

Question 1)

Article 1 = ANSSI - Dix règles de base

Article 2 = Economie.gouv - Comment assurer votre sécurité numérique

Article 3 = Site W - Naviguez en toute sécurité sur Internet

Question 2)

LastPass

Question 3)

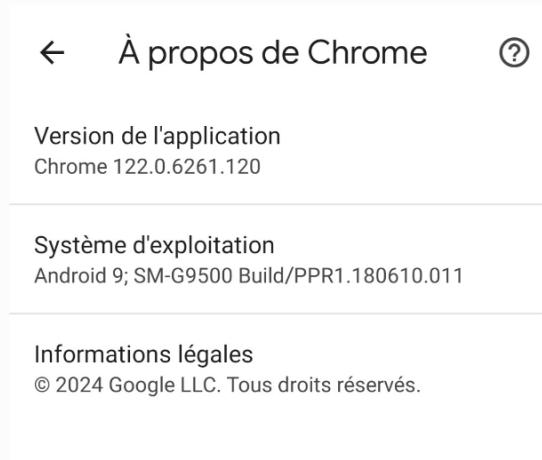
1) les adresses internet qui semblent malveillants :

www.morvel.com pour marvel

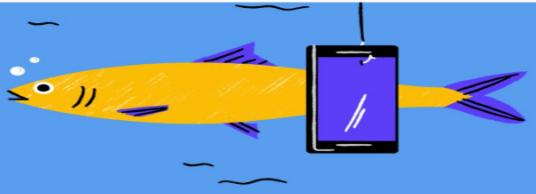
www.fessebook.com pour facebook

www.instagam.com pour Instagram

2)



Question 4)



Bon travail,
kora !
Vous avez obtenu
un score de 5/8.

Plus vous vous entraînerez, 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/2SV.

Partager le questionnaire :



Question 5)

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)

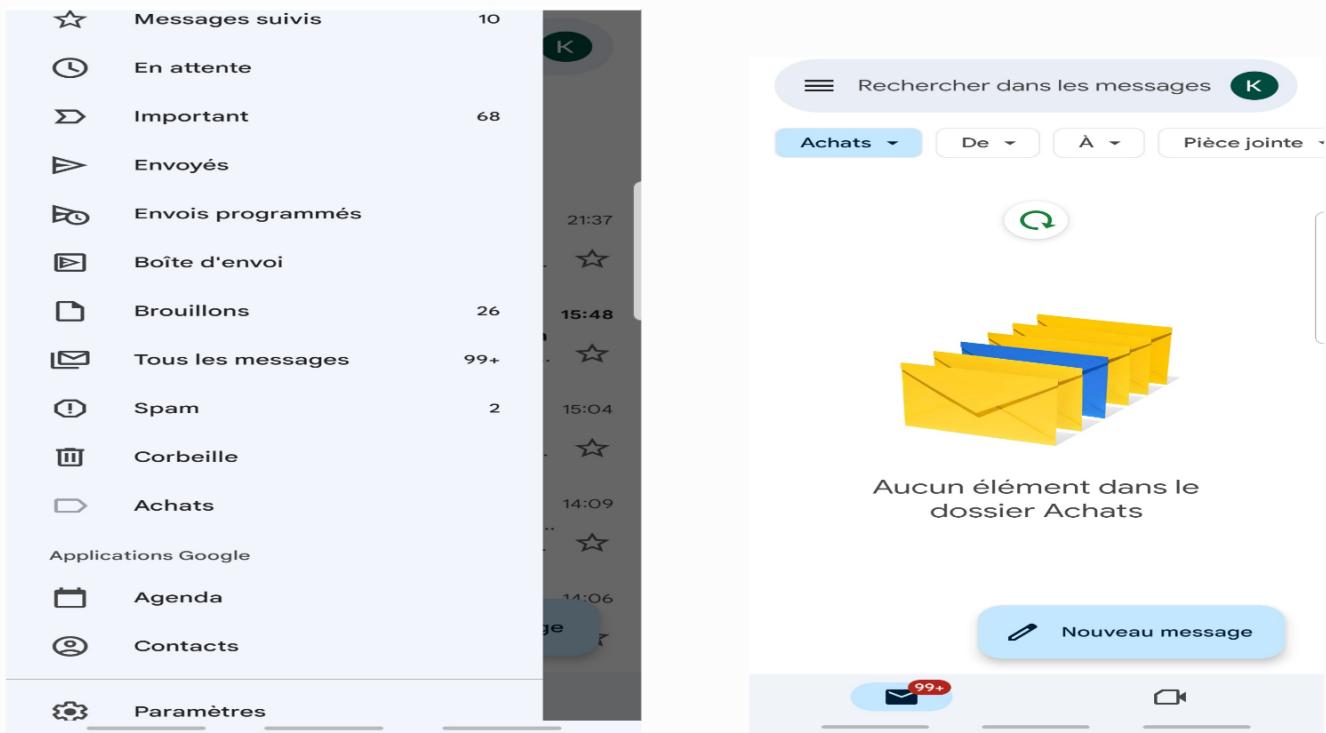
Site n°3

Indicateur de sécurité (Not secure)

