



Les Dangers du Numérique Cybersécurité et Protection des données



CONSEILLER
NUMÉRIQUE





Quelles sont les principales menaces?



Attaques techniques



Vol et exploitation des données



Attaques humaines



Mauvaises pratiques





Attaques techniques



Malwares¹ (Virus, vers, chevaux de Troie...) : Programme conçu pour nuire, espionner ou endommager un appareil à l'insu de son utilisateur.



Ransomwares² : Virus qui verrouille vos fichiers (cryptage) et réclame une somme d'argent (rançon) en échange de la clé de déverrouillage.



Spywares³ et keyloggers : Logiciels espions qui surveillent votre activité. Le keylogger enregistre chaque touche tapée pour voler vos mots de passe.



Hacking⁴ : L'art de s'introduire dans un système informatique ou un réseau en exploitant ses faiblesses pour en prendre le contrôle.



Vulnérabilité Zero-day⁵ : Faille de sécurité fraîchement découverte ou encore inconnue des éditeurs de logiciels de protection.



Attaques par force brute : Méthode "bourrine" consistant à tester des milliers de combinaisons de mots de passe jusqu'à trouver la bonne.



Saturation de services web (DDoS⁶) : Attaque envoyant des millions de connexions simultanées vers un site pour le paralyser et le rendre inaccessible.



Faibles IoT⁷ : Faiblesses de sécurité dans les appareils "intelligents" (caméras, frigos, montres) permettant de s'introduire dans votre réseau domestique.



Security Break

Qu'est-ce qu'un Malware?

4min 4s

<https://www.youtube.com/watch?v=1IpW5klqLv0>



Cybermalveillance

Sécuriser ses objets connectés

2min 10s

<https://www.youtube.com/watch?v=vbCBSlyRSKs>





Attaques humaines



Phishing¹ : E-mail frauduleux imitant une administration vous incitant à communiquer des données personnelles.



Smishing : Même technique que le hameçonnage mais par sms.



Vishing : Même arnaque par téléphone où l'escroc se fait passer pour un conseiller technique ou bancaire.



Faux sites web : Copies presque parfaites de sites officiels dans le but de voler des données personnelles ou bancaires.



Faux profils : Identités créées sur les réseaux sociaux dans le but de gagner votre confiance pour vous arnaquer par la suite.



Faux support technique : Alerte sur l'écran simulant une panne pour vous faire appeler un numéro surtaxé et/ou prendre le contrôle de l'appareil.



Fraude au président : Un escroc se fait passer pour le grand patron afin d'ordonner un virement urgent et secret à un comptable.



Deepfake² : Vidéo ou audio truqué par l'intelligence artificielle pour imiter parfaitement la voix ou le visage d'une personne connue.



Prévention MAIF

Le senior des ados - Phishing
2min 5s

<https://www.youtube.com/watch?v=bxylwlbhcu8>



Labo des Réseaux

Reconnaître un faux profil
3min 19s

<https://www.youtube.com/watch?v=knixPuiwNCg>



Cyber Malveillance

Escroquerie Faux support technique
2min 5s

<https://www.youtube.com/watch?v=T-cYAy6Yer4>



TF1 INFO

Arnaque au président
1min 44s

<https://www.youtube.com/watch?v=k04NvNQliGw>





Vol et exploitation des données



Surveillance clandestine : Surveillance discrète de vos activités (micro, caméra, écran) à des fins de chantage (par des Etats ou cybercriminels).



Vol d'identifiants (piratage ou négligence) : Capture de vos duos "e-mail + mot de passe" pour accéder à vos comptes personnels.



Fuites de données : Perte massive d'informations clients par une entreprise suite à une attaque ou une erreur humaine.



Usurpation d'identité : Utilisation de vos données personnelles pour commettre des délits en votre nom (crédits, achats, abonnements...).



