Module : Naviguer en toute sécurité

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

1/ En naviguant sur le web, consulte trois articles qui parlent de sécurité sur internet.

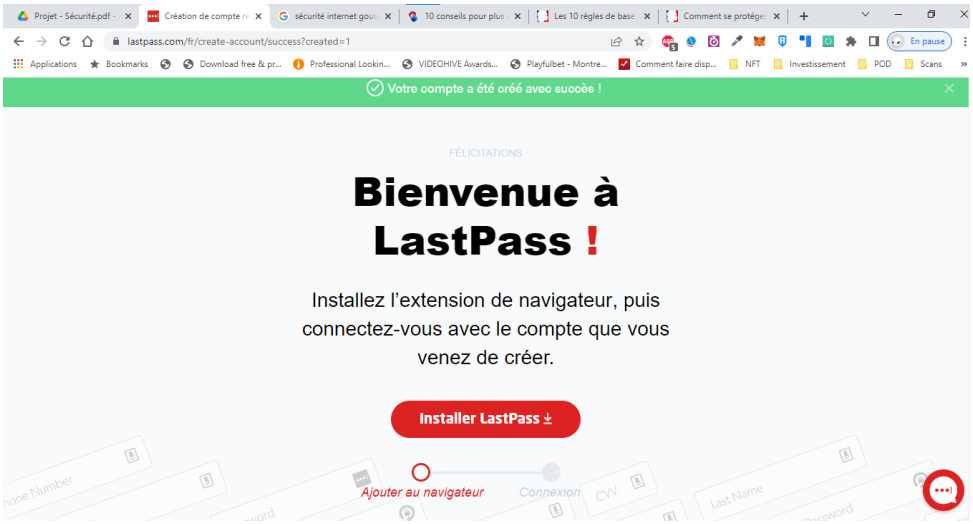
Pense à vérifier la source des informations et essaie de consulter des articles récents pour que les informations soient à jour. Saisis le nom du site et de l'article.

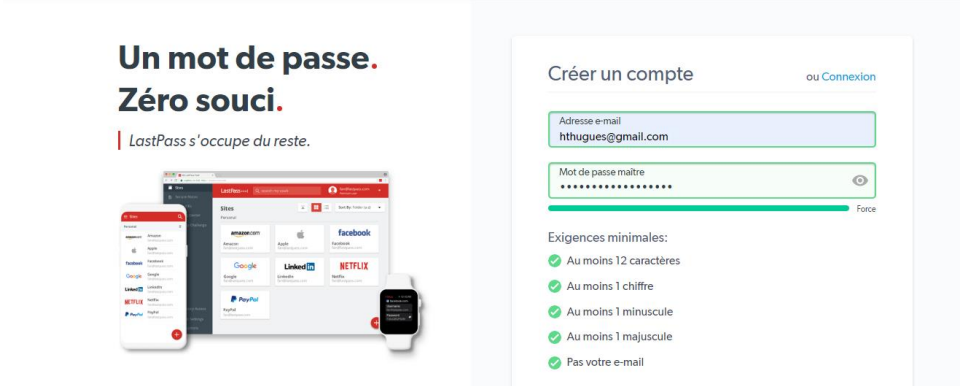
- Article 1 = cybermalveillance.gouv - Comment se protéger sur Internet ?
- Article 2 = swisscom.ch - 10 conseils pour plus de sécurité sur Internet
- Article 3 = cybermalveillance.gouv - Les 10 règles de base pour la sécurité numérique

