RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

SÉCURITÉ NUMÉRIQUE

10 RÈGLES D'OR À DESTINATION DES MEMBRES DES CABINETS MINISTÉRIELS

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 ;
- Police et gendarmerie.

EN SAVOIR PLUS

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

ÇA POURRAIT VOUS ARRIVER

« Soucieux d'adresser dans les temps un dossier sensible à son ministre, un membre de cabinet poursuit son travail depuis son domicile avec son ordinateur personnel. Ce dernier étant compromis, un attaquant intercepte le dossier et fait échouer le projet en faisant fuiter les données dans la presse. »

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 ou celle de votre institution.

Plus d'informations sur le site de l'ANSSI : www.ssi.gouv.fr.

Version 1.0 – Mai 2022
Licence Ouverte/Open Licence (Etalab — V1)

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.ssi.gouv.fr — communication@ssi.gouv.fr