

# SÉCURITÉ NUMÉRIQUE

## 10 RÈGLES D'OR POUR LES ÉQUIPES DE CAMPAGNE

---

# LES 10 RÈGLES D'OR PRÉVENTIVES

## **1 / SÉPAREZ VOS USAGES PRIVÉS DE CEUX LIÉS AU TRAVAIL.**

N'utilisez pas vos moyens de communication personnels (mail, téléphone, services de stockage en ligne, clé USB, etc.) dans le cadre professionnel, et inversement.

## **2 / METTEZ À JOUR VOS OUTILS NUMÉRIQUES** (ordinateur, smartphone, application, etc.).

**3 / CHOISISSEZ DES MOTS DE PASSE FORTS.** Ils doivent être longs et différents de vos mots de passe personnels, ne pas comprendre d'informations personnelles et rester secrets.

**4 / EN DÉPLACEMENT, PRENEZ GARDE À VOS ÉQUIPEMENTS** et n'emportez que le strict nécessaire.

**5 / VERROUILLEZ VOTRE ORDINATEUR** à chacune de vos absences et placez vos supports de stockage dans un mobilier adapté au niveau de sensibilité.

**6 / PROTÉGEZ VOTRE MESSAGERIE.** Faites preuve de vigilance avant d'ouvrir les pièces jointes et ne cliquez pas sur les liens douteux.

**7 / PRENEZ SOIN DE VOS INFORMATIONS PERSONNELLES EN LIGNE.** Préservez votre identité numérique en vous montrant vigilant sur Internet et les réseaux sociaux.

**8 / NE VOUS CONNECTEZ PAS SUR DES RÉSEAUX NON MAÎTRISÉS** (réseaux Wi-Fi publics, bornes de recharge USB, etc.).

**9 / FAITES ATTENTION LORS DE VOS ÉCHANGES TÉLÉPHONIQUES OU EN VISIOCONFÉRENCE.** La confidentialité des conversations n'est pas assurée.

**10 / ÉTEIGNEZ VOTRE SMARTPHONE** lorsque vous participez à des réunions sensibles et limitez la transmission de données (géolocalisation, bluetooth, autorisations des applications, etc.).

---

# LES 5 MESURES EN CAS D'ATTAQUE SUSPECTÉE

**1 / LAISSEZ LES ÉQUIPEMENTS ALLUMÉS** et n'intervenez pas davantage.

**2 / DÉCONNECTEZ LES ÉQUIPEMENTS** suspects du réseau (WiFi ou Ethernet).

**3 / NE CONNECTEZ PAS DE NOUVEL APPAREIL** sur le réseau.

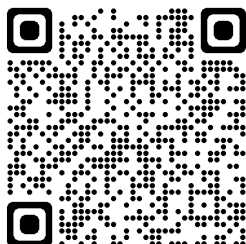
**4 / CONTACTEZ IMMÉDIATEMENT VOTRE SERVICE INFORMATIQUE** ou votre prestataire.

**5 / NOTIFIEZ LES AUTORITÉS COMPÉTENTES :**

- ▶ CNIL ;
- ▶ ANSSI ;
- ▶ [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) ;
- ▶ Police et gendarmerie.

## EN SAVOIR PLUS

RETROUVEZ TOUTES LES RESSOURCES UTILES POUR ASSURER VOTRE SÉCURITÉ NUMÉRIQUE SUR LE SITE DE L'ANSSI.



## CELA POURRAIT VOUS ARRIVER

« Par facilité, un conseiller utilise le même mot de passe pour tous ses outils numériques, personnels comme professionnels. À partir d'une fuite de données subie par un site anodin sur lequel le conseiller s'était inscrit, un attaquant identifie le mot de passe et accède à tous ses outils numériques. »

Votre fonction vous amène à traiter d'informations sensibles souvent sous forme numérique, méritant à ce titre une protection particulière.

Réunies dans ce livret réalisé par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), des bonnes pratiques permettent de se prémunir de cyberattaques souvent préjudiciables à votre image, celle de votre institution ou de votre parti.

**Plus d'informations sur le site de l'ANSSI :** [www.cyber.gouv.fr](http://www.cyber.gouv.fr).

Version 1.0 – Mars 2024  
Licence Ouverte/Open Licence (Etabl — V1)

**AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION**  
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP  
[www.cyber.gouv.fr](http://www.cyber.gouv.fr)

