الوكالة الوطنيّة للسّلامة المعلوماتيّة

Agence Nationale de la Sécurité Informatique

RECOMMANDATIONS ET BONNES PRATIQUES POUR PROTÉGER VOTRE IDENTITÉ NUMÉRIQUE

Avril 2020

tunCERT

Tunisian Computer Emergency ResponseTeam

Recommandations de sécurité liées aux mots de passe

UTILISER UN MOT DE PASSE UNIQUE POUR CHAQUE SERVICE DE MESSAGERIE

Choisissez des mots de passe différents pour vos messageries personnelles et professionnelles

NE PAS CRÉER UN MOT DE PASSE AVEC DES INFORMATIONS PERSONNELLES

Évitez les mots de passe composés de numéro de téléphone, d'une date de naissance ou d'un identifiant tel que le numéro de la carte d'identité nationale.
Ces mots de passe sont très faciles à deviner !

ADOPTER DES RÈGLES DE GESTION DES MOTS DE PASSE

Les mots de passe sont des informations critiques que vous devez créer vous même et les stocker,si besoin, **dans une machine sécurisée et évitez les supports papiers !**

MODIFIER IMPÉRATIVEMENT LES MOTS DE PASSE PAR DÉFAUT ET LES RENOUVELER PÉRIODIQUEMENT

Évitez les mots de passe simples lors du renouvellement des mots de passe, optez plutôt pour des mots de passe complexes composés de chiffres, lettres et caractères spéciaux !

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Pour plus de conseils, veuillez visiter notre site : https://www.ansi.tn/

tunCERT
Tunisian Computer Emergency ResponseTeam

Recommandations de sécurité liées aux boites e-mails

Utiliser un mot de passe robuste et difficile à deviner tout en veillant à le changer régulièrement.
(Veuillez consulter le document 1 relatif à la sécurité des mots de passe)

Activer l'authentification à 2 facteurs (authentification forte).
Cela va renforcer, d'une manière drastique, la sécurité de votre boite e-mail.

Vérifier l'authenticité de l'identité des expéditeurs avant la consultation de chaque e-mail et, en cas de doute, il ne faut pas l'ouvrir.

Ne pas répondre aux emails non sollicités demandant des informations personnelles ou des rançons.
En effet, ces e-mails sont des scams qui essayent de faire peur à leurs victimes et exploitent cet état de panique pour les manipuler.

Scanner les pièces jointes avec un antivirus mis à jour avant de les ouvrir.
En cas de doute quant à la source ou la véracité de l'identité de l'expéditeur, il ne faut pas ouvrir la pièce jointe.

Ne pas enregistrer les identifiants et les mots de passe au niveau du navigateur web tout en veillant à ce que ce dernier soit à jour. Enfin, il ne faut pas oublier de fermer la session après avoir consulté la boite e-mail.

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Pour plus de conseils, veuillez visiter notre site : https://www.ansi.tn/

tunCERT
Tunisian Computer Emergency ResponseTeam

Recommandations de sécurité liées aux réseaux sociaux

Ne jamais utiliser votre compte personnel pour gérer votre page publique

Pour la gestion de la page Facebook ou compte Twitter, il est recommandé de crée un second compte dedié uniquement à cette tâche car cela va minimiser le risque de compromettre la sécurité de la page si jamais vous perdez l'accès à votre compte personnel car ce dernier est plus exposé au risque de piratage.

Configurer les paramètres de confidentialité du compte

Protéger le compte en examinant les alertes de connexion activées et supprimer les appareils non reconnus.

Activer l'authentification forte (à 2 facteurs) pour plus de sécurité

Que ce soit pour le compte personnel ou professionnel, il est fortement recommandé d'activer l'authentification forte pour protéger les accès (recevoir un code de connexion sous forme de texto sur votre smarthphone) et activer l'option recevoir une alerte en cas de connexions non reconnues.

Protéger les informations personnelles

Il est possible de voir et de contrôler les applications et les services auxquels le compte accède avec Facebook, ainsi que les paramètres de géolocalisation.

Faire attention aux applications tierces

Il faut éviter les applications tierces qui viennent s'intégrer aux réseaux sociaux et ne jamais cliquer sur des liens suspects diffusés via ces réseaux .

Protéger les appareils utilisés pour la connexion

Activer le verrouillage automatique du Smartphone/ de la tablette et utiliser un mot de passe, empreinte digitale ou schémas pour le déverrouiller. Enfin, Il faut, aussi, se déconnecter du compte si on utilise un Pc.

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Pour plus de conseils, veuillez visiter notre site : https://www.ansi.tn/

tunCERT
Tunisian Computer Emergency ResponseTeam

La sécurité informatique ne s'improvise pas....

tunCERT
Tunisian Computer Emergency ResponseTeam

الوكالة الوطنيّة للسّلامة المعلوماتيّة

Agence Nationale de la Sécurité Informatique

CONTACTEZ-NOUS !

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

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

https://twitter.com/ATuncert

www.ansi.tn

49, Avenue Jean Jaurès, 1000 Tunis

ansi@ansi.tn

71 846 020