



Parcours : DISCOVERY

Module : Naviguer en toute sécurité

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

Tous vos travaux devront être déposés sur votre compte Github

Sommaire



1 - Introduction à la sécurité sur Internet

2 - Créer des mots de passe forts

3 - Fonctionnalité de sécurité de votre

navigateur 4 - Éviter le spam et le phishing

5 - Comment éviter les logiciels malveillants

6 - Achats en ligne sécurisés

7 - Comprendre le suivi du navigateur

8 - Principes de base de la confidentialité des médias

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

virus

1 - Introduction à la sécurité sur Internet

Objectif : *à la découverte de la sécurité sur internet*

1/ En naviguant sur le web, consultez 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. Saisissez le nom du site et de l'article.

- Article 1 = francais.lingolia - Réforme des retraites : la loi promulguée après six mois de conflit social
- Article 2 = maxicours - Russie : quels sont les défis économiques de Vladimir Poutine ?
- Article 3 = wikihow - Marvel : un nouvel univers cinématographique en préparation



2 - Créer des mots de passe forts

Objectif : *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.



(case à cocher)

- ☒ Accède au site de LastPass avec [ce lien](#)
- ☒ 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
 - Exemple de mot de passe maître : c3c!3s!l3M0!2P@SS3 (Ceci est le mot de passe, en remplaçant le "e" par "3" le "i", "t" par "!", "a" par "@" et les premières lettres en minuscules puis majuscules à partir de "mot")
 - Tu peux également générer un mot de passe maître, mais pense à l'écrire dans un endroit sûr pour pouvoir l'utiliser lorsque tu en as besoin
- ☒ 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
 - (1) En haut à droite du navigateur, clic sur le logo "Extensions"

 - (2) 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

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.marvel.com~~
- ☐ www.dccomics.com
- ☐ www.ironman.com
- ☒ ~~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 ce faire, suis les étapes suivantes.
(case à cocher)**

- ☒ Pour Chrome
 - Ouvre le menu du navigateur  et accède aux "Paramètres"
 - Clic sur la rubrique "À 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

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
4 - Spam et Phishing



suis les étapes qui y sont décrites : Exercice



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 <https://www.lemonde.fr/>
 - **Indicateur de sécurité**
 - ☒ HTTPS
 - ☐ HTTPS Not secure
 - ☐ Not secure
 - **Analyse Google**
 - ☒ Aucun contenu suspect
 - ☒ Vérifier un URL en particulier

- Site n°2 <https://www.torrent9.fm/>
 - **Indicateur de sécurité**
 - ☒ ■ HTTPS
 - ☐ ■ HTTPS Not secure
 - ☐ ■ Not secure
 - **Analyse Google**
 - ☒ ■ Aucun contenu suspect
 - ☒ ■ Vérifier un URL en particulier

<https://www.torrent9.fm/torrent/102811/konosuba-the-movie-god-s-blessing-on-this-wonderful-world-legend-of-crimson-french-webrip-x264-2023>

- Site n°3 http://w3.uqo.ca/iglewski/ens/inf1493/src/html2/html2_http.php
 - **Indicateur de sécurité**
 - ☐ HTTPS
 - ☐ HTTPS Not secure
 - ☒ Not secure
 - **Analyse Google**
 - ☒ Aucun contenu suspect
 - ☒ Vérifier un URL en particulier

http://w3.uqo.ca/iglewski/ens/inf1493/src/html2/html2_http.php

- Site n°4 <http://unblog.fr/>
 - **Indicateur de sécurité**
 - ☐ HTTPS
 - ☐ HTTPS Not secure
 - ☒ Not secure
 - **Analyse Google**
 - ☒ Aucun contenu suspect
 - ☒ Vérifier un URL en particulier



<http://playitagain.unblog.fr/2023/03/30/le-bossu-de-philippe-de-broca-1997/>

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. (case à cocher)

- ☒ 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

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*

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. (case à cocher)

