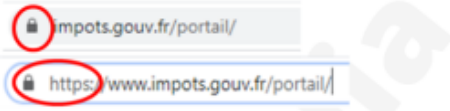
Les outils de sécurité

Mémo “Les outils de sécurité”

FICHE la Sécurité

Le cadenas

Lorsque vous naviguez sur internet, il est important de vérifier que vous vous trouvez bien sur un site sécurisé avant de communiquer un mot de passe, des données personnelles ou encore des numéros de carte bleu (vérifier si le paiement est sécurisé > privilégier les paiements via PayPal si vous avez).



Les mentions légales et conditions générales

Sur chaque site internet, tout en bas, dans le bandeau avec l’écriture en tout petit, vous devez avoir “Mentions légales” ou “Informations légales”. Tout site internet est obligé d’afficher des informations notamment son siège social et son numéro de Siret, TVA ou autres numéros liés à la vente. Si vous ne trouvez pas ces informations-là, fuyez.
Ensuite, pour connaître vos droits de remboursement, il faut lire les conditions générales (de vente). Vous allez avoir un article qui traite des droits de rétractation, c’est dans cet article que vous aurez toutes les informations nécessaires au renvoi et au remboursement.

Les antivirus

- Ce sont des logiciels informatiques destiné à identifier et à effacer les logiciels malveillants (malwares).
- La détection se repose sur 2 méthodes :
  - Reconnaissance d’un code déjà connu (appelé signature) et mémorisé dans une base de données afin d’être retrouvé plus vite.
  - Analyse du comportement d’un logiciel.
- Gratuit ou payant : les antivirus offrent le même niveau de protection face aux virus et aux malwares.
- 3 différences :
  - La confidentialité des données personnelles de l’utilisateur. En contrepartie de la gratuité, certains éditeurs collectent des informations pour les revendre à des entreprises.
  - Les fonctionnalités de protection : une offre payante sera toujours plus complète qu’une offre gratuite.
  - La publicité : contrepartie à accepter si on souhaite rester sur une offre gratuite.
- Il n’y en a pas un meilleur que les autres, il y en a beaucoup qui existent mais tous ne se valent pas. Le choix se fait en fonction des domaines ou on a besoin d’être protégé.

Windows Defender

Si vous voulez en avoir un gratuit, vous pouvez garder celui que tout ordinateur sur Windows 8/10/11 a : Windows defender. Il travaille tout seul et aucune publicité. Vous avez la possibilité de lancer des analyses si besoin.

Mémo “Les outils de sécurité”

FICHE la Sécurité

Les automatismes à mettre en place :

- Faites les mises à jour lorsque celles-ci sont proposées (logiciels, systèmes d'exploitation...).
- Vérifier l'adresse e-mail d'un message qui semble suspect.
- S'assurer d'avoir un anti-virus sur l'ordinateur -> UN SEUL SUFFIT S'IL EST BIEN PROGRAMMER.
- Se rappeler : aucune banque ou systèmes de paiement en ligne de vous demandera de fournir des identifiants de connexion ou encore les numéros bancaires ou numéro de sécurité sociale par mail.

Les gestionnaires de mot de passe

Cela permet d'éviter de les noter à des endroits risqués, tel que à proximité de vos appareils, sur votre téléphone portable... un seul mot de passe à retenir, qui vous permet d'accéder à tous ! Vous pouvez utiliser par exemple **Bitwarden**.

Le VPN

VPN : Virtuel Private Network => Réseau Privé Virtuel

- Création d'un tunnel sécurisé entre vous et Internet.
- Il permet de crypter les informations et vous permet d'obtenir une nouvelle adresse IP (numéro d'identification attribué à chaque périphérique relié à un réseau qui utilise Internet).
- Ce qui permet d'anonymiser la navigation.
- Généralement payants, certaines offres peuvent aussi être gratuites et se rajouter à vos navigateurs.

Vous avez par exemple **NordVPN** ou encore **Surfshark**. Certains antivirus vendent aussi des VPN.

Les sites utiles :

internet-signalement.gouv.fr

Aussi appelé PHAROS* plateforme d'Harmonisation, d'Analyse de Recoupement et d'Orientation des Signalements.
Permet de signaler des faits de :
-Pédophilie et pédopornographie,
-Expression du racisme, de l'antisémitisme et de la xénophobie,
-Incitations à la haine raciale, ethnique et religieuse,
-Apologie du terrorisme et actes terroristes,
-Escroqueries et arnaques financières utilisant internet.
Qu'ils soient sur des sites, blog, forum, tchat, réseaux sociaux etc.

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

-Informe sur la cybermalveillance
-Donne les moyens de se protéger
-Et propose des solutions.

Destination Multimédia

Mémo “Les outils de sécurité”

FICHE la Sécurité

signal spam

Signal Spam permet aux internautes de signaler tout ce qu'ils considèrent être un spam dans leur messagerie afin de l'assigner ensuite à l'autorité publique ou au professionnel qui saura le mieux prendre l'action qui s'impose pour lutter contre le spam signalé. *Nécessite la création d'un compte*

Service-Public permet d'informer les services d'enquêtes de l'existence de la fraude. Vous pouvez rester anonyme mais vous ne serez pas informé des suites de l'affaire.
N'empêche pas de faire un dépôt de plainte au commissariat ou par courrier en donnant votre identité pour être au courant de l'avancement du dossier. *Nécessite de se connecter par FranceConnect.*

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Service-Public.fr
Le site officiel de l'administration française

CNIL.

C'est la Commission Nationale de l'Informatique et des Libertés.
En charge de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.
6 missions : Informer, réguler, protéger, contrôler, sanctionner et anticiper.

Décodex est un outil pour aider à vérifier les informations qui circulent sur Internet et dénicher les rumeurs, exagérations ou déformations.
Il suffit de copier le lien et de le coller pour savoir si la source de l'information (celui ou celle qui l'a diffusé) est plutôt fiable ou non.

DÉCODEX

33700 La plateforme de lutte contre les spams vocaux et sms

33700 est un numéro qui vous permet de signaler les sms que vous pouvez recevoir.
Pour cela il suffit de transférer le sms que vous avez reçu à ce numéro.