

PROJET- Un peu plus de sécurité on n'en a jamais assez

1-Introduction à la sécurité sur l'internet	
-Les tres articles qui parle à la sécurité sur l'internet	
Nom du site	Nom de l'artcle
cybermalveillance.gouv.f	Black Friday, fêtes de fin d'année : 7 conseils pour éviter les cyber-arnaques
f-secure	Avez-vous besoin d'un VPN pour iPhone ?
kaspersky	Sécurité Internet : Qu'est-ce que c'est et comment vous protéger en ligne ?
2-Créer des mots de passe forts	

3-Fonctionnalité de sécurité de votre navigateur

The screenshot shows the Google Chrome settings interface. On the left, the 'Paramètres' (Settings) menu is open, with 'Confidentialité et sécurité' (Privacy and Security) selected. The main content area shows the 'À propos de Chrome' (About Chrome) section, which includes the Google Chrome logo, the text 'Chrome est à jour' (Chrome is up to date), the version number 'Version 122.0.6261.112 (Build officiel) (64 bits)', and links to 'Obtenir de l'aide avec Chrome' (Get help with Chrome), 'Signaler un problème' (Report a problem), and 'Règles de confidentialité' (Privacy rules).

4- Eviter le spam et le phishing

8 / 8

Bon travail, Moustapha Souane !
Vous avez obtenu un score de 7/8.

Plus vous vous entraînez, mieux vous saurez identifier les pièges et vous protéger des tentatives d'hameçonnage.

Quelques mesures très simples à mettre en place peuvent également améliorer la protection de vos comptes en ligne. Pour plus d'informations, consultez la page [g.co/25V](#).

Partager le questionnaire :

f

t

RECOMMENCER LE QUESTIONNAIRE



Activer Windows

Accédez aux paramètres pour activer Windows.

Confidentialité / Conditions / Commentaires

JIGSAW | Google

5-Comment éviter les logiciels malveillants

Check site status

https://visit-yvoire.com/

Q

Current status

✓

No unsafe content found

Site info

This info was last updated on Feb 13, 2024.

Site safety can change over time. Check back for updates.

Check site status

https://support.harver.com

Q

Current status

✓

No unsafe content found

Site info

This info was last updated on Mar 7, 2024.

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

Exercices pour vérifier la sécurité de votre appareil

1. Vérifiez les mises à jour:

Assurez-vous que votre système d'exploitation et vos applications sont à jour. Les mises à jour incluent souvent des correctifs de sécurité importants qui peuvent vous protéger des dernières menaces.

Sur Windows:

Ouvrez le menu Démarrer et sélectionnez "Paramètres".

Cliquez sur "Mise à jour et sécurité".

Cliquez sur "Windows Update" et vérifiez les mises à jour disponibles.

Sur Mac:

Cliquez sur l'icône Apple dans le coin supérieur gauche de l'écran.

Sélectionnez "Préférences Système".

Cliquez sur "Mise à jour de logiciels".

Vérifiez les mises à jour disponibles et installez-les.

Sur Android:

Ouvrez l'application "Paramètres".

Sélectionnez "Système".

Sélectionnez "Mises à jour du système".

Vérifiez les mises à jour disponibles et installez-les.

Sur iOS:

Ouvrez l'application "Réglages".

Sélectionnez "Général".

Sélectionnez "Mise à jour logicielle".

Vérifiez les mises à jour disponibles et installez-les.

2. Analysez votre appareil avec un antivirus:

Installez un antivirus réputé et effectuez une analyse complète de votre appareil. Cela permettra de détecter d'éventuels logiciels malveillants qui pourraient être présents.

Exemples d'antivirus:

Avast

Bitdefender

Kaspersky

Malwarebytes

3. Vérifiez vos mots de passe:

Assurez-vous que vos mots de passe sont forts et uniques. Un mot de passe fort doit contenir au moins 12 caractères, une combinaison de lettres majuscules et minuscules, de chiffres et de symboles.

