Parcours : DISCOVERY

Module : Naviguer en toute sécurité

Projet1 : Un peu plus de sécurité, on n'en a jamais assez !

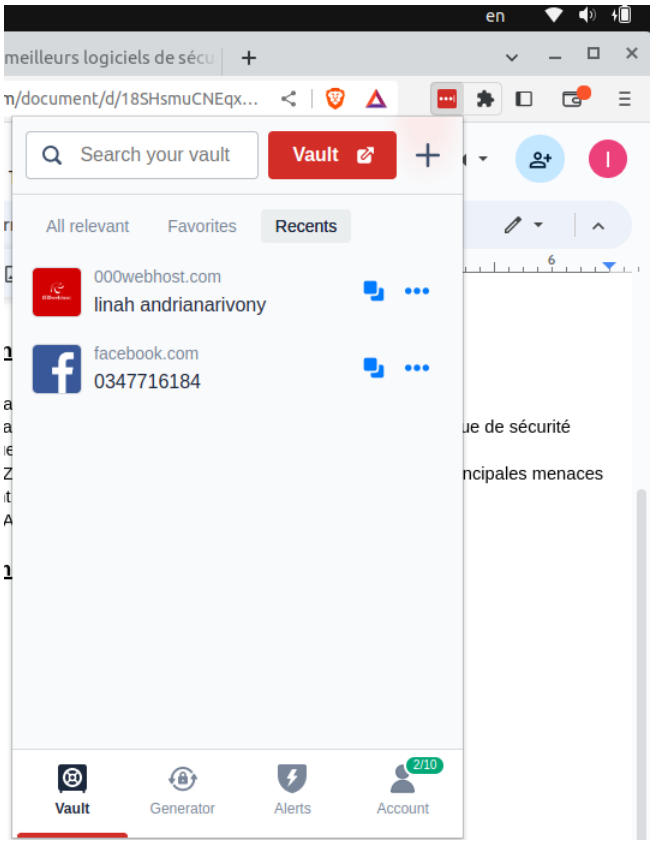
1 - Introduction à la sécurité sur Internet

Trois articles qui parlent de sécurité sur internet :

- Article 1 = ZDNet - "La sécurité des données dans le cloud: Les 10 principales menaces et comment s'en protéger"
- Article 3 = Avast - Les meilleurs logiciels de sécurité Internet en 2023.
- Article 3 = appviser - Pourquoi faut-il (absolument) adopter une politique de sécurité informatique dans votre entreprise ?

2 - Créer des mots de passe forts

Last pass ajouté :



3 - Fonctionnalités de sécurité de votre navigateur

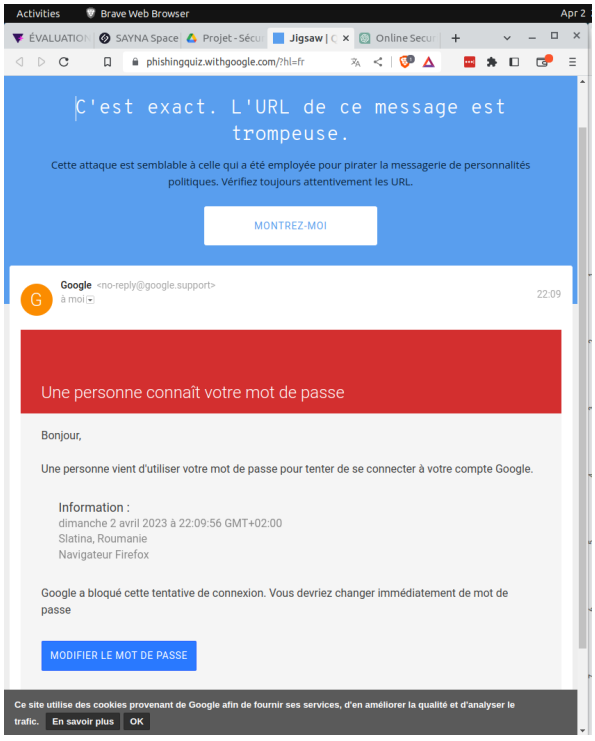
1) Les sites web qui semblent être malveillants sont :
    - www.morvel.com, un dérivé de www.marvel.com, le site web officiel de l'univers Marvel.
    - www.fessebook.com, un dérivé de www.facebook.com, le plus grand réseau social du monde.
    - www.instagam.com, un dérivé de www.instagram.com, un autre réseau social très utilisé.

    Les sites web qui semblent 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 (et non du super-héros issu de l'univers Marvel).

