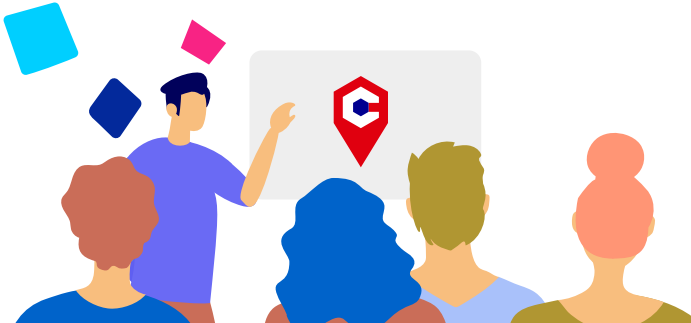
CORBIE

Les dangers du Numérique
Cybersécurité et Protection des données

CONSEILLER NUMÉRIQUE



CORBIE

Cybersécurité et Protection des données

Les dangers du Numérique

Les menaces Quelles sont les principales?

1 Logiciels malveillants (Malwares)

- Virus, vers, chevaux de Troie : endommagent / volent des données
- Ransomwares[1] : Bloquent les fichiers en échange d'une rançon.
- Spywares[2] et keyloggers : Espionnent les actions.

Security Break
4min 4s

2 Phishing[3] et escroqueries numériques

- Phishing : faux e-mails incitant à communiquer des données.
- Smishing : hameçonnage par sms.
- Vishing : hameçonnage par appel vocal.
- Faux sites web : imitent des sites connus pour voler des données.
- Faux profils : utilisés pour gagner la confiance et arnaquer.

association prévention MAIF
5min 5s

Labo Des Réseaux
3min 19s

3 Arnaques par ingénierie sociale

- Faux support technique : prétendent être légitime pour prendre le contrôle.
- Fraude au président (CEO Fraud) : usurpent l'identité d'un dirigeant.

CONSO MAG
2min 5s

TF1 INFO
1min 44s

1 : Rançongiciel; **2 :** Logiciel espion; **3 :** Hameçonnage;

4 Piratage et exploitation des failles

- Hacking : accès non autorisé à des systèmes informatiques
- Vulnérabilité Zero-day : failles encore inconnues des éditeurs
- Attaques par force brute : test d'une multitude de mots de passe.

5 Espionnage & vol de données

- Surveillance clandestine : par des Etats ou cybercriminels.
- Vol d'identifiants ou d'informations sensibles (piratage ou négligence)

6 Attaques par déni service (DDoS)

- Saturation de sites ou services web pour les rendre inaccessibles.

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

CONSEILLER NUMÉRIQUE

Cybersécurité et Protection des données

Les dangers du 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
1min 52s

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**

30s

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

30s

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

30s

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.

1min 6s

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

30s

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

Cybersécurité et Protection des données

Les dangers du 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).

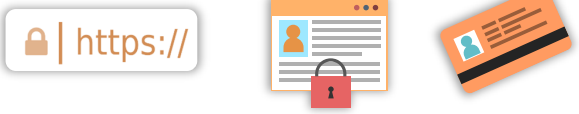
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/antivirus

1min 17s

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



2min 9s

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

1min 2s

1min 57s

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

4min 20s

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.

