




Les bonnes pratiques de cybersécurité


Les mots de passe




 Utilisez des mots de passe suffisamment complexes, et changez-les au moindre soupçon

 Utilisez un mot de passe différent pour chaque service

 Activez la « double authentification » lorsque c'est possible

 Ne communiquez jamais votre mot de passe à un tiers


 Utilisez un gestionnaire de mots de passe (do4Safe)

1234

Changez les mots de passe définis par défaut des différents services auxquels vous accédez


Les appareils

 Mettez en place des codes d'accès

 Utilisez une solution de sécurité contre les virus et autres attaques

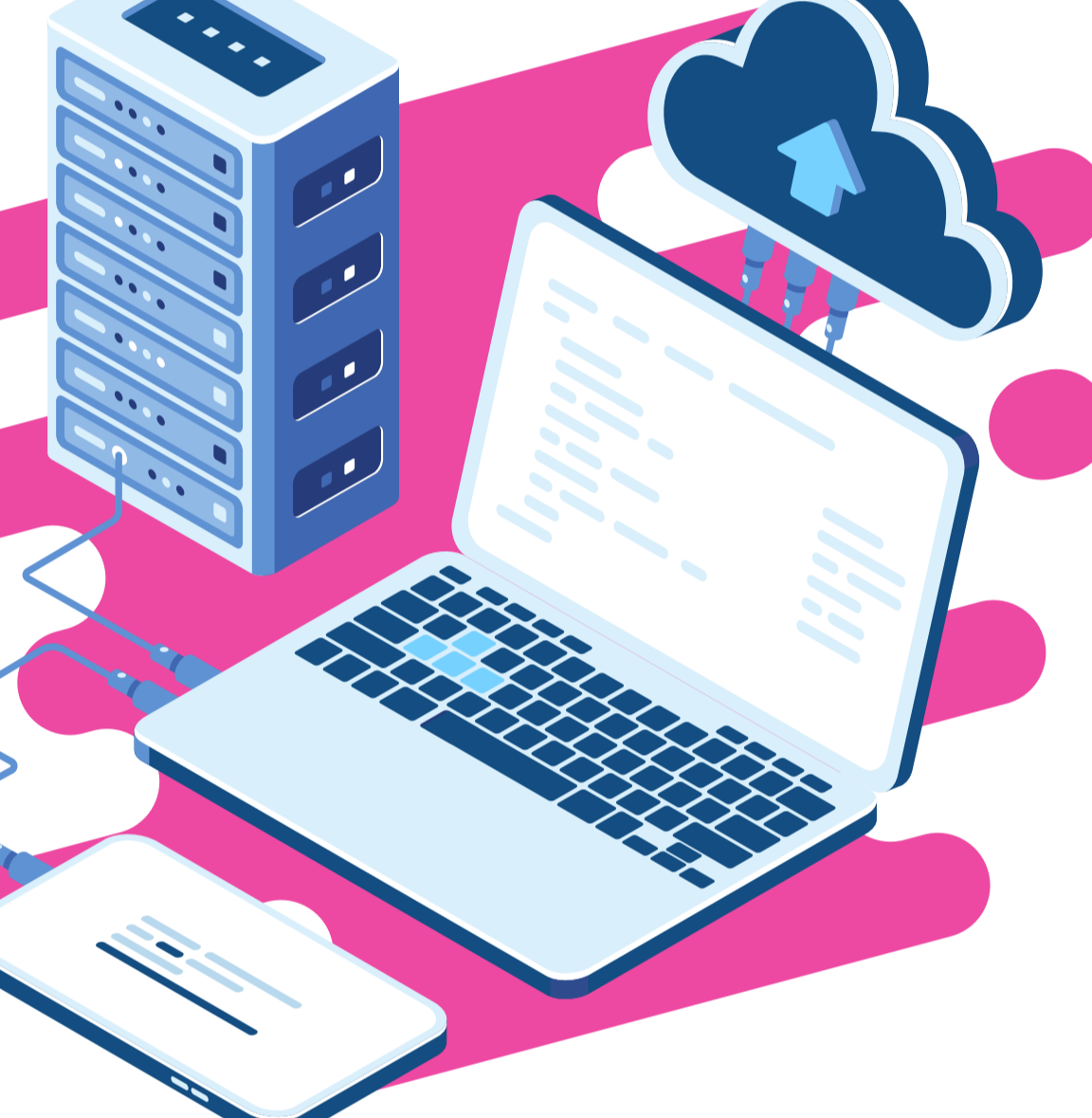
 Faites des sauvegardes


 Appliquez les mises à jour de sécurité


 Évitez les ordinateurs et les réseaux wifi publics




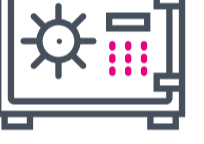
Les sauvegardes




 Identifiez les appareils et supports contenant des données

 Planifiez vos sauvegardes


 Effectuez des sauvegardes régulières de vos données


 Protégez vos sauvegardes

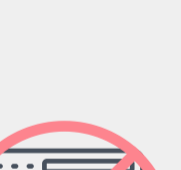
 Testez vos sauvegardes et vérifiez le support de sauvegarde

