

1 - Introduction à la sécurité sur Internet

1/

- Article 1 = internetetsecurite.ch - La protection internet est très importante !
- Article 2 = interieur.gouv.fr - L'hameçonnage
- Article 3 = sfrbusiness - Piratage informatique : comment les hackers ciblent les collaborateurs ?

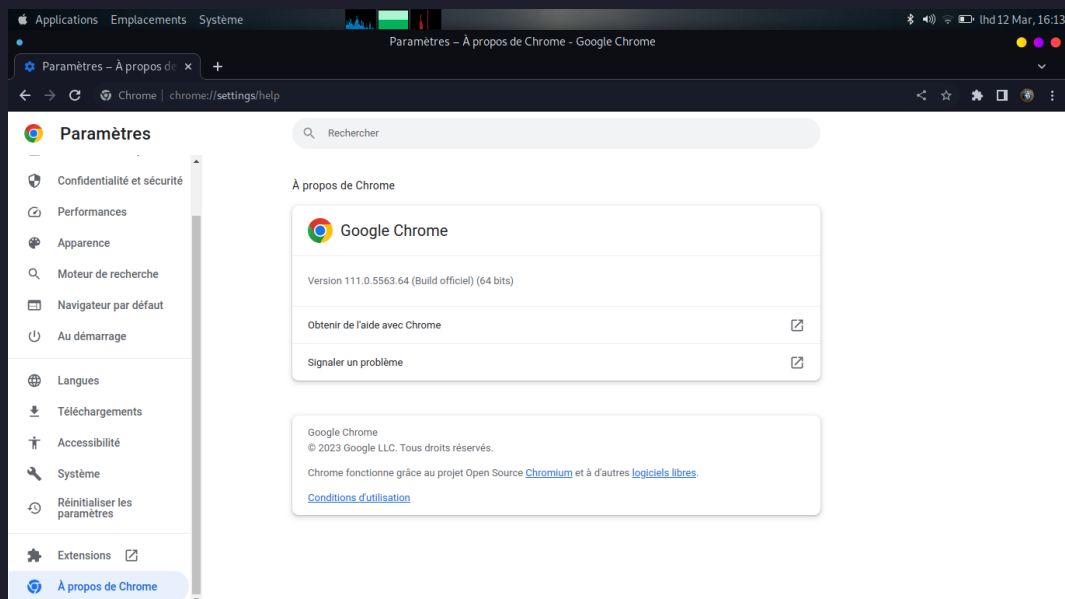
2 - Créer des mots de passe forts

3 - Fonctionnalité de sécurité de votre navigateur

1/Les sites web qui semblent être malveillants sont :

- www.morvel.com
- www.fessebook.com
- www.instagram.com

2/



4 - Éviter le spam et le phishing

Français

Savez-vous reconnaître une tentative d'hameçonnage ?

Il peut être plus difficile qu'il n'y paraît de repérer une tentative d'hameçonnage. Lors d'une tentative d'hameçonnage, une personne malveillante essaye de vous amener à communiquer des informations personnelles se faisant passer pour quelqu'un que vous connaissez. Arrivez-vous à distinguer le vrai du faux ?

RÉPONDRE AU QUESTIONNAIRE



 JIGSAW | Google

Confidentialité / Conditions / Commentaires

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

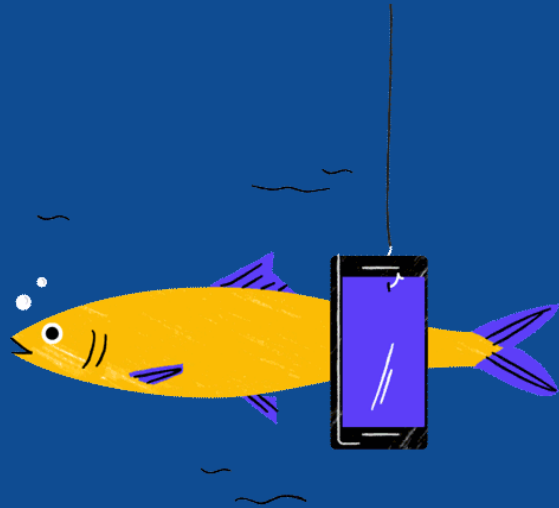
Plus vous vous entraînez, mieux vous saurez identifier les
pièges et vous protéger des tentatives d'hameçonnage.

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/2SV.

