LES 10 RÈGLES D'OR DE L'ANSSI

Agence nationale de la sécurité des systèmes d'information

1 **MÉFIEZ-VOUS DES MESSAGES SUSPECTS**
Faites attention aux messages que vous pouvez recevoir.

2 **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.

3 **METTEZ À JOUR VOS OUTILS NUMÉRIQUES**
Ordinateurs, smartphones, applications, les mises à jour proposées contiennent des correctifs de sécurité.

4 **EN DÉPLACEMENT, PRENEZ GARDE**
Ayez conscience que vous êtes entourés. Prenez garde à vos équipements, à vos conversations et faites attention aux regards malveillants sur les écrans. L'écoute passive et les fuites de données peuvent se produire lors de vos déplacements.

5 **VERROUILLEZ VOTRE ORDINATEUR**
Verrouillez votre poste de travail lorsque vous n'êtes pas à votre bureau et placez en lieu sûr tout matériel sensible.

6 **PLACEZ VOS DONNÉES DANS DES ESPACES SAUVEGARDÉS**
Veillez à placer vos données dans des espaces sauvegardés. En cas de piratage, mais également en cas de panne, de vol ou de perte de votre appareil, la sauvegarde est souvent le seul moyen de retrouver vos données.

7 **MÉFIEZ-VOUS DES SUPPORTS AMOVIBLES**
Les supports amovibles (clés USB, disques durs externes, appareils photo, cartes mémoires, CD/DVD) doivent faire l'objet d'une attention particulière. Ils pourraient contenir des programmes malveillants. N'insérez pas dans votre ordinateur une clé USB que vous auriez trouvé par hasard. Sauf en cas d'absolue nécessité, l'usage des supports amovibles est à éviter.

8 **MAÎTRISEZ VOS RÉSEAUX SOCIAUX**
Les réseaux sociaux contiennent de nombreuses informations personnelles, prenez garde à ce que vous partagez. Partager des informations concernant votre travail pourrait vous nuire.

9 **ÉVITEZ LES RÉSEAUX WI-FI PUBLICS OU INCONNUS**
Privilégiez un partage de connexion avec votre smartphone aux réseaux Wi-Fi publics. Ces réseaux Wi-Fi sont souvent mal sécurisés, et peuvent être contrôlés ou usurpés.

10 **UTILISEZ UN GESTIONNAIRE DE MOTS DE PASSE**
C'est un outil permettant de stocker et gérer de manière sécurisée un ensemble de mots de passe. KeepassXC est un outil gratuit et recommandé par l'ANSSI.

Document réalisé par le SIEEEN - juin 2025

énergies solidaires

LES 10 RÈGLES D'OR DE L'ANSSI

Agence nationale de la sécurité des systèmes d'information

1 MÉFIEZ-VOUS DES MESSAGES SUSPECTS

Faites attention aux messages que vous pouvez recevoir.

2 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.

3 METTEZ À JOUR VOS OUTILS NUMÉRIQUES

Ordinateurs, smartphones, applications, les mises à jour proposées contiennent des correctifs de sécurité.

4 EN DÉPLACEMENT, PRENEZ GARDE

Ayez conscience que vous êtes entourés. Prenez garde à vos équipements, à vos conversations et faites attention aux regards malveillants sur les écrans. L'écoute passive et les fuites de données peuvent se produire lors de vos déplacements.

5 VERROUILLEZ VOTRE ORDINATEUR

Verrouillez votre poste de travail lorsque vous n'êtes pas à votre bureau et placez en lieu sûr tout matériel sensible.

6 PLACEZ VOS DONNÉES DANS DES ESPACES SAUVEGARDÉS

Veillez à placer vos données dans des espaces sauvegardés. En cas de piratage, mais également en cas de panne, de vol ou de perte de votre appareil, la sauvegarde est souvent le seul moyen de retrouver vos données.

7 MÉFIEZ-VOUS DES SUPPORTS AMOVIBLES

Les supports amovibles (clés USB, disques durs externes, appareils photo, cartes mémoires, CD/DVD) doivent faire l'objet d'une attention particulière. Ils pourraient contenir des programmes malveillants. N'insérez pas dans votre ordinateur une clé USB que vous auriez trouvé par hasard. Sauf en cas d'absolue nécessité, l'usage des supports amovibles est à éviter.

8 MAÎTRISEZ VOS RÉSEAUX SOCIAUX

Les réseaux sociaux contiennent de nombreuses informations personnelles, prenez garde à ce que vous partagez. Partager des informations concernant votre travail pourrait vous nuire.

9 ÉVITEZ LES RÉSEAUX WI-FI PUBLICS OU INCONNUS

Privilégiez un partage de connexion avec votre smartphone aux réseaux Wi-Fi publics. Ces réseaux Wi-Fi sont souvent mal sécurisés, et peuvent être contrôlés ou usurpés.

10 UTILISEZ UN GESTIONNAIRE DE MOTS DE PASSE

C'est un outil permettant de stocker et gérer de manière sécurisée un ensemble de mots de passe. KeepassXC est un outil gratuit et recommandé par l'ANSSI.

Document réalisé par le SIEEEN - juin 2025

énergies solidaires