Credential Stuffing¹ : Utiliser une liste de mots de passe volés sur un site pour tester automatiquement leur validité sur des dizaines d'autres sites.



Christophe Boutry

Fuites de données – 10 Réflexes
31min

<https://www.youtube.com/watch?v=35su8AJYz88>



Cyber
Malveillance.gouv.fr

<https://www.cybermalveillance.gouv.fr/>





Mauvaises pratiques



Mots de passe faibles : Utiliser des codes trop simples (ex: "123456") faciles à deviner pour un logiciel.



Absence MFA¹ : Ne pas activer la "double vérification" (le code reçu par SMS/App), laissant le mot de passe comme seul rempart.



Wi-Fi² public : Utiliser des réseaux ouverts (gares, cafés) où les données peuvent être interceptées par n'importe qui.



Apps³ douteuses : Applications mobiles gratuites qui demandent des autorisations excessives pour piller vos contacts et photos.



Prévention MAIF

Mots de Passe
1min 52sec
<https://www.youtube.com/watch?v=qKzDK2EE1Fg>



La Techno

Authentification multifacteurs (MFA)
59sec
<https://www.youtube.com/shorts/meoz80dKm2Q>



01net

Arrêtez d'utiliser les Wi-Fi publics!
59sec
<https://www.youtube.com/shorts/LvE4l2KjXu0>





Les bonnes pratiques générales (1/2)



Choisir des mots de passes robustes (et différents)

Plus un mot de passe est long et compliqué, plus le compte sera difficile à pirater.

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe>

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

CST-CSE Canada

Créez un mot de passe fort

3min 8sec

<https://www.youtube.com/watch?v=cBPXxwYTPHw>



Utiliser la double authentification (MFA)

Pour protéger vos comptes sensibles (e-mail, banque...).

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/double-authentification>



Cybermalveillance

La double authentification

2min 18sec

<https://www.youtube.com/watch?v=4GQxevlvFG8>



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>



Cybermalveillance

Pourquoi faire les mises à jour ?

2min 4sec

<https://www.youtube.com/watch?v=wouVXIKsYL4>



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.



Cybermalveillance

Applications – Les autorisations

1min 6sec

https://www.youtube.com/watch?v=SppE-O_gZZw



Messages inattendus. (Phishing², 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>



ConsoMag

Reconnaissance du Phishing

2min 7sec

<https://www.youtube.com/watch?v=DHmkVQNcJyQ>



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



**Cyber
Malveillance.gouv.fr**

<https://www.cybermalveillance.gouv.fr/>

1 : Mise à jour; 2 : Hameçonnage;





Les bonnes pratiques générales (2/2)



Utiliser un antivirus (Gratuit ou payant)

Protège 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>



ConsoMag

Comment sécuriser mes appareils?

1min 17sec

<https://www.youtube.com/watch?v=fbKdgrLpNWw>



Sauvegarder ses données (Clé USB, disque dur, cloud¹...)

Protège vos données des piratages, des pannes, des vols ou pertes de vos appareils.

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes>



ConsoMag

Sauvegardes des données

2min 3sec

<https://www.youtube.com/watch?v=Xaa-EuFkdSA>



Maîtriser ses réseaux sociaux

Sécuriser les accès, définir les autorisations, vérifier les informations...

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/reseaux-sociaux>



Prévention MAIF

Confidentiel ou pas

1min 48sec

<https://www.youtube.com/watch?v=UbWxdeJN1fE>



Cybermalveillance

Réseaux sociaux en sécurité

1min 57sec

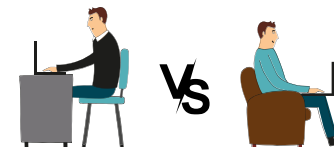
<https://www.youtube.com/watch?v=sgvFt0wl1YE>



Séparer les différents usages (Personnels / Professionnels)

Pour ne pas nuire à la sécurité personnelle ou de votre entreprise

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securite-usages-pro-perso>



Adeosys

Usage pro et perso : pourquoi?

