CORBIE

Atelier numérique

La cybersécurité

CONSEILLER NUMÉRIQUE France services

La cybersécurité

Atelier numérique

Les menaces Quelles sont les principales?

1 Logiciels malveillants (Malwares)
Terme désignant une famille de logiciels hostiles et/ou intrusifs ayant pour but d'installer des virus ou encore bloquer les données en échange d'une rançon. (Ransomware[1], spyware[2], Trojans[3], adware[4]…etc)

Security Break

2 Hameçonnage (Phishing)
Technique frauduleuse incitant un internaute à communiquer des données personnelles.

association prévention MAIF

3 Fuite de données
Exposition volontaire ou involontaire sur internet de données confidentielles.

Conscio Technologies

4 Fraude au président (usurpation d'identité)
Consiste à usurper une identité (président) dans le but d'effectuer des transactions bancaires.

TF1 INFO

5 Arnaque au faux support technique
Consiste à effrayer l'utilisateur en indiquant un problème technique grave.

CONSO MAG

6 Faux sites / Faux profils
Consiste à se faire passer pour quelqu'un d'autre (personne fictive) dans un but malveillant.

Labo Des Réseaux

En savoir plus

Serious games

1 : Rançongiciel; **2 :** Logiciel espion; **3 :** Cheval de Troie; **4 :** Logiciel publicitaire;

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

CONSEILLER NUMÉRIQUE France services

La cybersécurité

Atelier numérique

Les bonnes pratiques générales (1/2)

1 Choisir des mots de passes robustes (et différents)

Plus un mot de passe et long et complié, plus le compte sera difficile à pirater.
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe

association prévention MAIF

La méthode des premières lettres
Un tiens vaut mieux que deux tu l'auras
> **1tvmQ2tl'A**

La méthode phonétique
J'ai acheté huit CD pour cent euros
> **ght8CD%E**

2 Sauvegarder ses données (Clé USB, disque dur, cloud[1]…)

Pour protéger vos données des piratages, des pannes, des vols ou pertes de vos appareils.
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes

3 Mises à jour des logiciels (Pour corriger les failles de sécurité)

Ne télécharger que depuis des sites officiels!!! Il est possible d'automatiser les mises à jour
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mises-a-jour

4 Attention à la provenance des applications! (Sites officiels)

Vérifier la provenance des applications à installer pour limiter les risques. Eviter les sites internet frauduleux qui pourraient installer des virus.

5 Messages inattendus. (Phishing[3], virus en pièce jointe ou lien malveillant)

Attention aux messages inattendus ou alarmistes (courriel, sms ou tchat), vérifier par un autre moyen l'identité de l'expéditeur.
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing

1 : Nuage; **2 :** Mise à jour; **3 :** Hameçonnage;

Sources : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/10-mesures-essentielles-assurer-securite-numerique

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

CONSEILLER NUMÉRIQUE France services

La cybersécurité

Atelier numérique

Les bonnes pratiques générales (2/2)

6 Utiliser un antivirus (Gratuit ou payant)

Permet de se protéger d'une majorité d'attaques et de virus connus. (Mises à jour et analyses régulières).
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/antivirus

7 Vérifier les sites d'achats (https[1], cadenas fermé…)

Attention aux offres trop alléchantes. Attention aux sites non sécurisés.
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/fraude-carte-bancaire

8 Maîtriser ses réseaux sociaux (Informations personnelles)

Sécuriser les accès, définir les autorisations, ne pas relayer d'informations sans les vérifier…
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/reseaux-sociaux

association prévention MAIF

9 Séparer les différents usages (Personnels / Professionnels)

Pour qu'un accès personnel ne puisse pas nuire à la sécurité de votre entreprise ou inversement.
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securite-usages-pro-perso

10 Se méfier des réseaux WiFi[2] publics. (Souvent gratuits ils ne sont pas toujours sécurisés)

Mal sécurisés ces réseaux peuvent être contrôlés par des pirates et se saisir de vos informations privées.

1 : Hyper Text Transfert Protocol Secure; 2 : Wireless Fidelity;

Sources : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/10-mesures-essentielles-assurer-securite-numerique

