1. Introduction à la sécurité sur Internet

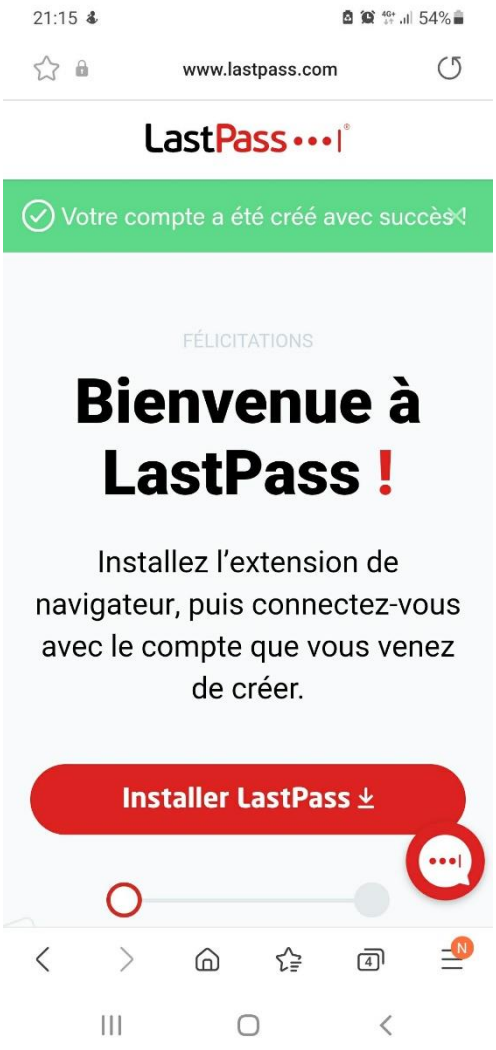
Consulter trois articles qui parlent de sécurité sur Internet. Pense à vérifier la source des informations et essaie de consulter des articles récents pour que les informations soient à jour. Saisis le nom du site et de l'article.

- Article 1 : **Cybermalveillance.gouv - comment se protéger sur internet ?**
- Article 2 : **La Poste - 5 conseils pour être en sécurité sur internet**
- Article 3 : **Kaspersky - Sécurité Internet : Qu'est-ce que c'est et comment vous protéger en ligne**

2. Créer des mots de passe forts

Comment utiliser pour la première fois un gestionnaire de mot de passe nommé LastPass.

- Accéder au site
- Créer un compte en remplissant le formulaire
- Suivre les étapes et se connecter



3. Fonctionnalité de sécurité de votre navigateur

Identifie les adresses internet qui te semblent provenir de sites web malveillants.

- www.morvel.com: c'est un site malveillant, le site officiel est www.marvel.com un site de l'univers Marvel
- www.dccomics.com: site officiel de l'univers DC Comics
- www.ironman.com: site official Triathlons Worldwide
- www.fessebook.com: site malveillant, le site officiel est www.facebook.com site de réseau sociaux du monde
- www.instagam.com: site malveillant, le site officiel est www.instagram.com un réseau sociaux international

Vérifier si les navigateurs utilisés Chrome et Firefox sont à jour

- Pour chrome :
- Pour Firefox :

4. Eviter le spam et le phishing

Exercer la capacité à déceler les erreurs dans les messages cachant une action malveillante en arrière-plan.

Le phishing ou hameçonnage est une technique frauduleuse destinée à leurrer un internaute pour l'inciter à communiquer des données personnelles en faisant passer pour un service connu ou u proche. On retrouve en effet souvent des indicateurs similaires :

- Une notification de la messagerie ou de l'antivirus : assurer que votre antivirus est activé et à jour.
- Un email d'un service ou d'une société dont vous n'êtes pas client : se méfier de ces sociétés, une cybercriminalité peut s'en prendre aux vrais clients.
- Mail phishing : un nom d'expéditeur inhabituel : des messages inattendu d'une adresse email inhabituel doit éveiller votre attention.
- Une adresse d'expédition fantaisie : penser à vérifier l'adresse email de l'expéditeur.
- Un objet d'email trop alléchant ou alarmiste : un intitulé aguicheur ou inquiétant.
- Une apparence suspecte : se méfier lors des différences entre l'apparence du mail reçu et celle des mails habituels.
- Une absence de personnalisation :
- Une demande inhabituelle : connaitre l'adresse email de l'expéditeur n'est pas u critère de confiance absolu.
- Une demande d'information confidentielle : ne communiquer rien de confidentiel en écrit.
- Un message aguicheur ou inquiétant : un mail fraudeur peut également faire état d'un besoin urgent ou d'une menace imminente qui requiert une action immédiate.
- Des fautes de français surprenantes : être vigilant à la qualité du texte de l'email.
- Une incitation à cliquer sur un lien ou une pièce jointe : éviter de cliquer sur ces liens.