Conseils pour créer des mots de passe forts:

Utilisez une phrase de passe plutôt qu'un seul mot.
N'utilisez pas d'informations personnelles comme votre nom ou votre date de naissance.
Ne réutilisez pas le même mot de passe pour plusieurs comptes.
Utilisez un gestionnaire de mots de passe pour stocker vos mots de passe en toute sécurité.
4. Activez l'authentification multifacteur:
L'authentification multifacteur (MFA) ajoute une couche de sécurité supplémentaire à vos comptes en vous demandant de fournir une information supplémentaire en plus de votre mot de passe, comme un code temporaire envoyé à votre téléphone portable.
Activez la MFA pour tous vos comptes importants, tels que vos comptes de messagerie, vos réseaux sociaux et vos comptes bancaires.
5. Soyez prudent avec les liens et les pièces jointes:
Ne cliquez pas sur les liens provenant de sources inconnues ou suspectes.
Ne ouvrez pas les pièces jointes provenant de personnes que vous ne connaissez pas.
Si vous n'êtes pas sûr de la légitimité d'un lien ou d'une pièce jointe, contactez l'expéditeur pour le vérifier.
6. Sauvegardez vos données régulièrement:
En cas de cyberattaque ou de perte de votre appareil, vous pourrez restaurer vos données si vous les avez sauvegardées régulièrement.
Plusieurs options de sauvegarde existent:
Sauvegarde sur un disque dur externe
Sauvegarde dans le cloud
Sauvegarde sur un serveur local
En suivant ces conseils, vous pouvez améliorer la sécurité de votre appareil et vous protéger des cyberattaques.
Voici les étapes générales pour installer et utiliser un antivirus ou antimalware :
1. Choisir un antivirus ou antimalware:
Il existe de nombreux antivirus et antimalware disponibles sur le marché. Vous pouvez choisir un antivirus gratuit ou payant, en fonction de vos besoins et de votre budget.
Voici quelques exemples d'antivirus populaires :
Avast
Bitdefender

Kaspersky
Malwarebytes
2. Télécharger et installer l'antivirus:
Téléchargez l'antivirus depuis le site web officiel de l'éditeur.
Exécutez le fichier d'installation et suivez les instructions à l'écran.
Redémarrez votre appareil après l'installation.
3. Mettre à jour l'antivirus:
Il est important de maintenir votre antivirus à jour pour qu'il puisse détecter les dernières menaces.
La plupart des antivirus se mettent à jour automatiquement. Vous pouvez également vérifier manuellement les mises à jour et les installer.
4. Effectuer une analyse de votre appareil:
Lancez une analyse complète de votre appareil pour détecter d'éventuels logiciels malveillants.
Vous pouvez également programmer des analyses automatiques régulières.
5. Supprimer les logiciels malveillants:
Si l'antivirus détecte des logiciels malveillants, il vous proposera de les supprimer.
Suivez les instructions à l'écran pour supprimer les logiciels malveillants.
6. Gérer les exceptions:
Vous pouvez exclure certains fichiers ou dossiers de l'analyse antivirus.
Cela peut être utile si vous avez des fichiers qui sont faussement détectés comme étant malveillants.
7. Désactiver l'antivirus temporairement:
Dans certains cas, vous pouvez avoir besoin de désactiver l'antivirus temporairement.
Par exemple, si vous installez un logiciel qui est détecté comme étant malveillant par l'antivirus.
N'oubliez pas de réactiver l'antivirus dès que vous n'en avez plus besoin.
Voici quelques conseils supplémentaires pour utiliser un antivirus ou antimalware :
N'utilisez qu'un seul antivirus à la fois. L'utilisation de plusieurs antivirus peut entraîner des conflits et des problèmes de performance.
Ne désactivez pas l'antivirus en permanence. Cela peut laisser votre appareil vulnérable aux attaques.
Soyez prudent avec les liens et les pièces jointes suspectes. Ne cliquez pas sur les liens provenant de sources inconnues et n'ouvrez pas les pièces jointes provenant de personnes que vous ne connaissez pas.
Mettez à jour votre système d'exploitation et vos logiciels régulièrement. Les mises à jour de sécurité

peuvent vous protéger des dernières menaces.
En suivant ces conseils, vous pouvez utiliser un antivirus ou antimalware pour protéger votre appareil contre les logiciels malveillants.
Voici quelques liens vers des tutoriels spécifiques pour installer et utiliser un antivirus ou antimalware sur différents appareils :
Windows:
Installer un antivirus sur Windows 10:
Utiliser l'antivirus intégré à Windows 10:
Mac:
Installer un antivirus sur Mac:
Utiliser l'antivirus intégré à macOS: https://support.apple.com/fr-fr/HT201268
Android:
Installer un antivirus sur Android:
Utiliser l'antivirus intégré à Android: