

La minute du PSIR

5 Mai 2021 - # 20



CONSEILS POUR SECURISER VOS USAGES PRO ET PERSO



La transformation numérique modifie en profondeur les usages et les comportements. Être connecté est devenu le quotidien. Le développement des technologies mobiles (PC portables, tablettes, smartphones) offre désormais la possibilité d'accéder, depuis presque n'importe où, à ses informations personnelles mais aussi à son système informatique professionnel : la frontière numérique entre la vie professionnelle et personnelle devient de plus en plus poreuse. Face à cette évolution, il est nécessaire d'adapter ses pratiques afin de protéger tant votre organisation, que votre espace de vie privée

Voici 10 bonnes pratiques à adopter pour la sécurité de vos usages pro-perso.

- **Utilisez des mots de passe différents** pour tous les services professionnels et personnels auxquels vous accédez, vous limiterez ainsi les risques en cas de vol de mot de passe
- **Ne mélangez pas votre messagerie professionnelle et personnelle**, vous pourriez commettre des erreurs compromettantes, notamment des erreurs de destinataires.
- **Ayez une utilisation responsable et raisonnable d'internet au travail** et limitez-vous en à un usage professionnel. Ayez à l'esprit que votre organisation est en droit de contrôler votre utilisation de la connexion qu'elle met à votre disposition. Ne l'utilisez donc pas pour des choses qui n'ont, selon vous, pas à être connues.
- **Maîtrisez vos propos sur les réseaux sociaux.**
- **N'utilisez pas de services de stockage en ligne personnel à des fins professionnelles** ou du moins sans avoir pris les mesures de sécurité qui s'imposent pour protéger les informations surtout si elles sont confidentielles.
- **Faites les mises à jour de sécurité de vos équipements régulièrement**, elles corrigent des failles de sécurité.
- **Utilisez une solution de sécurité contre les virus et autres attaques et maintenez-la à jour.** Même si aucune solution n'est totalement infaillible, de nombreux produits peuvent vous aider à vous protéger des différentes attaques comme les virus, rançongiciels, hameçonnage...
- **N'installez les applications que depuis les sites ou magasins officiels.** Méfiez-vous des sites « parallèles » qui ne contrôlent pas les applications qu'ils proposent ou qui offrent gratuitement des applications normalement payantes en téléchargement illégal : *elles sont généralement piégées.*
- **Méfiez-vous des supports USB** : si on vous en offre ou que vous en trouvez lors d'une manifestation, partez du principe qu'elle est piégée et passez-la à l'antivirus avant tout usage.
- **Évitez les réseaux Wi-Fi publics ou inconnus**, ils peuvent être contrôlés par des personnes malveillantes et ainsi récupérer au passage des informations confidentielles

NIVEAU DE DIFFICULTÉ



Sécurité informatique

PERSONNES CONCERNÉES



Pour en savoir plus, cliquer ici : [Retrouvez les 10 bonnes pratiques](#)