1min 11s

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

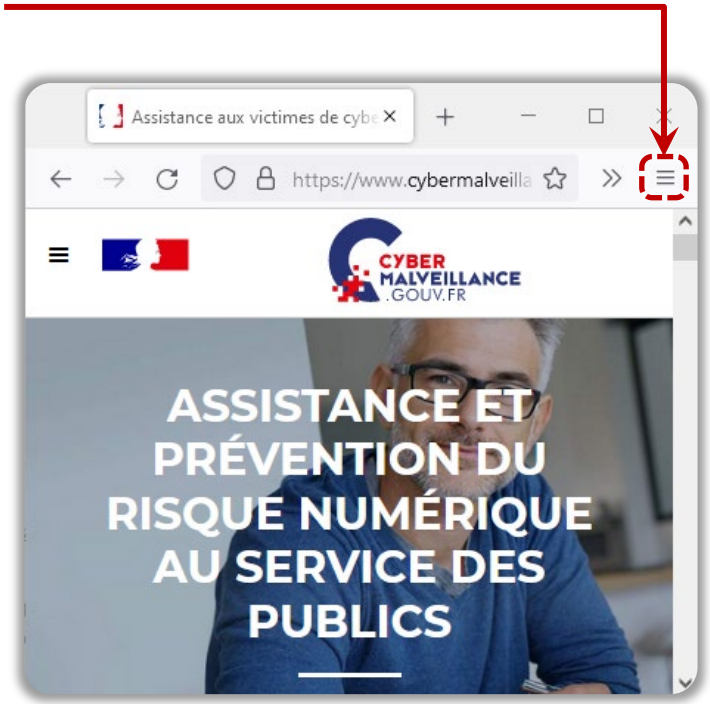
CONSEILLER NUMÉRIQUE

Cybersécurité et Protection des données

Les dangers du 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)



Google Chrome · Microsoft Edge · Mozilla Firefox · Apple Safari · Opera

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

Cybersécurité et Protection des données

Les dangers du 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

Cybersécurité et Protection des données

Les dangers du Numérique

Ressources (1/2)

Vérification d'URL

Google Safe Browsing
Vérifie si un site est signalé comme dangereux.
https://transparencyreport.google.com/safe-browsing

Nord VPN – Link checker
Analyse d'URL - Détection de logiciels malveillants / faux sites.
https://nordvpn.com/fr/link-checker/

Fuite de données

Have i been pwned?
Savoir si son email a fait l'objet de fuite de données.
https://haveibeenpwned.com/

Gestionnaire de mots de passe

Proton Pass
Application mobile ou extension de navigateur web. (Gratuit)
https://proton.me/fr/pass

KeePass
Logiciel de gestion de mot de passe. (Gratuit)
https://keepass.info/

Bitwarden
Application mobile ou extension de navigateur web. (Gratuit)
https://bitwarden.com/download/

Choisir son mot de passe

Cybermalveillance.gouv.fr
Choisir un bon mot de passe
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-choisir-un-bon-mot-de-passe

Robustesse des mots de passe

Dice Ware
Générateur de mots et phrases de passe. (Gratuit)
https://diceware.rempe.us/

Bitwarden - Password generator
Générateur de mots de passe.
https://bitwarden.com/password-generator/#password-generator

Bitwarden - Password stength
Testeur de robustesse de mots de passe.
https://bitwarden.com/password-strength/

Nothing 2 Hide
Testeur de mot de passe
https://nothing2hide.org/fr/verifier-la-robustesse-de-votre-mot-de-passe/

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

CONSEILLER NUMÉRIQUE

Cybersécurité et Protection des données

Les dangers du Numérique

Ressources (2/2)

Données personnelles

Je ne suis pas une data

L'outil pour reprendre la main sur vos données.

https://www.jenesuispasunedata.fr/

Exodus Privacy

Analyse les problèmes de vie privée. (Applications Android)

https://exodus-privacy.eu.org/fr/

Démarchage téléphonique

Bloctel.gouv.fr

Service de régulation du démarchage téléphonique.

https://www.bloctel.gouv.fr/

Spams

Signal Spams

Se Protéger, Signaler, Agir.
Du signalement à l'identifaction.

https://www.signal-spam.fr/

33700.fr

Plateforme de lutte contre les spams vocaux et sms.

https://www.33700.fr/

Serious Games

La Banque Postale

Alertes et Fraudes

https://www.labanquepostale.fr/particulier/footer/alertes-et-fraudes/serious-game.html

BNP Paribas

Phishing

https://mabanque.bnpparibas/fr/serious-game-phishing/jeu

Cyber Malveillance

Cybermalveillance.gouv.fr

Cyber Guide Familles

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

Cybermalveillance.gouv.fr

Quizz

https://www.cybermalveillance.gouv.fr/medias/2020/01/Quizz.pdf

Cybermalveillance.gouv.fr

Cybermenaces

https://www.cybermalveillance.gouv.fr/cybermenaces

Cybermalveillance.gouv.fr

Sécuriser ses achats.

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

Cybermalveillance.gouv.fr

Réseaux Sociaux - Fiche pratique

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

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

CONSEILLER NUMÉRIQUE

CORBIE

Nous avons terminé…

Merci!

Crédits images : Freepik / Vecteezy / CNFS

CONSEILLER NUMÉRIQUE

CC BY NC SA

Guillaume GOBERT

Màj 14/05/2025