---

2 - Créer des mots de passe forts

Objectif : utiliser un gestionnaire de mot de passe LastPass





3 - Fonctionnalité de sécurité de votre navigateur

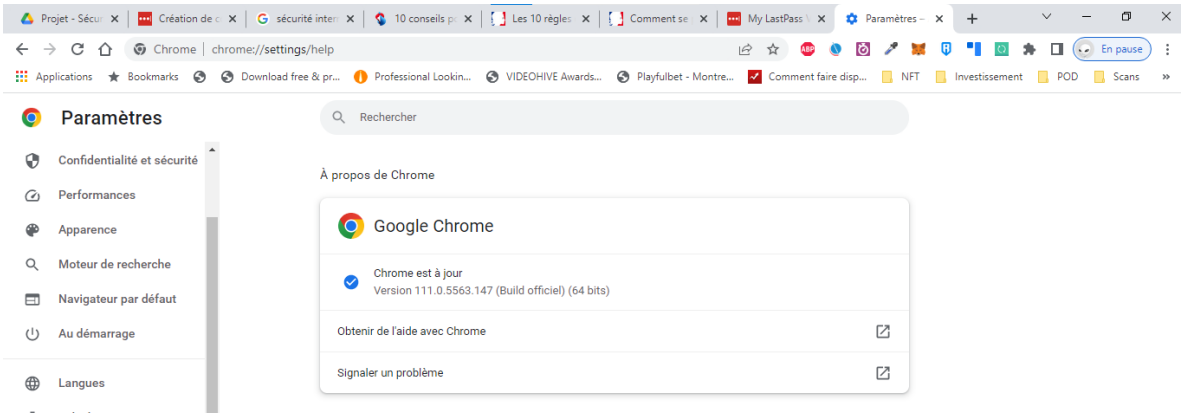
Objectif : identifier les éléments à observer pour naviguer sur le web en toute sécurité

1/ Identifie les adresses internet qui te semblent provenir de sites web malveillants. (case à cocher)

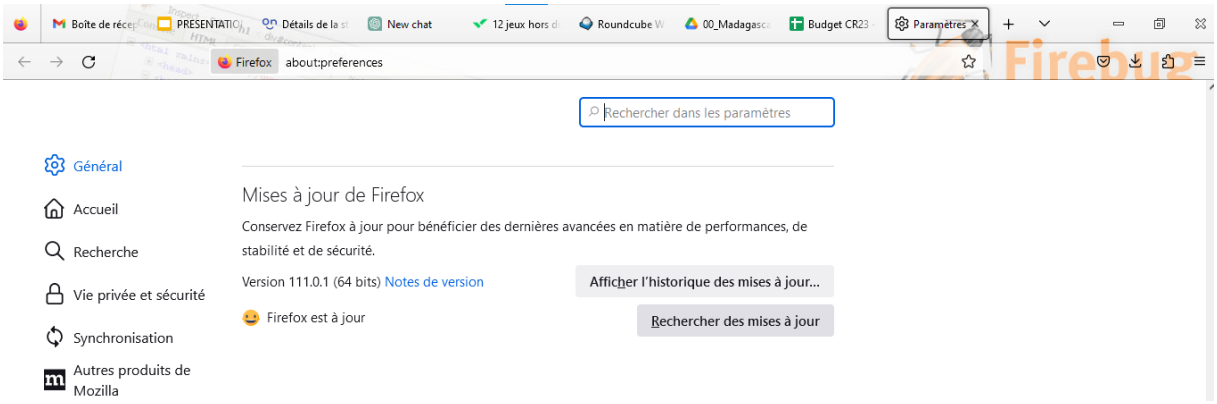
- www.morvel.com (semble être suspect)
- www.dccomics.com
- www.ironman.com
- www.fessebook.com (semble être suspect)
- www.instagam.com (semble être suspect)

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. (case à cocher)

