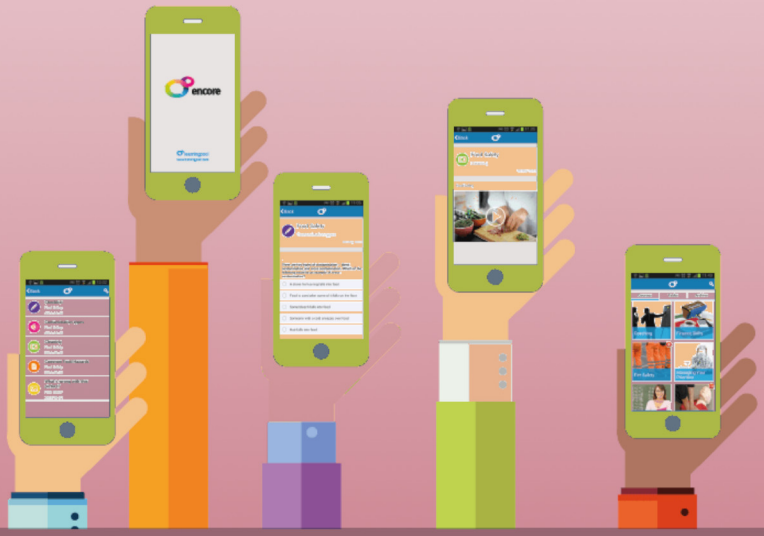
الوكالة الوطنيّة للسّلامة المعلوماتيّة

Agence Nationale de la Sécurité Informatique



BYOD (Bring Your Own Device)

Recommandations et bonnes pratiques

tunCERT

Tunisian Computer Emergency ResponseTeam

BYOD (Bring Your Own Device)

Recommandations et bonnes pratiques

Qu'est-ce que le BYOD ?

Le BYOD « Bring your Own device » désigne l'usage d'équipements informatiques personnels dans un contexte professionnel (smartphone, tablette, Pc ...). Les utilisateurs professionnels se connectent de plus en plus à n'importe quel réseau via leurs propres appareils pour accéder aux applications et données de leurs entreprises.

Quels sont les risques ?

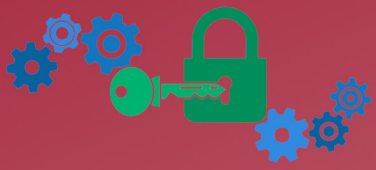
A défaut de protection, ces appareils peuvent représenter une menace pour la sécurité des applications et des données de l'entreprise. En effet, un appareil non sécurisé peut compromettre la sécurité de tout le système d'information et peut être exploité pour propager les malwares (logiciels malveillants).

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

tunCERT
Tunisian Computer Emergency ResponseTeam

Recommandations et bonnes pratiques pour les entreprises

Contrôler l'accès distant par un dispositif d'authentification robuste de l'utilisateur.



Mettre en place des mesures de chiffrement des flux d'informations (VPN, HTTPS, etc...).

Prévoir une procédure de sécurité en cas de panne ou perte du terminal (déclaration de perte, mise à disposition d'un équipement alternatif, suppression à distance des données professionnelles stockées, etc...)

Exiger le respect de la politique de sécurité tel que le verrouillage du terminal avec un mot de passe conforme aux bonnes pratiques et l'utilisation d'un antivirus à jour.

Sensibiliser les utilisateurs aux risques, formaliser les responsabilités de chacun et préciser les précautions à prendre dans une charte.

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

tunCERT
Tunisian Computer Emergency ResponseTeam

Recommandations et bonnes pratiques pour les employés

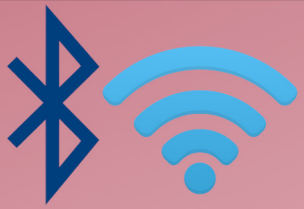
Veiller à appliquer régulièrement les mises à jour du terminal et activer le verrouillage automatique des équipements.
Utiliser un mot de passe, empreinte digitale ou schéma pour le déverrouillage.

Choisir un mot de passe robuste pour l'accès aux différents comptes et le changer périodiquement.

Ne jamais utiliser le même mot de passe pour les comptes personnels et professionnels et optimiser la sécurité des accès en optant pour l'authentification forte (ou à 2 facteurs).

Décocher l'option «Connexion automatique» pour les applications professionnelles. Il est conseillé de re-saisir le mot de passe à chaque authentification.

Se méfier des sites douteux / applications tierces qui viennent s'intégrer aux réseaux sociaux et ne jamais cliquer sur les liens suspects diffusés via ces réseaux.



Désactiver les fonctionnalités wifi et Bluetooth lorsqu'on n'en a pas besoin.

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

tunCERT
Tunisian Computer Emergency ResponseTeam

tunCERT
Tunisian Computer Emergency ResponseTeam

الوكالة الوطنيّة للسّلامة المعلوماتيّة

Agence Nationale de la Sécurité Informatique

Votre partenaire en sécurité de l'information...

CONTACTEZ-NOUS !

https://www.facebook.com/ansitn/

https://www.linkedin.com/in/ansi-tuncert-80bb4b172/

www.ansi.tn

ansi@ansi.tn

71 846 020

49, Avenue Jean Jaurès, 1000 Tunis