Partager le questionnaire :



RECOMMENCER LE QUESTIONNAIRE



JIGSAW | Google

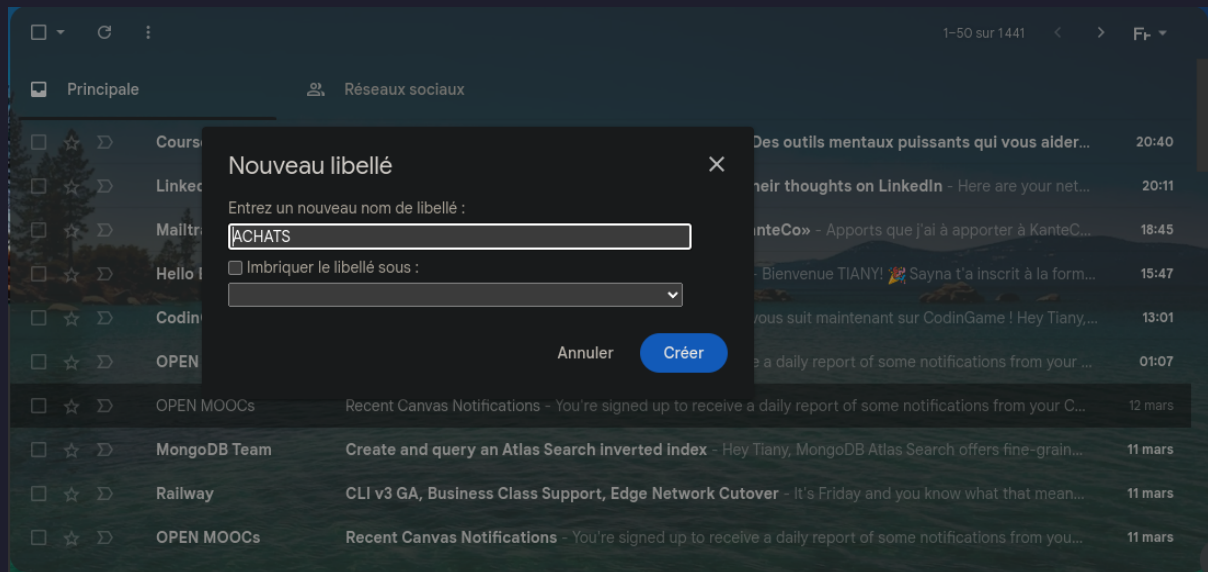
[Confidentialité](#) / [Conditions](#) / [Commentaires](#)