- Pour Chrome



- Pour Firefox



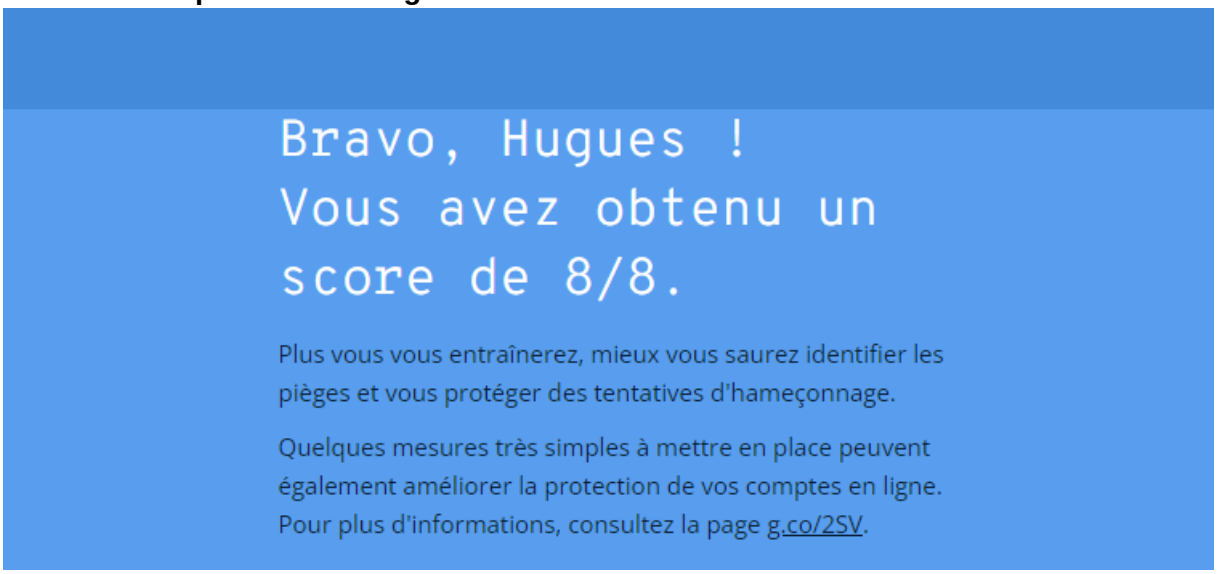
4 - Éviter le spam et le phishing

Objectif : 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.

Pour ce faire accède au lien suivant et suis les étapes qui y sont décrites :

Exercice 4 - Spam et Phishing



5 - Comment éviter les logiciels malveillants

Objectif : 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. Lorsque le doute persiste tu peux t'appuyer sur un outil proposé par Google : Google Transparency Report (en anglais) ou Google Transparence des Informations (en français). Afin d'améliorer ta lecture de la sécurité sur internet, tu vas devoir analyser les informations de plusieurs sites. Pour chaque site tu devras préciser l'indicateur de sécurité et le rapport d'analyse de l'outil Google. Il te suffit d'accéder aux liens proposés ci-dessous pour observer l'indicateur de sécurité et de copier-coller l'URL du site dans l'outil Google. (choix multiples)

- **Site n°1**
    - Indicateur de sécurité
        - **HTTPS** (Vrai)
        - ~~HTTPS Not secure~~
        - ~~Not secure~~
    - Analyse Google
        - **Aucun contenu suspect**
        - ~~Vérifier un URL en particulier~~

- **Site n°2**
    - Indicateur de sécurité
        - **HTTPS**
        - ~~HTTPS Not secure~~
        - ~~Not secure~~
    - Analyse Google
        - **Aucun contenu suspect**
        - ~~Vérifier un URL en particulier~~

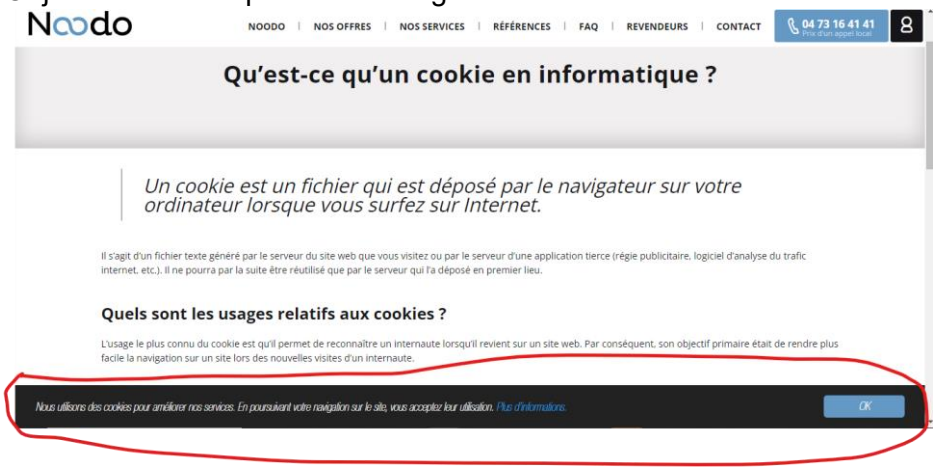
- **Site n°3**
    - Indicateur de sécurité
        - ~~HTTPS~~
        - ~~HTTPS Not secure~~
        - **Not secure**
    - Analyse Google
        - ~~Aucun contenu suspect~~
        - **Vérifier un URL en particulier**