- ☒ 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
 - ☒ Retourne dans les paramètres généraux en effectuant un clic sur la croix en haut à gauche. Tu peux continuer à explorer les rubriques pour personnaliser tes paramètres. On ne peut pas te dire ce que tu dois faire. C'est à toi de choisir les informations que tu souhaites partager et celles que tu veux garder privées. Voici tout de même quelques conseils :
 - Si tu utilises ton compte Facebook uniquement pour communiquer avec tes amis, règle les paramètres en conséquence en choisissant une visibilité "Amis" ou "Amis de leurs amis".
 - Beaucoup de personnes utilisent Facebook en mêlant réseau professionnel et réseau personnel. Il n'y a pas vraiment de contre-indication, mais on te conseille tout de même de ne pas trop mélanger les deux. Il existe LinkedIn pour utiliser un média social pour le réseau professionnel
 - Pour limiter les haters et les commentaires malveillants, tu peux restreindre les commentaires de tes publications. Ça se passe dans l'onglet "Publications publiques"
 - ☒ 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

Objectif :

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

- Vérification de la sécurité sur un ordinateur :
 - Ouvrez votre navigateur internet et rendez-vous sur le site WebRTC Leak Test (<https://www.browsersleaks.com/webrtc>).
 - Cliquez sur le bouton "Start" pour lancer le test de fuite WebRTC.
 - Si le test indique que votre adresse IP est visible ou si le test échoue, cela signifie que votre navigateur n'est pas sécurisé. Pour améliorer la sécurité, vous pouvez utiliser un VPN ou configurer manuellement les paramètres de votre navigateur.
- Vérification de la sécurité sur un smartphone :
 - Téléchargez l'application "Fing" sur l'App Store ou Google Play Store.
 - Lancez l'application et cliquez sur "Scan" pour rechercher les appareils



connectés à votre réseau Wi-Fi.

- Si vous voyez des appareils inconnus sur la liste, cela peut indiquer que votre réseau Wi-Fi est compromis. Pour améliorer la sécurité, vous pouvez changer votre mot de passe Wi-Fi ou utiliser un réseau privé virtuel (VPN).
- Vérification de la sécurité sur un routeur :
 - Connectez-vous à votre routeur en entrant l'adresse IP de votre routeur dans votre navigateur web. Pour connaître l'adresse IP de votre routeur, vous pouvez consulter le manuel d'utilisation ou contacter votre fournisseur d'accès Internet.
 - Accédez à la section "Sécurité" ou "Firewall" de votre routeur et vérifiez que les paramètres de sécurité sont configurés de manière appropriée. Assurez-vous que le pare-feu est activé et que les ports non utilisés sont fermés.
 - Si votre routeur prend en charge le chiffrement WPA2, activez-le pour sécuriser votre réseau Wi-Fi.

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

Objectif : Installer et utiliser un antivirus + antimalware pour protéger votre ordinateur.

Matériel requis : Un ordinateur et une connexion Internet.

Étapes :

1. Recherchez et téléchargez un logiciel antivirus + antimalware fiable. Des options populaires incluent McAfee, Norton, Kaspersky et Bitdefender.
2. Ouvrez le fichier d'installation du logiciel que vous avez téléchargé.
3. Suivez les instructions d'installation pour installer le logiciel sur votre ordinateur.
4. Une fois l'installation terminée, ouvrez le programme antivirus + antimalware et effectuez une analyse complète de votre ordinateur.
5. Si le programme détecte des virus ou des logiciels malveillants, suivez les instructions pour les supprimer.
6. Assurez-vous que le programme antivirus + antimalware est mis à jour régulièrement en activant les mises à jour automatiques.
7. Planifiez des analyses régulières de votre ordinateur pour détecter tout nouveau virus ou logiciel malveillant.
8. Enfin, évitez de télécharger des fichiers ou des programmes provenant de sources non fiables et évitez de cliquer sur des liens suspects dans les e-mails ou sur les



réseaux sociaux.