République Tunisienne

Ministère des Technologies de l'Information et de la Communication

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Sécurité du poste de travail

Principaux risques

& Mesures de protection

Sommaire

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

1. Les principaux risques.
2. Protection de poste de travail contre le vol, la perte et les accès illégitimes.
3. Endommagement et disfonctionnement.
4. La perte des données électroniques.
5. L’infection virale.
6. Chiffrement des supports de stockage.
7. Configuration maîtrisée et mise à jour régulièrement.
8. Mots de passe robustes et personnels.

1. Les principaux risques

- Vol et Perte
- Endommagement
- Disfonctionnement
- Infection par les virus, les troyens, les vers, logiciels espion (spyware) et les portes dérobées
- Vol de données
- Manipulation à distance
- Espionnage

2. Protection contre le vol, la perte et les accès illégitimes:

Les bonnes pratiques contre le vol :

- Au bureau:

✓ Fermer à clé la porte de son bureau

✓ Attacher l'ordinateur portable avec un câble

- Dans les transports:

✓ Ne pas laisser son matériel en vue (dans une voiture, train, etc.)

✓ Ne pas laisser son matériel sans surveillance.

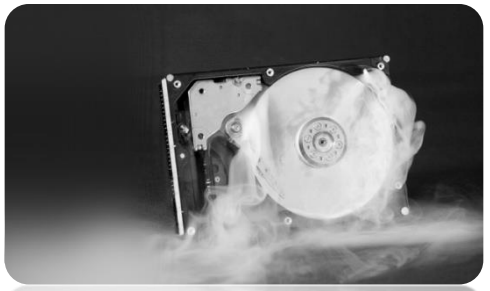
✓ Mettre un signe distinctif sur l'appareil et sa housse pour le surveiller plus facilement et éviter les échanges volontaires ou involontaires.

2. Protection contre le vol, la perte et les accès illégitimes:

Les bonnes pratiques vis à vis du prêt à des tiers :

- ✓ Le prêt ne peut être que très ponctuel dans le temps en cas de réelle nécessité (votre poste de travail n'est pas une console de jeux …).

- ✓ Rester près de la personne qui utilise votre ordinateur pour vérifier qu'il n'accède pas à des données professionnelles et qu'il ne cherche pas à modifier la configuration de votre ordinateur (installation de logiciels, etc.).



3. Endommagement et disfonctionnement

- **Arrêt brutal du système :** il ne faut jamais interrompre un processus ou une application en cours d'exécution, ni arrêter brutalement un système d'exploitation. S'il le faut, n'hésitez pas à perdre quelques minutes pour donner une chance à un processus, bloqué en apparence, de se terminer proprement. Évitant peut-être un «plantage» grave, vous gagnerez un temps précieux et éviterez de perdre des informations.

- **Obésité du système de fichiers :** les disques se remplissent à une vitesse effrayante. Certains utilisateurs atteignent sans ambages des taux de remplissage supérieurs à 80 %. Si c'est votre cas, vous flirtez dangereusement avec l'incident car un disque trop plein gêne.
- **Système corrompu :** Si votre machine affiche systématiquement un message d'erreur (au démarrage par exemple), cela doit vous alerter.
- **Bogues des logiciels :** Faites toujours preuve de lucidité. Les outils informatiques ne viennent jamais sans leur ration de bogues et sont susceptibles d'engendrer des erreurs

4. La perte des données électroniques

Il existe un moyen simple et très efficace de se protéger contre la perte des données : la sauvegarde systématique et quotidienne des données. Il faut conserver plusieurs copies des données importantes. La sauvegarde (multiple) est la seule méthode fiable qui vous préserve à coup sûr de la perte malencontreuse d'informations.

- ✓ Sauvegardez vos données vitales sur un support amovible : sur CD-Rom, réinscriptible ou non, ou sur bande. Vous pouvez aussi investir dans un disque dur externe sur lequel vous pourrez très facilement obtenir une copie très complète de vos données.
- ✓ Dans votre profession, si votre administrateur vous a alloué un espace de travail sur le serveur de l'entreprise, n'hésitez pas non plus à conserver une image de vos données vitales sur le disque local de votre ordinateur.

4. La perte des données électroniques

- ✓ Aujourd'hui, tout le monde possède sa propre clé USB. Utilisez cet espace pour stocker les données les plus récentes (entre deux sauvegardes). Si vous vous déplacez fréquemment avec votre ordinateur portable, ne rangez pas la clé USB dans la housse de l'ordinateur ! Mettez-la dans votre poche.

- ✓ Archivez les données sur un support non réinscriptible (CD-Rom par exemple). Fabriquez deux jeux d'archives que vous ne stockerez pas physiquement au même endroit.

4. La perte des données électroniques

- ✓ **Activer et paramétrer l'enregistrement automatique des documents :**

Si vous utilisez Microsoft Office, vous pouvez configurer Word, Excel et Powerpoint afin que ceux-ci enregistrent régulièrement une copie de sauvegarde des documents en cours d'édition. Dans Word par exemple, déroulez le menu Outils, sélectionnez Options, puis cliquez sur l'onglet Enregistrement. En cas de panne secteur ou d'extinction intempestive de votre machine, vous pourrez restaurer votre travail.