Analyse Google (Vérifier un URL en particulier)

Site web consulté (<https://whynohttps.com/>)

Question 6)



Question 7)

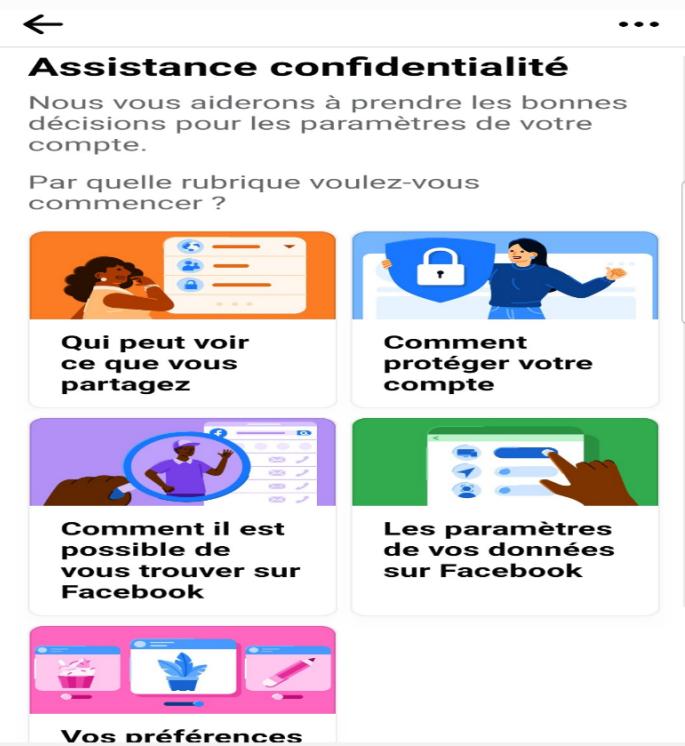
La gestion des cookies

Les cookies sont des petits fichiers textes qui peuvent être utilisés par les sites web pour rendre l'expérience utilisateur plus efficace. La loi stipule que nous ne pouvons stocker des cookies sur votre appareil que s'ils sont strictement nécessaires au fonctionnement de ce site. Pour tous les autres types de cookies, nous avons besoin de votre permission. Ce site utilise différents types de cookies. Certains cookies sont placés par les services tiers qui apparaissent sur nos pages. À tout moment, vous pouvez modifier ou retirer votre consentement dès la Déclaration relative aux cookies sur notre site web.

L'utilisation de la navigation privée

La navigation privée vise à effacer les traces locales des sites Web que vous avez visités, des recherches que vous

avez effectuées, des formulaires en ligne que vous avez soumis, etc. Elle est destinée à masquer votre activité aux autres personnes ayant accès à l'ordinateur personnel.



Alors, comment utiliser la navigation privée (le mode Incognito) ? Les différents navigateurs ont des noms différents pour la navigation privée. Par exemple, Mozilla Firefox, Opera et Apple Safari parlent de « navigation privée », tandis que Google Chrome l'appelle « Incognito » et Microsoft Edge « InPrivate ». Voici comment vous pouvez activer la navigation privée dans un des principaux navigateurs :

Navigation privée dans Chrome

Le mode Incognito de Google Chrome n'enregistre pas l'historique de votre navigation, les cookies, les données du site, ni les informations que vous saisissez dans les formulaires. Il conservera les fichiers que vous téléchargez ainsi que vos favoris.

Pour activer le mode Incognito sur votre ordinateur, Android, iPhone ou iPad, procédez comme suit :

- Ouvrez Chrome.
- Cliquez sur le menu Outils (trois points verticaux sur Mac et sur Windows) dans le coin supérieur droit.
- Choisissez « Nouvelle fenêtre de navigation privée » pour ouvrir une nouvelle fenêtre de navigation privée.

Vous pouvez aussi utiliser un raccourci clavier en appuyant sur **Ctrl+Maj+N** pour ouvrir une nouvelle fenêtre de navigation privée. Vous pouvez reconnaître la nouvelle fenêtre de navigation privée à son fond sombre et à une icône d'espion stylisée à gauche du menu à trois points. Chrome rappelle également aux utilisateurs ce que le mode Incognito fait et ne fait pas chaque fois qu'une nouvelle fenêtre est ouverte.

