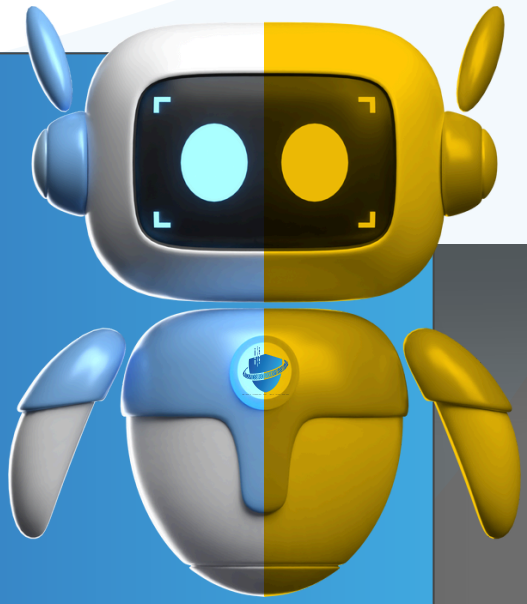
SÉCURITÉ
USAGES PRO-PERSO

CENTRE CYBER DU PACIFIQUE

EN BREF

POURQUOI C'EST IMPORTANT ?

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 entreprise* ou votre organisation, que votre espace de vie privée.



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

1. UTILISEZ DES MOTS DE PASSE DIFFÉRENTS POUR LE PRO ET PERSO
2. NE MÉLANGEZ PAS VOTRE MESSAGERIE PRO ET PERSO
3. AYEZ UNE UTILISATION RESPONSABLE D'INTERNET AU TRAVAIL
4. MAÎTRISEZ VOS PROPOS SUR LES RÉSEAUX SOCIAUX
5. N'UTILISEZ PAS DE SERVICES DE STOCKAGE EN LIGNE PERSONNEL À DES FINS PROFESSIONNELLES
6. FAITES LES MISES À JOUR DE SÉCURITÉ DE VOS ÉQUIPEMENTS
7. UTILISEZ UNE SOLUTION DE SÉCURITÉ CONTRE LES VIRUS ET AUTRES ATTAQUES
8. N'INSTALLEZ DES APPLICATIONS QUE DEPUIS LES SITES OU MAGASINS OFFICIELS
9. MÉFIEZ-VOUS DES SUPPORTS USB
10. ÉVITEZ LES RÉSEAUX WI-FI PUBLICS OU INCONNUS

▶ Voir détail page "10 BONNES PRATIQUES À ADOPTER"

SÉCURITÉ
USAGES PRO-PERSO

CENTRE CYBER
DU PACIFIQUE

10 BONNES PRATIQUES À ADOPTER

1. UTILISEZ DES MOTS DE PASSE DIFFÉRENTS POUR TOUS LES SERVICES PROFESSIONNELS ET PERSONNELS AUXQUELS VOUS ACCÉDEZ

Si vous utilisez le même mot de passe pour différents services et qu'un de ces services est piraté, un cybercriminel pourrait accéder à tous vos autres comptes (banque, messagerie, réseaux sociaux). Si ce mot de passe est aussi utilisé pour votre entreprise, cela met également en danger l'organisation.

2. NE MÉLANGEZ PAS VOTRE MESSAGERIE PROFESSIONNELLE ET PERSONNELLE

Mélanger vos deux messageries peut conduire à des erreurs de destinataires, partageant ainsi des informations professionnelles avec des contacts personnels, ou l'inverse. Cela peut compromettre la confidentialité des données de votre entreprise, surtout si votre messagerie personnelle est piratée.

3. AYEZ UNE UTILISATION RESPONSABLE D'INTERNET AU TRAVAIL

Même si l'usage personnel d'Internet au travail est toléré, évitez les pratiques répréhensibles comme le téléchargement illégal ou des publications sensibles. Votre entreprise est en droit de surveiller l'utilisation de sa connexion Internet. N'utilisez pas la connexion professionnelle pour des activités que vous ne voulez pas voir découvertes.