4min 20sec

<https://www.youtube.com/watch?v=pvXiWVmNIZg>



Se méfier des réseaux WiFi² 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.



Cybermalveillance

WiFi public : Comment se protéger

1min 11sec

<https://www.youtube.com/watch?v=u6YkTqvOF3M>



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



**Cyber
Malveillance.gouv.fr**

<https://www.cybermalveillance.gouv.fr/>

1 : Nuage; 2 : Wireless Fidelity;



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 pisté)

D'un navigateur à l'autre la démarche diffère.
Se rendre dans les paramètres (Vie privée ou Sécurité)



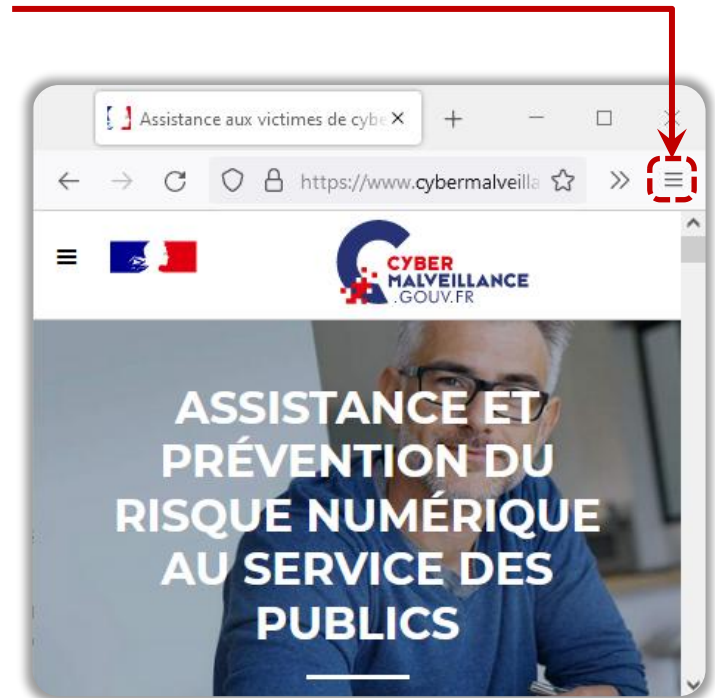
Supprimer les données de navigations (Régulièrement)

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**

<https://www.cybermalveillance.gouv.fr/>



Naviguer sur le web (Les bonnes pratiques) Suite



Se méfier des offres trop alléchantes (Comparer)

Un produit à **prix cassé** cache souvent une arnaque!



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.



S'assurer des données chiffrées (protocole https://)

Vérifier que l'URL² (**adresse web**) du site comporte la mention https://
Il s'agit du protocole LS qui garantit le chiffrement des données bancaires.



Examiner les CGU³ ou CGV⁴ (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.



Vérifier l'URL² qui se cache derrière un lien

Avant de cliquer sur un lien, l'**adresse web** du site s'affiche en bas à gauche.



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/>

Cybermalveillance

Guide des achats en ligne

https://www.cybermalveillance.gouv.fr/medias/2020/01/2019_GUIDE_Achats-en-ligne.pdf



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



**Cyber
Malveillance.gouv.fr**

<https://www.cybermalveillance.gouv.fr/>

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





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 strength

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/>





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/>



NumériQuiz

numeriqueethique.fr

Protéger sa vie privée sur Internet

<https://numeriquiz.fr/quiz/protoger-sa-vie-privee-sur-internet>

Spams



Signal Spams

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

<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/eu>

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





Nous avons terminé... Merci!

Crédits images : [QrcodeMonkey](#) / [Freepik](#) / [Vecteezy](#) / [Pexels](#) / [CN](#)



**CONSEILLER
NUMÉRIQUE**



Guillaume GOBERT

Màj 17/03/2026