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

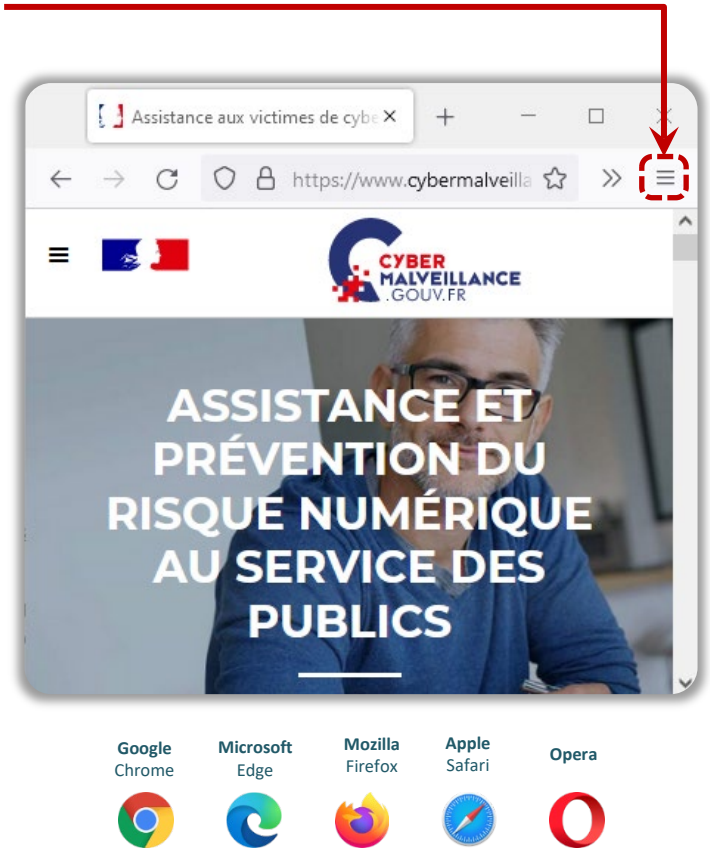
CONSEILLER NUMÉRIQUE France services

La cybersécurité

Atelier numérique

Naviguer sur le web (Les bonnes pratiques)

- **Mises à jour du navigateur** (Manuelles ou automatiques)
  D'un navigateur à l'autre la démarche diffère. Se rendre dans les paramètres.
- **Naviguer en mode "privé"** (ou incognito)
  Ce mode permet de ne pas enregistrer l'historique de navigation.
  Très important si l'ordinateur n'est pas le sien!!!
- **Configurer le navigateur** (Refus d'être pister)
  D'un navigateur à l'autre la démarche diffère.
  Se rendre dans les paramètres (Vie privée ou Sécurité)
- **Supprimer les données de navigations** (Régulièrement)
  D'un navigateur à l'autre la démarche diffère.
  Se rendre dans les paramètres (Vie privée ou Sécurité)
- **Installer un bloqueur de publicité**
  Les publicités peuvent cacher des arnaques ou des virus potentiels.
  Certains sites ne les acceptent pas (il faudra alors le désactiver)



Sources : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/10-mesures-essentielles-assurer-securite-numerique

La cybersécurité

Atelier numérique

Naviguer sur le web (Les bonnes pratiques) Suite

1. **Se méfier des offres trop alléchantes** (Comparer)
   Un produit à **prix cassé** cache souvent une arnaque!

2. **Vérifier l'identité du vendeur** (si pas connu)
   Faire une recherche du **nom du site** associé du mot **"arnaque",** ou **" avis"**.
   Privilégier les annonces avec un e-mail et un téléphone (Pour les contacter).
   Préférer les annonces où les produits peuvent être récupérer en main propre.

3. **S'assurer des données chiffrées** (protocole https[1]:///)
   Vérifier que l'URL[2] (**adresse web**) du site comporte la mention https://
   Il s'agit du protocole LS qui garantit le chiffrement des données bancaires.

4. **Examiner les CGU[3] ou CGV[4]** (et les mentions légales)
   Pour connaître les **conditions** de vente, d'utilisation et de reprise.
   Et pour savoir **qui** se trouve **derrière** le site web.

5. **Vérifier l'URL[2] qui se cache derrière un lien**
   Avant de cliquer sur un lien, l'**adresse web** du site s'affiche en bas à gauche.

6. **Utiliser des outils externes** (pour analyser les sites)
   Copier / coller l'adresse du site dans ces outils et lancer l'analyse.
   https://transparencyreport.google.com/safe-browsing/
   https://www.scamdoc.com/

Guide des achats en ligne

1 : Hyper Text Transfert Protocol Secure; 2 : Uniform Resource Locator; 3 : Conditions Générales d'Utilisation ; 4 : Conditions Générales de Vente;

Sources : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/10-mesures-essentielles-assurer-securite-numerique

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

CONSEILLER NUMÉRIQUE France services

La cybersécurité

Atelier numérique

Ressources

Achats en ligne

Cybermalveillance.gouv.fr

Comment sécuriser ses achats sur internet

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-securiser-ses-achats-sur-internet

Les réseaux sociaux

Cybermalveillance.gouv.fr

Fiche pratique

https://www.cybermalveillance.gouv.fr/medias/2019/11/Fiche-Pratique_reseaux-sociaux.pdf

Fuite de données

Have i been pwned?

Savoir si son email a fait l'objet de fuite de données

https://haveibeenpwned.com/

Cyber Malveillance

Cybermalveillance.gouv.fr

Cyber Guide Familles

https://www.cybermalveillance.gouv.fr/medias/2022/09/Cyber_Guide_Familles.pdf

Cybermalveillance.gouv.fr

Cyber quiz

https://quiz.cybermalveillance.gouv.fr/

Les mots de passes

Nothing 2 Hide

Vérificateur de mot de passe

https://nothing2hide.org/fr/verifier-la-robustesse-de-votre-mot-de-passe/

Economie.gouv.fr

Créer un mot de passe sécurisé

https://www.economie.gouv.fr/particuliers/creer-mot-passe-securise

CORBIE

Nous avons terminé…

Merci!

Crédits images : Freepik / Vecteezy / CNFS

CONSEILLER NUMÉRIQUE France services

Guillaume GOBERT

15/02/2024