République Tunisienne

Ministère des Technologies de la Communication

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Guide de sécurité Informatique

Les dix commandements pour sécuriser votre PC

Public Cible	Date de Publication	Date de Révision	Version
Simple Utilisateur	Mai 2008	Mai 2009	02

Les dix commandements pour sécuriser votre PC

1- Installer un antivirus et mettez-le régulièrement à jour (au strict minimum une fois par semaine), en activant l'option de mise à jour automatique de l'anti-virus (base de signatures). A noter que beaucoup d'éditeurs offrent des versions gratuites pour usage domestique (ordinateur personnel)

2- Ne pas ouvrir d'email ou de pièces jointes de messages suspects (en anglais, source inconnue…..)

Être méfiant des pièces jointes aux e-mails, même si celui-ci apparaît comme avoir été envoyé d'une source connue, car certains virus se propagent en utilisant l'adresse mail du client qu'ils infectent.

3- « Patcher » votre système

Les systèmes d'exploitation et les applications utilisées, renferment des failles de sécurité (erreur de programmation), qui doivent être corrigés via l'application des « Patchs » correspondants, publiés par l'éditeur. Un système sans mise à jours de sécurité est un système vulnérable, ouvert à tout type d'attaques (virus, attaques directes).

4- Ne pas partager l'accès à son ordinateur

Éviter les partages (non protégés par mot clé) de répertoires sur le réseau, et éviter aussi les partages P2P qui servent à échanger les fichiers sur Internet (KaZaa, …), qui constituent une source de vulnérabilité dangereuse. Éviter aussi l'échange de fichier sur les messageries instantanées (Chat).

5- Protéger son ordinateur contre les intrusions

Utiliser un « Firewall personnel ». Ce logiciel permet de protéger votre PC contre les attaques actives, en contrôlant les communications entrantes et sortantes, et en alertant l'utilisateur pour donner la permission au trafic. A noter que beaucoup d'éditeurs offrent des versions gratuites pour usage domestique

6- Ne pas visiter les sites web douteux

En y accédant, certains sites douteux peuvent vous infecter par des moyens détournés (aciveX infectés, failles des explorateurs…) ou via les téléchargements de fichiers offerts (chevaux de Trois, spywares, virus,…). Pour vous en protéger, installez un Firewall PC et un outil anti-spyware.

7- Utiliser des mots de passe difficiles à deviner.

Combiner des majuscules, minuscules, chiffres, et des caractères spéciaux, et surtout s'assurer que la taille du mot de passe dépasse les dix caractères, car des outils (dits de crack) peuvent retrouver (casser) les mots de passe simples en quelques secondes. Ne jamais prêter vos mots de passe et éviter de les exposer, en les notant sur des bouts de papier, ...

8- Sauvegarder régulièrement les données importantes

Sauvegarder régulièrement vos données sur des supports amovibles (disquettes, CDs, …), car un virus ou une panne physique pourraient endommager les fichiers et les données stockées sur le disque.

9- Ne pas laisser son poste connecté en réseau (et surtout à l'Internet), sans contrôle

Un poste sans contrôle est sujet à tout type de malversations (entre autres physiques). Ainsi, prière de verrouiller l'accès réseau ou fermer votre PC, en cas d'absence même temporaire de votre poste de travail, une personne malveillante pourrait profiter de votre absence pour accéder physiquement ou via le réseau, à votre poste et l'endommager ou compromettre sa sécurité (installer des programmes espions, …).

10- Avoir la bonne réaction!

En cas de doute d'infection ou d'attaque active sur votre ordinateur. Il est primordial de ne pas paniquer et par prudence de se déconnecter temporairement du réseau, puis de diagnostiquer le problème via les outils installés (lancer un scan complet par l'antivirus de tous les disques, inspecter le log de votre Firewall, ..) et ne pas hésiter à contacter l'Agence pour toute assistance nécessaire.