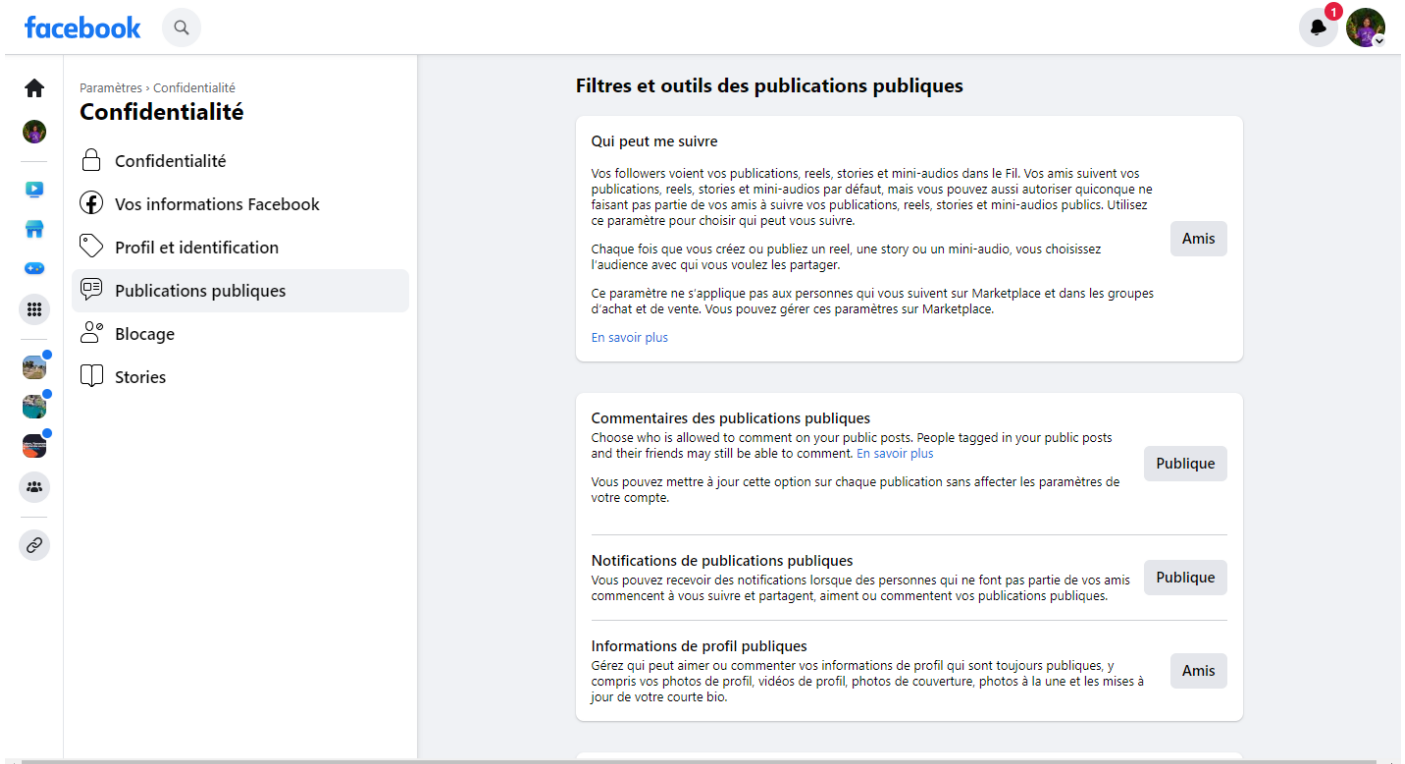
J'ai compris.

8 - Principes de base de la confidentialité des médias sociaux

Régler les paramètres de confidentialité de Facebook

1/ Plus tôt dans le cours (Internet de base) tu as déjà été amené à utiliser ce réseau social en partageant une publication. Dans cet exercice on va te montrer le réglage des paramètres de confidentialité pour Facebook. Suis les étapes suivantes.

- ✓ Connecte-toi à ton compte Facebook
- ✓ Une fois sur la page d'accueil, ouvre le menu Facebook , puis effectue un clic sur "Paramètres et confidentialité". Pour finir, clic sur "Paramètres"
- ✓ Ce sont les onglets "Confidentialité" et "Publications publiques" qui nous intéressent. Accède à "Confidentialité" pour commencer et clic sur la première rubrique
- ✓ Cette rubrique résume les grandes lignes de la confidentialité sur Facebook
- ✓ La première rubrique (orange) te permettra de régler la visibilité de tes informations personnelles
- ✓ La deuxième rubrique (bleu) te permet de changer ton mot de passe
- ✓ La troisième rubrique (violet) te permet de gérer la visibilité de ton profil pour la gestion des invitations
- ✓ La quatrième rubrique (vert) permet de gérer la connexion simplifiée sur des applications ou des sites utilisés qui permettent cela
- ✓ La dernière rubrique (rose) permet de gérer les informations récoltées par Facebook utiles pour les annonceurs



1/ Proposer un ou plusieurs exercice(s) pour vérifier la sécurité en fonction de l'appareil utilisé ??????

Pour un téléphone :

Ouvrez l'application Paramètres de votre téléphone. Appuyez sur Sécurité. L'état de sécurité de votre appareil et de votre compte Google s'affiche en haut de l'écran. Vous verrez apparaître un message d'avertissement si des actions importantes sont nécessaires pour sécuriser votre appareil ou vos comptes.

Contrôle de sécurité sur iPhone :

Si votre sécurité personnelle est compromise, utilisez « Contrôle de sécurité » sur iPhone (exécutant iOS 16 ou ultérieur) afin d'interrompre rapidement le partage de vos informations, ou de passer en revue et de mettre à jour le partage avec certaines personnes et apps.

Contrôle de sécurité sur un ordinateur :

Cliquez sur l'icône représentée par une petite flèche montante, sur la barre des tâches, afin d'ouvrir la zone de notifications : Cliquez ensuite sur l'icône « Centre de sécurité » : Et vérifiez maintenant l'état actuel de la protection antivirus de votre ordinateur.

2/ un exercice pour installer et utiliser un antivirus + antimalware pour un ordinateur :

Pour installer un antivirus et un antimalware sur votre ordinateur, vous pouvez suivre les étapes suivantes :

1. Téléchargez l'antivirus et l'antimalware de votre choix à partir de leur site officiel.
2. Ouvrez le fichier d'installation téléchargé et suivez les instructions à l'écran pour installer le logiciel.
3. Une fois l'installation terminée, ouvrez le programme et mettez-le à jour avec les dernières définitions de virus et de logiciels malveillants.
4. Exécutez une analyse complète de votre ordinateur pour détecter les virus et les logiciels malveillants existants.
5. Configurez le programme pour qu'il s'exécute automatiquement en arrière-plan et effectue des analyses régulières.

Il est important de noter que vous ne devez pas installer plusieurs antivirus ou antimalwares sur votre ordinateur en même temps car cela peut entraîner des conflits entre les programmes et réduire l'efficacité de la protection¹²³.