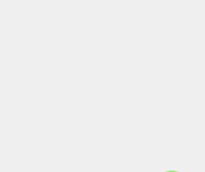
Les mises à jour

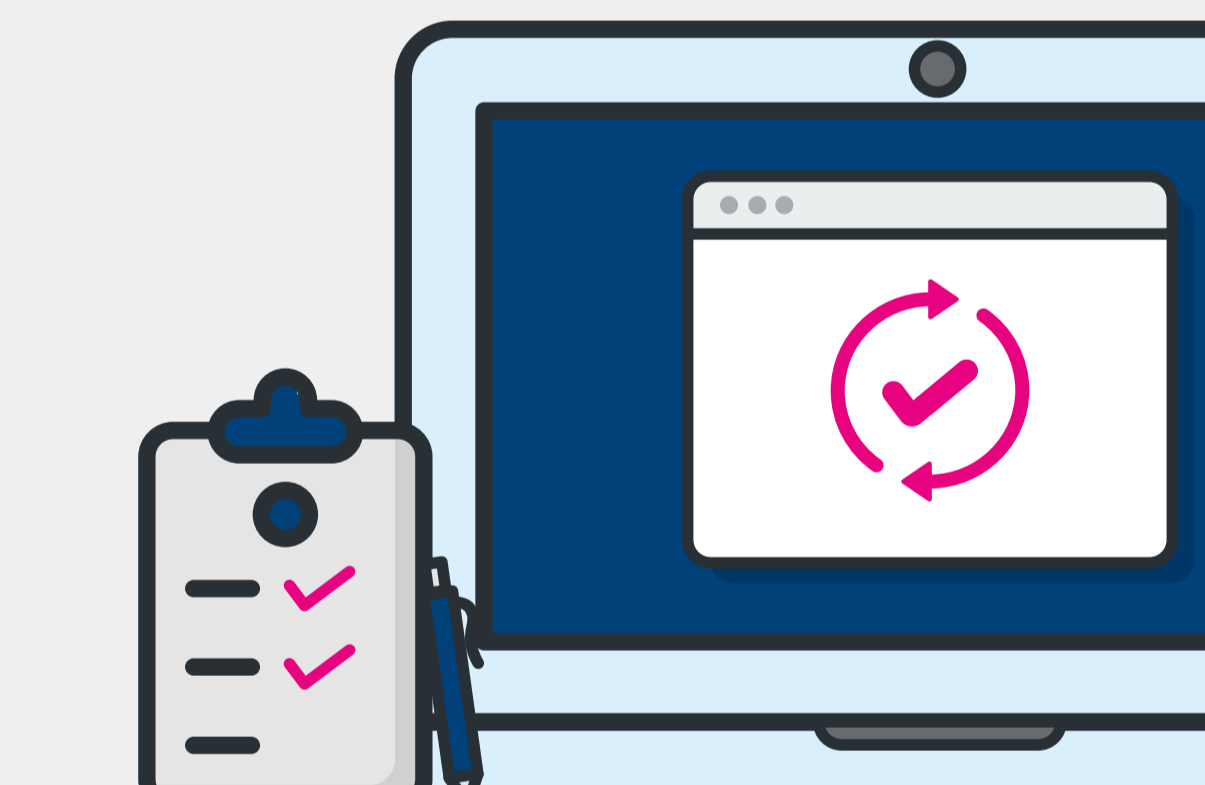
 Identifiez l'ensemble des appareils et logiciels utilisés

 Pensez à mettre à jour sans tarder l'ensemble de vos appareils et logiciels

 Téléchargez les mises à jour uniquement depuis les sites officiels


 Méfiez-vous des fausses mises à jour sur internet


 Activez l'option de téléchargement et d'installation automatique des mises à jour



Le télétravail




 N'ouvrez pas les pièces jointes et les liens provenant de destinataires inconnus, ou dont le titre ou le format paraissent incohérents

 Ne branchez pas de supports de stockage (USB) inconnus

 Ne mélangez pas votre messagerie professionnelle et personnelle

 Maîtrisez vos propos sur les réseaux sociaux

 N'installez des applications que depuis les sites ou magasins officiels

 N'utilisez pas de services de stockage en ligne personnel à des fins professionnelles



@SecuriteVFLIT

Alertes, actus et bonnes pratiques : restez en veille sur notre compte Twitter dédié à la sécurité informatique !

Vous faciliter l'IT



ExpertCyber est un label gouvernemental certifiée par l'Afnor, visant à guider les TPE, PME et collectivités vers des entreprises de sécurité informatique, et avec lequel nous sommes labellisés sur Cybermalveillance.gouv.fr.