6 - Achats en ligne sécurisés

Objectif : créer un registre des achats effectués sur internet

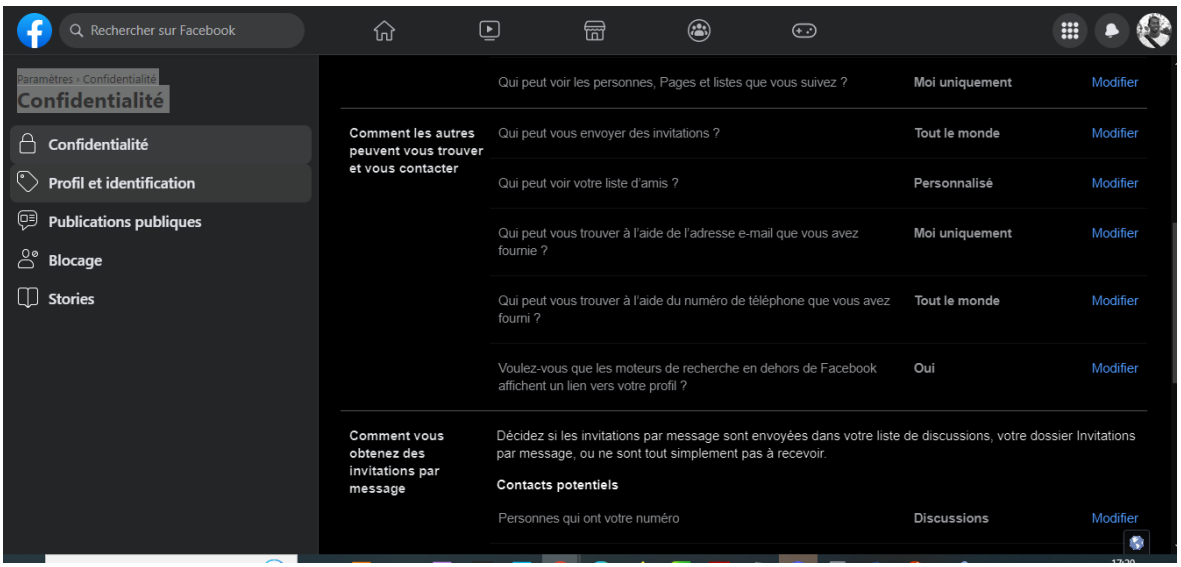
7 - Comprendre le suivi du navigateur

Objectif : exercice présent sur la gestion des cookies et l'utilisation de la navigation privée



8 - Principes de base de la confidentialité des médias sociaux

Objectif : Régler les paramètres de confidentialité de Facebook



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

Objectif :

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

Réponse :

Si votre ordinateur est infecté par un virus, la première chose à faire est de l'éteindre immédiatement pour éviter la propagation du virus. Ensuite, vous pouvez démarrer votre ordinateur en mode sans échec pour identifier et supprimer le virus à l'aide d'un logiciel antivirus fiable. Après avoir supprimé les fichiers infectés et nettoyé le registre Windows, vous devez changer tous vos mots de passe pour assurer la sécurité de vos données sensibles.

Pour vérifier la sécurité de votre ordinateur et de vos autres appareils, vous devez effectuer des mises à jour régulières de votre système d'exploitation, de votre navigateur et de tous les logiciels installés. Vous devez également utiliser des logiciels de sécurité fiables, évité de cliquer sur des liens suspects, utiliser des mots de passe forts et sauvegarder régulièrement vos données importantes.

En suivant ces étapes, vous pouvez protéger votre ordinateur et vos autres appareils contre les attaques malveillantes et garantir la sécurité de vos données sensibles.

2/ Proposer un exercice pour installer et utiliser un antivirus + antimalware en fonction de l'appareil utilisé.

Réponse :

1. Tout d'abord, assurez-vous que votre appareil dispose d'une connexion internet active et stable.
2. Recherchez en ligne un logiciel antivirus fiable et un antimalware adapté à votre appareil. Il existe de nombreuses options gratuites et payantes disponibles. Assurez-vous de télécharger à partir d'un site de confiance.
3. Une fois les téléchargements terminés, installez les logiciels en suivant les instructions à l'écran. Assurez-vous de sélectionner les options de configuration appropriées pour votre appareil.
4. Après l'installation, effectuez une analyse complète de votre appareil à l'aide de l'antivirus et de l'antimalware. Ces analyses permettront de détecter et de supprimer tous les virus et logiciels malveillants présents sur votre appareil.
5. Configurez les paramètres de l'antivirus et de l'antimalware en fonction de vos préférences et des recommandations du fournisseur. Assurez-vous que les mises à jour automatiques sont activées pour garantir que les programmes disposent toujours des dernières définitions de virus.
6. Effectuez régulièrement des analyses complètes de votre appareil pour assurer sa sécurité continue. Évitez également de télécharger des fichiers suspects et de cliquer sur des liens non fiables pour réduire les risques d'infection.

En suivant ces étapes, vous pouvez installer et utiliser efficacement un antivirus et un antimalware pour protéger votre appareil contre les attaques malveillantes et garantir la sécurité de vos données sensibles.