Naviguer en toute sécurité

1. Introduction à la sécurité sur Internet

- ***Trois articles qui parlent de sécurité sur internet*** **:**

➔ Article 1 : Economie.gouv-Comment assurer votre sécurité numérique ?
➔ Article 2 : www.wesur.fr-Piratage Informatique : Quelles protections ?
➔ Article 3 :ANSSI-DIX RÈGLES D'OR PRÉVENTIVES

2. Créer des mots de passe forts

☑ Accès au site de LastPass avec ce lien
☑ Création de compte
☑ Installation de l'extension
☑ Ajout à Chrome
☑ Accès+Connexion à LastPass :Épingler l'extension //Connexion

3. Fonctionnalité de sécurité de votre navigateur

a. Les adresses internet qui te semblent provenir de sites web malveillants

➔ **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
➔ **www.ironman.com** : Le site est notifié comme non sécurisé par le navigateur

b. Vérifier si Chrome et Firefox sont à jour :

- Pour Chrome

☑ Ouvre le menu du navigateur et accède aux "Paramètres"
☑ Clic sur la rubrique "A propose 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

- ☑ Quiz sur les 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 : HTTPS
- ➔ 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

Création registre d’achats

- ☑ Accès boîte mail
- ☑ Création libellée « ACHATS »
- ☑ Accès gestion libellés

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

- ☑ Connexion Facebook
- ☑ Accès “Paramètres et confidentialité”
- ☑ Parcours des rubriques “Confidentialité” et “Publications publiques”

- ☑ Personnalisation d'autres paramètres
- ☑ Consultation de l'onglet « Cookies » sur Facebook

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

9-1. Vérifier la sécurité des appareils :

Plusieurs points sont à vérifier pour s'assurer de la sécurité de nos machines. Généralement, ce sont les mêmes procédures sur les ordinateurs et les appareils mobiles tels que les portables et les tablettes. Ci-après des actions à mener pour vérifier si nos appareils sont sécurisés ou pas :

Observer le comportement de l'appareil : Vérifier si l'appareil concerné ne se comporte de façon inhabituelle. À savoir de gros ralentissement injustifié, des publicités intempestives, des fenêtres contextuelles suspectes, des altérations détectées sur le système (installation d'application non désirée, modification des paramètres/fichiers à notre insu), consommation inhabituelle de la batterie, de la mémoire ou de la data.

Checker s'il n'y a pas d'alerte de sécurité : Des notifications sont envoyées par les antivirus, antimalwares ou du système lui-même en cas d'infection des appareils

Effectuer une analyse anti-virus ou anti-malware, vérifier si aucune menace n'a été détectée

Surveiller les connexions réseau et les historiques de connexion, ce afin de voir si les activités correspondent aux nôtres ou pas (avec Wireshark par exemple)

9-2. Installation et utilisation d'un antivirus :

L'utilisation d'internet n'étant pas sans risque au vu du développement des malwares et de différentes formes de piratage, il est primordial de protéger nos matériels informatiques, de prévenir l'hacking.
Plusieurs mesures doivent être prises afin de maximiser la sécurité de nos données, à savoir l'installation d'un antivirus ou d'un antimalware.

➔ ***Comment fait-on pour s'y prendre ?***

Déjà, il faut préciser qu'un antivirus n'est pas un antimalware, par contre un antimalware peut inclure un antivirus. Il est ainsi mieux de s'équiper directement d'un antimalware, ses fonctionnalités étant plus complètes, donc plus efficace pour lutter contre tout type de menaces.

Dans l'idéal, il est suggéré d'opter pour les antimalwares payants, qui offrent une meilleure qualité de service et une meilleure garantie de sécurité. Il existe néanmoins des logiciels gratuits qui assurent également la protection des appareils, seulement leurs fonctionnalités sont réduites comparées à celles des versions payantes.

Selon les comparaisons fournies par différents sites, Bitdefender est l'un des meilleurs antimalware payant en 2023, voire le premier sur le podium, et Avast One, celui des logiciels gratuits.

➔ ***Comment installer un antivirus/un antimalware ?***

L'installation d'un antivirus peut varier en fonction des appareils utilisés, mais aussi selon le système d'exploitation.

Pour les ordinateurs sous Windows, on se rend directement sur le site officiel du logiciel en question pour le téléchargement, ensuite exécuter le programme et suivre les instructions.
Quant aux ordinateurs sous Mac ou Linux, on peut télécharger un antimalware, seulement ces systèmes intègrent déjà des logiciels de sécurité qui sont privilégiés. Pour installer des antimalwares tiers, ce sera la même procédure que sur Windows pour les Macs, et en fonction de la distribution Linux pour les Linux.

Concernant les appareils mobiles, cela va dépendre également du SE. Pour les Android, il suffit de se rendre sur le store du mobile pour choisir et télécharger l'antimalware, ensuite l'installer. Pour les iOS, ce sont des systèmes suffisamment sécurisés. Apple a décidé de restreindre l'utilisation d'antivirus sur les iPhone et iPad, mais comme on dit, on n'est jamais trop sécurisé ni trop prudent, il est ainsi possible de faire appel à d'autres applications de sécurité qui sont disponibles sur l'Apple Store.

En exemple, nous allons voir comment installer et utiliser Bitdefender :

- **Sur un ordinateur :**

➔ Se rendre sur le site officiel du logiciel
➔ Choisir entre les formules proposées en fonction de nos attentes
➔ Suivre les différentes étapes de l'achat
➔ Télécharger le programme
➔ Exécuter le programme d'installation puis suivre les instructions
➔ Configurer les paramètres du logiciel (Généralement, il y a déjà un guide au lancement du logiciel pour nous indiquer toutes les fonctionnalités proposées)
➔ Lancer une analyse depuis l'interface de Bitdefender
➔ Configurer les horaires d'analyse pour que ça soit automatique

- **Sur un appareil mobile :**

➔ Rechercher l'application Bitdefender sur le store du mobile
➔ Cliquer sur « Installer » ou « Obtenir »
➔ Ouvrir l'application et suivre les instructions sur l'écran
➔ Configurer l'application en suivant les étapes proposées et selon le paramétrage souhaité
➔ Lancer une première analyse
➔ Configurer les horaires d'analyse pour que ça soit automatique

Il est à noter que les fonctionnalités de Bitdefender sur les iOS sont restreintes par rapport à celles sur Android en raison des limitations imposées par Apple.