Question 8)

pour aller plus loin : site consulté

Voici les quelques conseils que YOURinfoGRAPHIC nous propose d'appliquer pour être en sécurité sur les médias sociaux :

1. Créer son anonymat

Créez une nouvelle adresse email. Ne pas avoir de caractéristiques identifiables (telles que nom et prénom, année de naissance, ou un code postal) dans l'adresse e-mail ou les paramètres de profil.

Créez des pages sur les réseaux sociaux en utilisant cette nouvelle adresse e-mail et ajouter seulement ceux en qui vous avez vraiment confiance. Évitez également l'identification des photos.



2. Utiliser des mots de passe forts

Mettez à jour vos mots de passe pour tous les comptes que



vous avez, et assurez-vous d'utiliser des mots de passe forts sur tous les nouveaux comptes que vous créez. Utilisez des



lettres (au moins une MAJUSCULE) et des chiffres, et envisagez également d'utiliser des caractères spéciaux (! @ # \$ %).



Ne pas utiliser un mot de passe que l'on peut deviner.

3. Augmenter et améliorer ses paramètres de confidentialité

Chaque réseau social possède une option pour « les paramètres de confidentialité » pour vous permettre d'augmenter la sécurité de votre compte, de sorte à ce que seuls vos amis ou des listes spécifiques de personnes

peuvent voir vos messages et informations privées. Ne laissez jamais les paramètres par défaut

Question 9)

1) Verification de la sécurité des appareils

Gérer vos paramètres de sécurité

- Ouvrez l'application Paramètres de votre téléphone.
- Appuyez sur Sécurité.
- L'état de sécurité de votre appareil et de votre compte Google s'affiche en haut de l'écran. Vous verrez apparaître un message d'avertissement si des actions importantes sont nécessaires pour sécuriser votre appareil ou vos comptes.

Comprendre l'état de la sécurité

Aucun problème détecté : votre appareil ou votre compte Google ne présentent aucun problème de sécurité.

La sécurité peut être améliorée : des recommandations de sécurité sont disponibles.

La sécurité peut être compromise : veuillez consulter les recommandations de sécurité et prendre les mesures nécessaires pour sécuriser votre compte ou votre appareil.

La sécurité est compromise : des problèmes de sécurité

critiques requièrent votre attention. Veuillez consulter les recommandations de sécurité et prendre les mesures nécessaires pour sécuriser votre compte ou votre appareil.

2) Installer et utiliser un antivirus et une antimalware

Pour PC :

Au moment d'installer votre logiciel antivirus, n'oubliez pas de mettre en place **un scan de vos fichiers** sur les supports amovibles et le disque dur. Ceci permettra d'identifier un logiciel malveillant.

En premier lieu, vous devez **choisir l'antivirus qui convient le mieux à vos besoins**. Il y a plusieurs options, dont **Bitdefender** qui est l'un des meilleurs logiciels sur le marché.

Il suffit donc de **télécharger le fichier d'installation**, souvent en format archive, que vous allez extraire et installer sur votre PC. La deuxième étape consiste à effectuer une mise à jour pour définir le programme à la dernière version.

pour téléphone :

Avant tout, il convient de rappeler qu'il y a des antivirus payants et des antivirus gratuits. Pour ce qui en est de l'installation, i n'y a rien de plus compliqué. Installer un antivirus sur un téléphone portable est assez simple.

La première chose à faire est alors de **vous rendre dans la boutique numérique de votre mobile**. Pour ceux qui utilisent un téléphone portable Android, il suffit d'aller sur **Play Store** et rechercher un programme antivirus gratuit. Si votre appareil fonctionne sur iOS, il faut se rendre sur **App Store**

L'utilisation d'un antivirus

Avec un logiciel antivirus, les logiciels malveillants et les virus stockés sur votre disque dur pourront être détectés. Mais des solutions plus complètes vous proposent en plus un **pare-feu** efficace pour protéger votre ordinateur d'attaques. Certains antivirus peuvent également scanner votre mémoire vive, vos e-mails entrants et sortants ainsi que votre secteur d'amorçage. Ces différentes options permettent ainsi de mieux écarter les dangers et risques.

Autre point important : votre logiciel antivirus doit être en mesure **de placer en quarantaine** les fichiers qui pourraient être touchés et endommagés par un virus. Mieux vaut être prudent !

<https://whynohttps.com/>

<https://vostfree.tv/>

<https://www.tv5monde.com/>

<https://www.baidu.com/>