4. MAÎTRISEZ VOS PROPOS SUR LES RÉSEAUX SOCIAUX

Sur les réseaux sociaux, évitez de parler de votre travail ou de votre entreprise, car les propos peuvent être interprétés et diffusés sans que vous ayez le contrôle. Verrouillez vos profils pour limiter l'accès à vos informations et réfléchissez avant de poster.

5. N'UTILISEZ PAS DE SERVICES DE STOCKAGE EN LIGNE PERSONNEL À DES FINS PROFESSIONNELLES

Les services de stockage en ligne gratuits pour les particuliers ne garantissent pas toujours un niveau de sécurité suffisant pour protéger les informations professionnelles. Utilisez des solutions professionnelles et sécurisées approuvées par votre employeur.

SÉCURITÉ
USAGES PRO-PERSO

CENTRE CYBER
DU PACIFIQUE

10 BONNES PRATIQUES À ADOPTER

6. FAITES LES MISES À JOUR DE SÉCURITÉ DE VOS ÉQUIPEMENTS

Installez les mises à jour de sécurité dès qu'elles sont disponibles sur vos appareils personnels et professionnels. Elles corrigent des failles critiques qui pourraient être exploitées par des cybercriminels pour accéder à vos données ou à celles de votre entreprise.

7. UTILISEZ UNE SOLUTION DE SÉCURITÉ CONTRE LES VIRUS ET AUTRES ATTAQUES

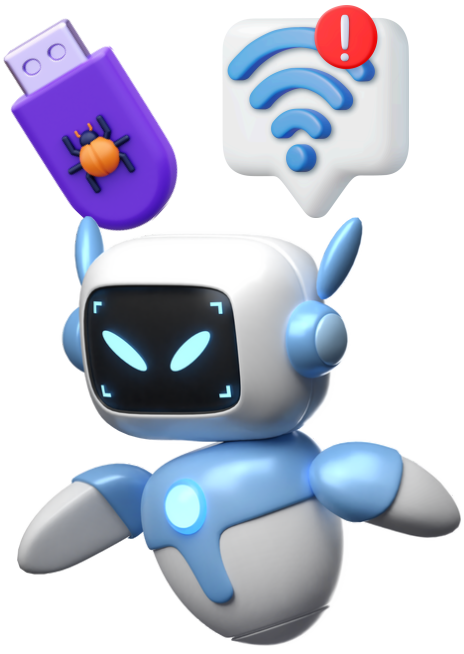
Protégez vos appareils avec des solutions antivirus et maintenez-les à jour. Cela réduit le risque d'infections par des virus, rançongiciels, ou autres attaques. Si un cybercriminel prend le contrôle de vos équipements, il pourrait également accéder au réseau de votre entreprise.

8. N'INSTALLEZ DES APPLICATIONS QUE DEPUIS LES SITES OU MAGASINS OFFICIELS

Téléchargez vos applications uniquement depuis des sources officielles pour limiter les risques de virus. Les sites non officiels ou les téléchargements illégaux peuvent contenir des programmes malveillants. Consultez les avis et les téléchargements avant d'installer une nouvelle application.

9. MÉFIEZ-VOUS DES SUPPORTS USB

Ne branchez jamais une clé USB dont vous ignorez la provenance, car elle pourrait être infectée et compromettre vos équipements. Utilisez des clés USB distinctes pour vos usages personnels et professionnels afin d'éviter que l'infection de l'un n'affecte l'autre.



10. ÉVITEZ LES RÉSEAUX WI-FI PUBLICS OU INCONNUS

Les réseaux Wi-Fi publics ou inconnus peuvent être utilisés par des cybercriminels pour intercepter vos données. Ne transmettez jamais d'informations confidentielles via ces réseaux, car cela pourrait entraîner le vol de vos identifiants ou informations bancaires.