

Module : Naviguer en toute sécurité






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

1 - Introduction à la sécurité sur Internet

1/ Trois articles qui parlent de sécurité sur internet.

- Article 1 = **Cybermalveillance.gouv.fr** - *Les 10 règles de base pour la sécurité numérique*
- Article 2 = **Ministère de l'Économie et des Finances** - *Comment assurer votre sécurité numérique*
- Article 3 = **Le Monde** - *Fraude sur Internet : « Tout le monde peut, un jour ou l'autre, tomber dans le panneau »*

2 - Créer des mots de passe forts

- Accède au site de LastPass avec ce lien 
- Crée un compte en remplissant le formulaire 
- Une fois la création du compte effectuée, Lance l'installation en effectuant un clic sur le bouton prévu à cet effet 
- 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
- Il ne te reste plus qu'à te connecter 

3 - Fonctionnalité de sécurité de votre navigateur

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

 www.fessebook.com

 www.instagram.com

2/ Dans cet exercice, nous allons vérifier si les navigateurs utilisés, Chrome et Firefox

dans notre exemple, sont à jour.

● 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

● 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

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

● 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

6 - Achats en ligne sécurisés

1. Créer un dossier sur ta messagerie électronique


- Pour commencer, accède à ta messagerie électronique. ✓
- 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" ✓
- Effectuer un clic sur le bouton "Créer" pour valider l'opération ✓
- 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

8 - Principes de base de la confidentialité des médias sociaux

- 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

● Retourne dans les paramètres généraux en effectuant un clic sur la croix en haut à Gauche. 

● Dans les paramètres de Facebook tu as également un onglet “Cookies”. On t’en a parlé dans le cours précédent (Comprendre le suivi du navigateur). Maintenant que tu sais comment sont utilisées tes données, tu es capable de choisir en pleine conscience ce que tu souhaites partager. 

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

1-Si votre ordinateur est infecté par un virus, voici quelques exercices pour vérifier et rétablir la sécurité en fonction de l’appareil utilisé :

1. Exercice : Analyse avec un antivirus

- **Comment faire ?**
 - Installez un logiciel antivirus réputé (si ce n’est pas déjà fait).
 - Lancez une analyse complète du système.
 - Suivez les recommandations pour supprimer les fichiers infectés ou mettre en quarantaine les menaces détectées.

2. Exercice : Mettre à jour le système et les logiciels

- **Comment faire ?**
 - Vérifiez si votre système d’exploitation et vos logiciels sont à jour.
 - Appliquez toutes les mises à jour disponibles pour combler les éventuelles failles de sécurité.

3. Exercice : Vérification des applications et extensions

- **Comment faire ?**
 - Désinstallez les applications ou extensions que vous ne reconnaissez pas ou n’utilisez plus.
 - Réinitialisez les paramètres de votre navigateur pour supprimer d’éventuels logiciels malveillants.

2 -Installer un logiciel antivirus et antimalware pour protéger votre appareil (ordinateur ou smartphone) contre les menaces et apprendre à l'utiliser efficacement.

Étapes :

1. Choix et téléchargement

- **Comment faire ?**
 - Identifiez un antivirus réputé et compatible avec votre appareil (par exemple, Avast, Norton, Malwarebytes).
 - Accédez au site officiel du logiciel pour éviter les téléchargements frauduleux.

2. Installation

- **Comment faire ?**
 - Téléchargez le fichier d'installation depuis le site officiel.
 - Exécutez le fichier d'installation et suivez les instructions affichées.
 - Redémarrez l'appareil si demandé.

3. Configuration et analyse

- **Comment faire ?**
 - Lancez le logiciel installé.
 - Activez les fonctionnalités recommandées (protection en temps réel, mise à jour automatique, etc.).
 - Effectuez une analyse complète du système pour détecter les menaces.

4. Mise à jour régulière

- **Comment faire ?**
 - Configurez l'antivirus pour se mettre à jour automatiquement.
 - Vérifiez manuellement les mises à jour de temps en temps pour rester protégé contre les nouvelles menaces.

5. Conseils pratiques

- Supprimez ou mettez en quarantaine les fichiers infectés détectés.

- Exécutez une analyse rapide une fois par semaine et une analyse complète une fois par mois.