5 - Comment éviter les logiciels malveillants

3/

- 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

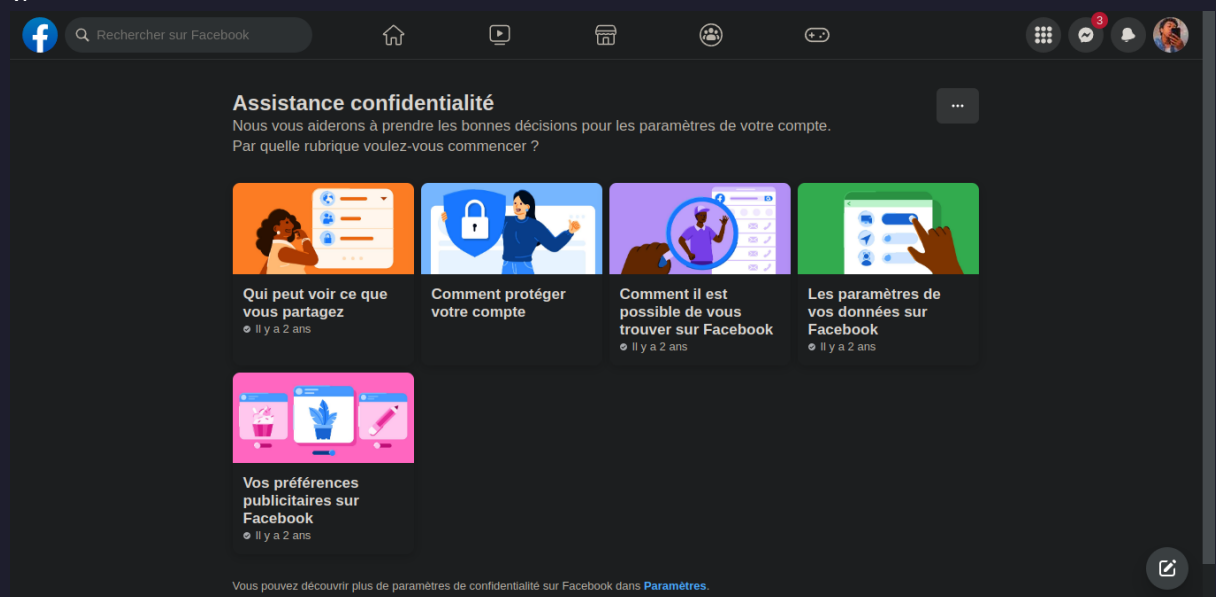
6 - Achats en ligne sécurisés



7 - Comprendre le suivi du navigateur

8 - Principes de base de la confidentialité des médias sociaux

1/



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

1/

Voici quelques mesures à prendre pour vérifier la sécurité en fonction de l'appareil utilisé :

1. Ordinateur de bureau ou portable :

- Assurez-vous que votre système d'exploitation est à jour avec les derniers correctifs de sécurité.
- Utilisez un logiciel antivirus et antimalware pour vous protéger contre les menaces en ligne.
- Utilisez des mots de passe forts et un gestionnaire de mots de passe pour stocker en toute sécurité vos informations de connexion.

- Évitez les téléchargements depuis des sources non fiables et ne cliquez pas sur des liens suspects ou inconnus.
2. Smartphone :
 - Mettez régulièrement à jour votre système d'exploitation et les applications pour corriger les vulnérabilités de sécurité connues.
 - Utilisez un code PIN ou une empreinte digitale pour verrouiller votre téléphone.
 - Évitez de télécharger des applications depuis des sources non officielles ou inconnues.
 - Désactivez la géolocalisation pour les applications qui n'en ont pas besoin.
 - Évitez de vous connecter à des réseaux Wi-Fi publics non sécurisés.
 3. Tablette :
 - Utilisez un mot de passe ou une empreinte digitale pour verrouiller votre tablette.
 - Utilisez des mots de passe forts pour vos applications et utilisez un gestionnaire de mots de passe pour les stocker en toute sécurité.
 - Évitez de télécharger des applications depuis des sources non officielles ou inconnues.
 - Désactivez la géolocalisation pour les applications qui n'en ont pas besoin.
 - Évitez de vous connecter à des réseaux Wi-Fi publics non sécurisés.

2/

Voici comment installer et utiliser un antivirus + antimalware en fonction de l'appareil utilisé:

1. Ordinateur de bureau ou portable :
 - Recherchez un antivirus et un antimalware de confiance. Il existe de nombreuses options disponibles, telles que McAfee, Norton, Avast, Malwarebytes, etc.
 - Téléchargez le logiciel à partir du site Web du fournisseur d'antivirus/antimalware et suivez les instructions d'installation.
 - Une fois installé, effectuez une analyse complète de votre ordinateur et configurez les paramètres de l'antivirus/antimalware selon vos préférences.
 - Gardez le logiciel à jour en téléchargeant les dernières mises à jour de définitions de virus pour vous protéger contre les menaces les plus récentes.
2. Smartphone :
 - Recherchez un antivirus et un antimalware pour votre système d'exploitation (Android, iOS, etc.). Les options populaires comprennent Avast, Norton, Kaspersky, etc.
 - Téléchargez l'application depuis le Google Play Store ou l'App Store et suivez les instructions d'installation.



- Une fois installé, effectuez une analyse complète de votre téléphone et configurez les paramètres de l'antivirus/antimalware selon vos préférences.
 - Gardez le logiciel à jour en téléchargeant les dernières mises à jour de définitions de virus pour vous protéger contre les menaces les plus récentes.
3. Tablette :
- Les étapes pour installer et utiliser un antivirus/antimalware sur une tablette sont similaires à celles pour un smartphone. Vous pouvez utiliser les mêmes logiciels antivirus/antimalware pour votre tablette que pour votre smartphone.
 - Recherchez un antivirus et un antimalware pour votre système d'exploitation (Android, iOS, etc.). Les options populaires comprennent Avast, Norton, Kaspersky, etc.
 - Téléchargez l'application depuis le Google Play Store ou l'App Store et suivez les instructions d'installation.
 - Une fois installé, effectuez une analyse complète de votre tablette et configurez les paramètres de l'antivirus/antimalware selon vos préférences.
 - Gardez le logiciel à jour en téléchargeant les dernières mises à jour de définitions de virus pour vous protéger contre les menaces les plus récentes.