2) J'ai pu constater que les paramètres par défaut des navigateurs Chrome et Firefox sont réglés pour réaliser les mises à jour automatiquement. Comme d'habitude, Firefox affiche une personnalisation des paramètres un peu plus poussée.

4 - Eviter le spam et le phishing

1) Exercice pour déceler les erreurs dans les messages cachant une action malveillante en arrière-plan :



5 - Comment éviter les logiciels malveillants

- Site n°1 :
  - Indicateur de sécurité
    - HTTPS
  - Analyse Google
    - Aucun contenu suspect

- Site n°2 :
  - Indicateur de sécurité
    - HTTPS
  - Analyse Google
    - Aucun contenu suspect

- Site n°3 :
  - Indicateur de sécurité
    - HTTPS
  - Analyse Google
    - Vérifier un URL en particulier (analyse trop générale)

6 - Achats en ligne sécurisés

Exemple d'organisation de libellé pour gérer sa messagerie électronique :

- Achats : historique, facture, conversations liés aux achats.
- Administratif : toutes les démarches administratives.
- Banque : tous les documents et les conversations liés à la banque personnelle.
- Création de compte : tous les messages liés à la création d'un compte (message de bienvenue, résumé du profil, etc.).
- Job : tous les messages liés à mon projet professionnel.
- SAYNA : tous les messages liés à mon activité avec SAYNA.
- Linkedin : tous les messages liés à mon compte Linkedin.

7 - Comprendre le suivi du navigateur

8 - Principes de base de la confidentialité des médias sociaux

Réglage des paramètres de confidentialité pour Facebook:

- ☑ Je me connecte à mon compte facebook.

- ☑ Une fois sur la page d’accueil, j’ouvre le menu Facebook , puis j’effectue un clic sur“Paramètres et confidentialité”. Pour finir, je clic sur “Paramètres”.
- ☑ Ce sont les onglets “Confidentialité” et “Publications publiques” qui m'intéressent. J’accède à “Confidentialité” pour commencer et je clic sur la première rubrique.
- ☑ Cette rubrique résume les grandes lignes de la confidentialité sur Facebook.
- ☑ Retourne dans les paramètres généraux en effectuant un clic sur la croix en haut à gauche. Je peux continuer à explorer les rubriques pour personnaliser mes paramètres.
- ☑ Dans les paramètres de Facebook j’ai également un onglet “Cookies”. On m’en a parlé dans le cours précédent (Comprendre le suivi du navigateur). Maintenant que je sais comment sont utilisées mes données, je suis capable de choisir en pleine conscience ce que je souhaite partager.

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

1)

Voici quelques exercices pour vérifier la sécurité en fonction de l'appareil utilisé :

a) Ordinateur : Utilisez un logiciel antivirus pour scanner votre ordinateur à la recherche de virus ou de logiciels malveillants. Assurez-vous également que votre système d'exploitation et vos applications sont à jour avec les derniers correctifs de sécurité. Vérifiez également que votre pare-feu est activé pour bloquer les connexions non autorisées.
b) Smartphone : Installez une application antivirus pour scanner votre téléphone à la recherche de virus ou de logiciels malveillants. Évitez également de télécharger des applications à partir de sources non fiables, car celles-ci peuvent contenir des logiciels malveillants. Activez également la fonction de verrouillage de l'écran pour empêcher l'accès non autorisé à votre téléphone.
c) Routeur Wi-Fi : Changez le mot de passe par défaut de votre routeur Wi-Fi pour un mot de passe fort et unique. Assurez-vous également que votre routeur est protégé par un pare-feu et que le chiffrement Wi-Fi est activé. Évitez également de partager votre mot de passe Wi-Fi avec des personnes que vous ne connaissez pas ou en public

2)

Voici un exemple d'exercice pour installer et utiliser un antivirus + antimalware en fonction de l'appareil utilisé :

a) Ordinateur : Téléchargez un logiciel antivirus + antimalware réputé et installez-le sur votre ordinateur.Une fois installé, exécutez une analyse complète pour

détecter les virus, les logiciels malveillants et les autres menaces. Si une menace est détectée, suivez les instructions du logiciel pour la supprimer.

b) Smartphone : Téléchargez une application antivirus + antimalware pour smartphone et installez-la sur votre téléphone. Ouvrez l'application et exécutez une analyse complète pour détecter les virus, les logiciels malveillants et les autres menaces. Si une menace est détectée, suivez les instructions de l'application pour la supprimer.
c) Tablette : Téléchargez une application antivirus + antimalware pour tablette et installez-la sur votre appareil. Ouvrez l'application et exécutez une analyse complète pour détecter les virus, les logiciels malveillants et les autres menaces. Si une menace est détectée, suivez les instructions de l'application pour la supprimer.