

PARCOURS : DISCOVERY

MODULE : Naviguer en toute sécurité

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

1-Introduction à la sécurité sur internet

Trois articles qui parlent de sécurité sur internet

- **Article 1=** cyber.gc - Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information
<https://www.cyber.gc.ca/fr/orientation/les-10-mesures-de-securite-des-ti-visant-protoger-les-reseaux-internet-et-0>
- **Article 2=** CNIL - Sécurité : Sécuriser les sites web
<https://www.cnil.fr/fr/securite-securiser-les-sites-web>
- **Article 3=** cybermalveillance- 10 regles de base pour la sécurité numérique
<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/les-10-regles-de-base-pour-la-securite-numerique>

2- Créer mot de passe fort

- Création de compte : Succès
- Installation de Lastpass : Succès
- Epinglage de l'extension : Succès
- Essaie pour ajout de compte manuel e, accédant au coffre-fort : Succès

3- Fonctionnalité de sécurité de votre navigateur

- Exercice d'identification des adresses internet qui semblent provenir de sites web malveillants

☒ www.morvel.com

☐ www.dccomics.com

☐ www.ironman.com

☒ www.fessebook.com

☒ www.instagram.com

Toutes les adresses identifiées sont tous des dérivés des sites web connus, obtenu juste avec quelque modification des caractères seulement. Ainsi il faut être toujours attentif à ces petits détails.

- Exercices de vérifications si les navigateurs utilisés : Les paramètres des navigateurs usuels (Chrome et Firefox) sont réglés par défaut pour effectuer des mises à jour automatique.

4-Eviter le spam et le phishing



- Exercices pour déceler les erreurs dans les messages cachant une action malveillante en arrière-plan. D'après le test, du même principe que les exercices précédents, il faut être vigilant aux adresses emails, les détails inhabituelles, les messages frauduleuses et aux liens rédigés vers des sites malveillants.



5-Comment éviter les logiciels malveillants

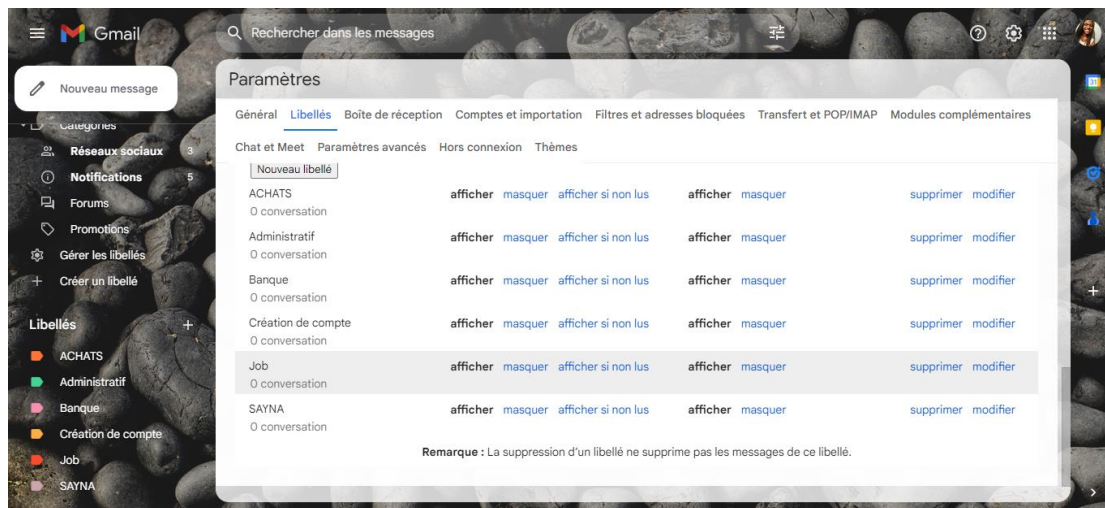
Il faut être vigilant aux adresses emails, les détails Exercices pour repérer les indicateurs de sécurité (Cadenas sécurisé, cadenas non sécurisé, ou un message non sécurisé) ; et ensuite vérifier l'état du site avec transparence des informations (<https://transparencyreport.google.com/>)

Sites	Indicateur de sécurité	Analyse Google
Vostfree	 https://vostfree.tv	Aucun contenu suspect détecté

Tv5monde	 https://www.tv5monde.com	Aucun contenu suspect détecté
Baidu	 Non sécurisé www.baidu.com	Vérifier une URL en particulier

6-Achats en ligne sécurisés

Création de dossier sur le messagerie électronique avec un exemple d'organisation de libelle



7-Comprendre le suivi du navigateur

8-Principes de base de la confidentialité des médias sociaux

Exercice portant sur l'internet de base, gestion des paramètres de confidentialités sur les réseaux sociaux : fait avec succès

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

Exercice 1 :

Pour le cas de Windows 10, comme mon ordinateur, voici un exemple des exercices à faire pour vérifier l'état de sécurité :

- **Vérifier l'état de protection antivirus (barre des tâches) ; comment faire :**

Cible : Barre des tâches->Zone de notifications->Centre de sécurité

1-Cliquez sur l'icône représentée par une petite flèche montante, sur la barre des tâches, afin d'ouvrir la zone de notifications ;

2-aller dans centre de sécurité

3-vérifiez l'état actuel de la protection antivirus de votre ordinateur. Si Windows Defender est activé, vous devriez obtenir ceci (voir capture écran ci-dessous).