5. Comment éviter les logiciels malveillants

Analyser les informations de plusieurs sites : préciser l'indicateur de sécurité, le rapport d'analyse de l'outil Google.

- Site n°1 : (VOSTFREE)
  Indicateur de sécurité : **https**
  Analyse Google : **aucun contenu suspect**
- Site n°2 : (TV5 MONDE)
  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

Créer un dossier sur la messagerie électronique

- ✓ Accéder à Gmail
- ✓ Trouver à gauche les libellés initiaux
- ✓ Cliquer sur « Plus » et faire un clic sur « créer un libellé » et le renommer « ACHATS »

7. Comprendre le suivi du navigateur

Les navigateurs internet sont les logiciels qui permettent d'aller sur le web, et de traduire du code.

Pour limiter les traces, on peut effectuer deux actions :

- ➢ Limiter l'utilisation des cookies dans le paramètre du navigateur ou en utilisant la navigation privée
- ➢ Effacer les cookies déposés par les sites web sur l'appareil

8. Principe de base de la confidentialité des médias sociaux

Comme tous les réseaux sociaux, Facebook met à disposition des internautes une politique de confidentialité. L'utilisateur peut gérer ses paramètres de confidentialité par le biais d'une interface, dans laquelle il peut contrôler la visibilité de ses données :

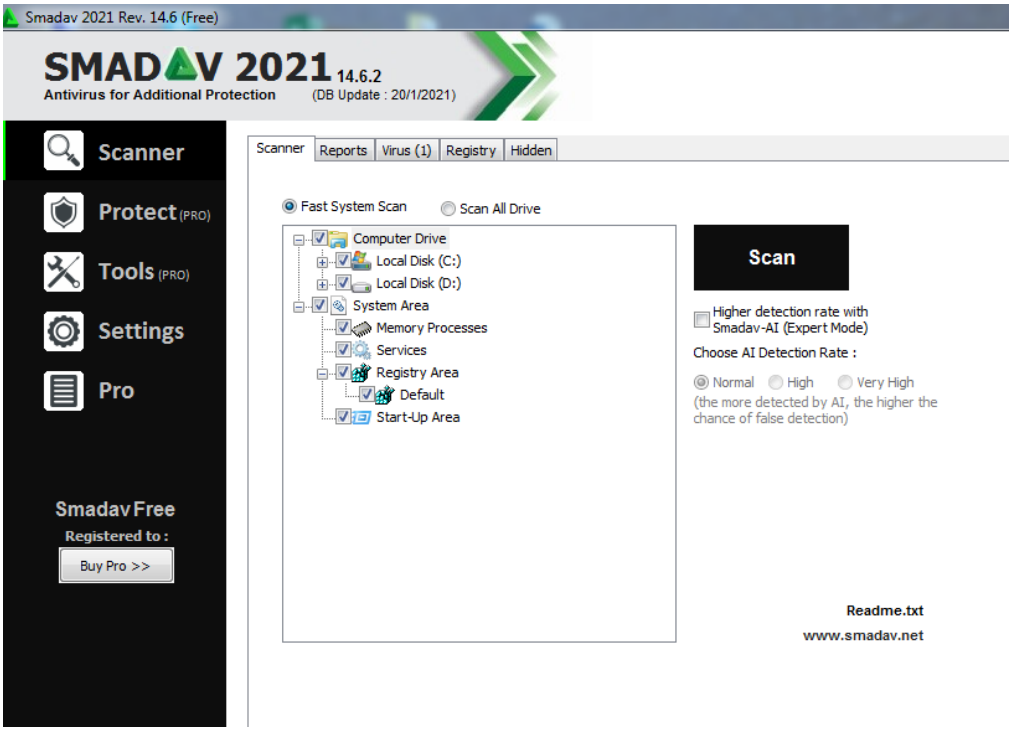
- ➢ Contrôler l'accès à chacune des publications
- ➢ Désactiver ou supprimer son compte
- ➢ Bloquer certains utilisateurs
- ➢ Permet de modifier la visibilité des informations
- ➢ Le partage d'information sur le profil est régi par le paramètre de confidentialité
- ➢ Permet d'accéder à l'historique des activités et aux commandes pour gérer les informations
- ➢ Personnaliser les expériences sue Facebook
- ➢ Mettre à jour les informations pour assurer la sécurité du compte

