



Fiche Mémor

Cybersécurité



MOTS DE PASSE FORTS

Utilisez des mots de passe longs et uniques pour chaque compte.



MISES À JOUR RÉGULIÈRES

Maintenez vos systèmes, logiciels et antivirus à jour.



AUTHENTIFICATION À DEUX FACTEURS

Activez la double authentification partout où c'est possible.



SAUVEGARDEZ VOS DONNÉES

Faites des sauvegardes régulières de vos données importantes.



VÉRIFIEZ LA PROVENANCE

Vérifiez l'expéditeur, l'adresse email et soyez attentif aux fautes d'orthographe.



VERROUILLEZ VOS APPAREILS

Verrouillez votre session lorsque vous vous absentez.



LIENS ET PIÈCES JOINTES

Ne cliquez que sur les liens et n'ouvrez que les pièces jointes dont vous êtes sûr de la source.



SOYEZ VIGILANT ET INFORMÉ

Restez informé des menaces et sensibilisez votre entourage.



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>



Nord VPN – Link checker

Analyse d'URL - Détection de logiciels malveillants / faux sites.

<https://nordvpn.com/fr/link-checker/>



vera

Vérifie les faits (appel ou whatsapp)

Numéro Gratuit à ajouter aux contacts

<https://www.askvera.org/> | 09 74 99 12 95



**CONSEILLER
NUMÉRIQUE**



NumériQuiz
numeriqueethique.fr



Testez-vous sur le numérique

<https://numeriquiz.fr/>

Guillaume GOBERT
18/08/2026





Fiche Mémor

Cybersécurité



NE PARTAGEZ PAS VOS MOTS DE PASSE

Personne n'a besoin de votre mot de passe, ni par email, ni par téléphone.



N'UTILISEZ PAS DE RÉSEAUX Wi-Fi PUBLICS NON SÉCURISÉS

Évitez de vous connecter à des réseaux Wi-Fi publics pour des opérations sensibles.



NE CLIQUEZ PAS SUR DES LIENS SUSPECTS

Évitez de cliquer sur des liens dans des emails ou SMS inattendus.



NE TÉLÉCHARGEZ PAS DE LOGICIELS DOUTEUX

Téléchargez uniquement depuis des sites officiels et de confiance.



N'OUVREZ PAS DE PIÈCES JOINTES INATTENDUES

Elles peuvent contenir des virus ou des logiciels malveillants.



NE LAISSEZ PAS VOS APPAREILS SANS SURVEILLANCE

Un accès non autorisé peut compromettre vos données.



NE COMMUNIQUEZ PAS D'INFORMATIONS SENSIBLES

Ne partagez jamais vos données personnelles ou professionnelles par email ou téléphone.



NE REPORTEZ PAS UN COMPORTEMENT SUSPECT

En cas de doute, signalez-le immédiatement à votre référent informatique.



Signal Spams

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

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



Have i been pwned?

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

<https://haveibeenpwned.com/>



Je ne suis pas une data

L'outil pour reprendre la main
sur vos données.

<https://www.jenesuispasunedata.fr/>



CONSEILLER
NUMÉRIQUE



Cyber
Malveillance.gouv.fr

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

Guillaume GOBERT
18/08/2026