Si Windows Defender, l'antivirus intégré de Windows, n'est pas activé mais que votre ordinateur est protégé par un autre antivirus, le Centre de sécurité Windows Defender vous l'indiquera.

➤ **Vérifier la protection antivirus (panneau de configuration) : comment faire :**

Cible : Panneau de configuration->Système et sécurité->Sécurité et maintenance

1-Ouvrez le panneau de configuration (en tapant « panneau de configuration » dans la barre des tâches), ouvrez l'application,

2- cliquez sur « Système et sécurité »

3-Choisir sécurité et maintenance, déroulez l'onglet Sécurité en cliquant sur la flèche située à droite.

Si un antivirus est actif sur votre ordinateur, et lequel précisément. Pour mon cas, c'est Windows Defender qui est actif (car il fait bien le travail !). Si le pare-feu et l'antivirus sont actifs, tout va bien.

Exercice 2 : un exercice pour installer et utiliser un antivirus + antimalware (Pour mon cas, j'ai essayer bitdefender

➤ **Télécharger et installer**

1. Rendez-vous sur le site officiel de Bitdefender (www.bitdefender.com) pour télécharger le programme d'installation de Bitdefender. Assurez-vous de télécharger la version compatible avec Windows 10.
2. Une fois le fichier d'installation téléchargé, localisez-le sur votre ordinateur (par défaut, il se trouve dans le dossier "Téléchargements").
3. Double-cliquez sur le fichier d'installation pour le lancer. Vous pouvez être invité à autoriser les modifications apportées à votre système, cliquez sur "Oui" pour continuer.

4. L'assistant d'installation de Bitdefender s'ouvrira. Lisez attentivement les conditions d'utilisation et la politique de confidentialité, puis cliquez sur "Accepter et installer" pour poursuivre.
5. Le programme d'installation de Bitdefender commencera à télécharger les fichiers nécessaires à l'installation. Attendez que le processus de téléchargement soit terminé.
6. Une fois les fichiers téléchargés, l'installation proprement dite commencera. Suivez les instructions à l'écran pour configurer Bitdefender selon vos préférences. Vous pouvez choisir entre une installation standard ou personnalisée, en fonction des fonctionnalités que vous souhaitez activer.
7. Pendant l'installation, Bitdefender effectuera également une analyse de sécurité initiale de votre système pour détecter d'éventuelles menaces.
8. Une fois l'installation terminée, vous serez invité à créer un compte Bitdefender ou à vous connecter avec un compte existant. Si vous ne souhaitez pas créer de compte, vous pouvez passer cette étape, mais cela limitera certaines fonctionnalités du logiciel.
9. Une fois que vous avez terminé toutes les étapes de configuration, Bitdefender sera installé sur votre système Windows 10. Assurez-vous que le programme est à jour en exécutant les mises à jour disponibles.
10. Enfin, redémarrez votre ordinateur pour que les modifications prennent effet et pour que Bitdefender soit pleinement opérationnel.

➤ **Mode d'utilisation**

1. Interface Bitdefender : Ouvrez l'interface Bitdefender en double-cliquant sur l'icône Bitdefender dans la barre des tâches de votre ordinateur. L'interface principale affiche l'état de sécurité de votre système et fournit un accès aux différentes fonctionnalités de Bitdefender.
2. Analyse de votre système : L'une des premières choses à faire est d'effectuer une analyse complète de votre système pour détecter les éventuelles menaces. Dans l'interface Bitdefender, recherchez l'option "Analyse" ou "Analyser maintenant" et sélectionnez l'option d'analyse complète. Bitdefender examinera tous les fichiers et les applications de votre système à la recherche de logiciels malveillants.
3. Mises à jour de la base de données : Assurez-vous que Bitdefender est à jour en termes de signatures de virus et de bases de données de détection des menaces. Dans l'interface Bitdefender, recherchez les options de mise à jour ou de mise à jour des définitions de virus et assurez-vous de les exécuter régulièrement pour obtenir les dernières protections.
4. Planification des analyses : Vous pouvez configurer Bitdefender pour effectuer des analyses automatiques selon un planning prédéfini. Cela garantit que votre système est régulièrement scanné pour détecter les menaces. Recherchez les options de planification dans l'interface Bitdefender et configurez des analyses périodiques.
5. Protection en temps réel : Bitdefender offre une protection en temps réel pour surveiller activement votre système et bloquer les menaces potentielles. Assurez-vous que cette fonctionnalité est activée dans l'interface Bitdefender. Elle protégera votre système en temps réel contre les virus, les logiciels malveillants et autres menaces.
6. Paramètres de confidentialité : Bitdefender propose également des fonctionnalités de protection de la confidentialité, telles que la protection du navigateur, le contrôle parental et le pare-feu. Explorez les différentes options de confidentialité disponibles dans l'interface Bitdefender et configurez-les en fonction de vos besoins.

7. Analyse des fichiers et des dossiers : Si vous souhaitez analyser des fichiers ou des dossiers spécifiques, vous pouvez utiliser l'option d'analyse personnalisée de Bitdefender. Cela vous permet de sélectionner les fichiers ou les dossiers à analyser.
8. Rapports et historique des activités : Bitdefender enregistre les activités de sécurité et les événements importants dans l'interface. Vous pouvez consulter les rapports et l'historique des activités pour obtenir des informations sur les menaces détectées, les mises à jour effectuées et d'autres événements liés à la sécurité.