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

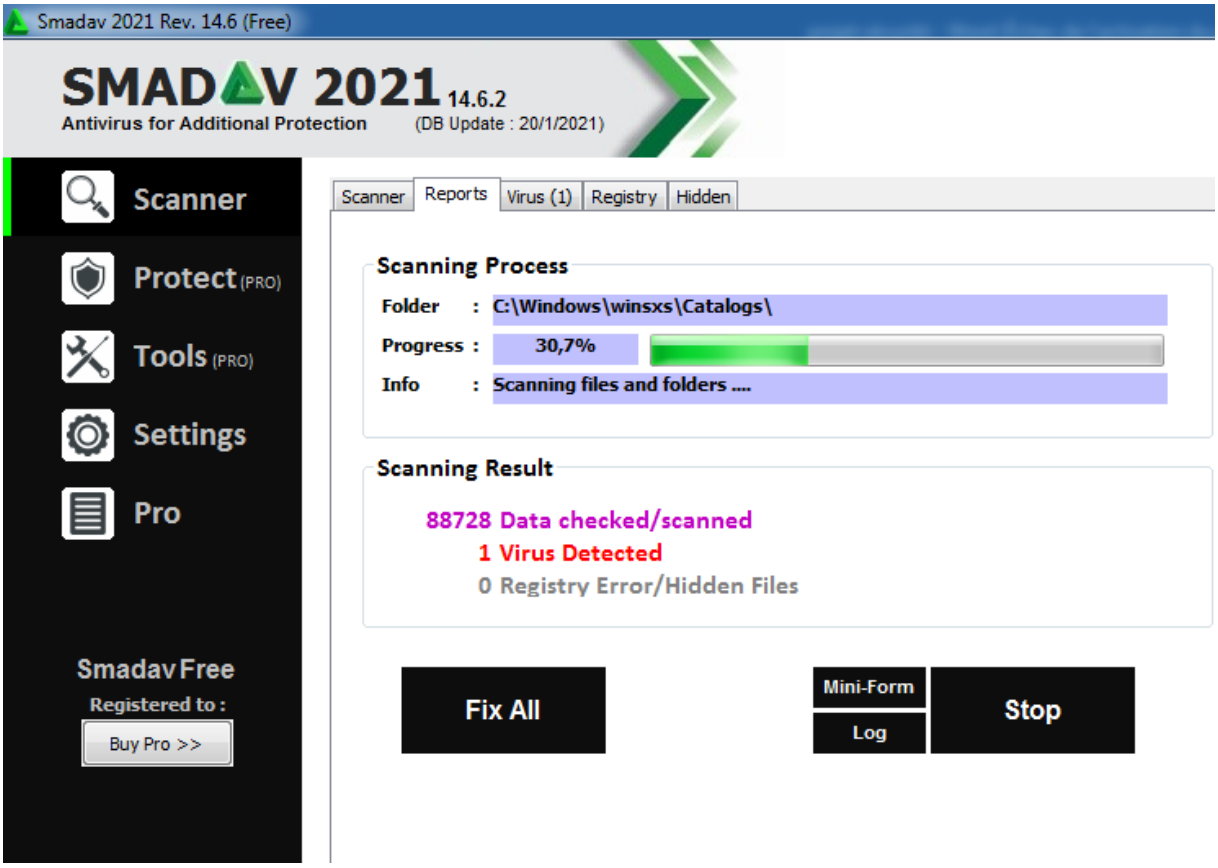
Proposer un ou plusieurs exercice(s) pour vérifier la sécurité e fonction de l'appareil utilisé ?

Comment faire ?

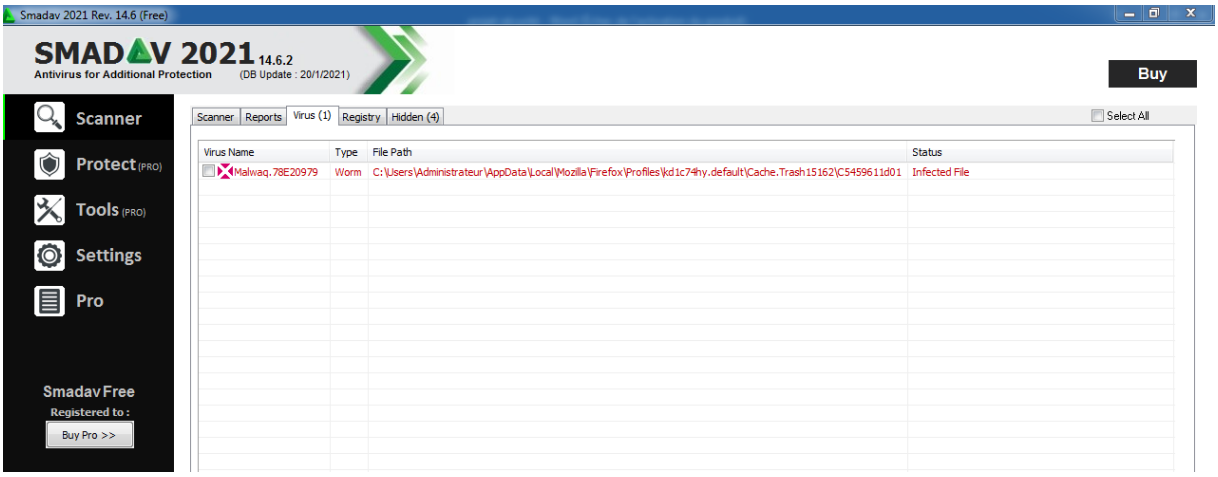
- ✓ Installer un logiciel antivirus
- ✓ Analyser le système

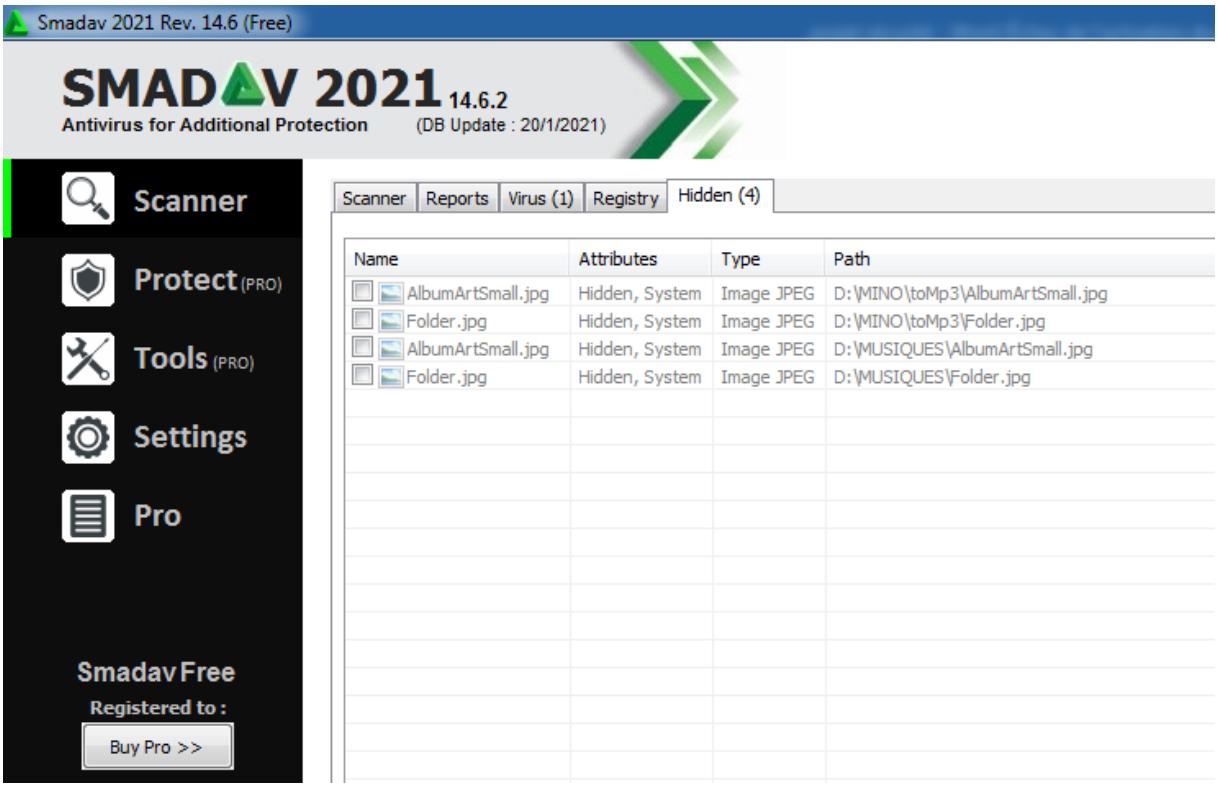


- ✓ Examiner les menaces



- ✓ Trouver les logiciels malveillants et les supprimer





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