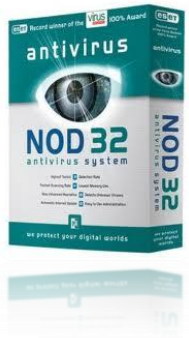
5. L’infection virale:

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Votre ordinateur connecté sur internet est la cible de toutes sortes d’attaques virales et de vers , l’infection peut même venir d’une clé USB infectée , installez un bon antivirus .

- ✓ Il existe des antivirus gratuits et efficaces

- ✓ Et des antivirus payants avec firewall intégré et autres fonctions Intéressantes



- ✓ Un antivirus qui n’est pas à jour ne protège pas.

6. Chiffrement des supports de stockage (postes nomades, clés, disques, etc.):

Les postes de travail sont de plus en plus légers et portables, leur exposition au vol a considérablement augmenté ces dernières années.

Or le poste de travail contient les données de travail mais également tous les codes d'accès aux réseaux, à la messagerie, aux applicatifs ainsi que les certificats électroniques permettant l'accès aux services en ligne et la signature de messages et de documents.

6. Chiffrement des supports de stockage (postes nomades, clés, disques, etc.):

- ✓ Il est indispensable de chiffrer les supports de stockage de données exposés au vol, en premier lieu les disques durs des PC portables.

- ✓ De même tout support amovible peut facilement être égaré ou volé, en particulier, il convient donc de chiffrer également les disques USB externes.

- ✓ Le chiffrement des disques internes et externes s'effectue en suivant les recommandations de votre informaticien. Ne tentez pas de le faire seul, le risque de perdre toutes vos données et de rendre inutilisable votre ordinateur est important !

- ✓ Les clés USB ne doivent être utilisées que pour transférer les données et non pas comme un moyen de stockage (risque de perte de données important).

7. Configuration maîtrisée et mise à jour régulièrement :

Au quotidien des dizaines de failles sont découvertes dans les systèmes (Windows, MacOS, Linux, etc.) et logiciels (Acrobat Reader, Outlook, Word, etc.) qui équipent le poste de travail, ces failles sont très rapidement exploitées par des virus ou par des kits que mettent en ligne les pirates les plus expérimentés.

- ✓ Il est donc important de désactiver les programmes qui ne sont pas indispensables au bon fonctionnement du poste de travail, ils sont autant de portes que les pirates pourront utiliser pour tenter de pénétrer sur ce poste.

- ✓ Il convient d'utiliser au quotidien et en particulier pour naviguer sur internet un compte ne possédant pas les privilèges «administrateur».

7. Configuration maîtrisée et mise à jour régulièrement :

- ✓ Il convient de désactiver l'exécution automatique des média amovibles.
- ✓ Il est indispensable de s’abonner à un service de mise à jour qui permette de garantir une mise à jour « au fil de l’eau » des principaux composants présents sur les postes de travail et des bases de signatures des virus découverts.
- ✓ Il est utile de protéger le poste de travail par un pare feu qui filtrera les tentatives d’accès illicites depuis Internet.

8. Mots de passe robustes et personnels:

Le mot de passe est la clé d'accès à l'information, cette clé doit être personnelle et suffisamment complexe pour ne pas pouvoir être trop facilement découverte – il existe des organisations qui louent de puissantes machines ou des réseaux de machines pour tenter de casser les mots de passe des utilisateurs qui détiennent des informations monnayables.

8. Mots de passe robustes et personnels:

- ✓ Un mot de passe doit rester personnel, pas de mot de passe partagé entre plusieurs utilisateurs.

- ✓ Un mot de passe doit être suffisamment complexe (utilisation d'un mélange de lettres, chiffres et ponctuation, longueur minimum de 8 à 15 caractères en fonction du risque acceptable pour l'utilisateur et de l'effort qu'il est prêt à produire pour se protéger).

- ✓ Un mot de passe doit être changé assez régulièrement, tous les trois mois c'est bien, plus fréquement c'est encore mieux !

- ✓ Un mot de passe doit être changé dès que l'on soupçonne sa compromission (vol ou perte du PC, divulgation à un tiers, etc.)

8. Mots de passe robustes et personnels:

- ✓ Il est recommandé d'utiliser des mots de passe différents sur chacun des sites sur lesquels on se connecte. Comme cela est humainement très difficile, il est conseillé d'utiliser un outil de gestion des mots de passe qui permet de n'avoir qu'un seul mot de passe à retenir pour déverrouiller le coffre-fort contenant l'ensemble des mots de passe.

- ✓ Un mot de passe ne doit pas être accessible sans protection (par exemple affiché sur un post-it collé sur le tableau ou bien en vue sur le bureau ...)

- ✓ Un ordinateur allumé avec une session utilisateur ouverte, laissé sans surveillance, même peu de temps (pause-café, etc.) permet à un intrus d'usurper facilement votre identité sans votre mot de passe principal et même de voler les autres mots de passe présents sur le poste de travail.

www.ansi.tn
http://tuncert.ansi.tn

N’hésitez pas à demander l’assistance du personnel du tunCERT de l’ANSI :

E-mail : assistance@ansi.tn

Tél : 71 843 200

94 avenue Jugurtha, Mutuelleville – 1002 Tunis - 94 شارع يوغرطة، موتيال فيل 1002 تونس

Fax +216 71 846 363 : الفاكس - Tel: +216 71 846 020 :الهاتف

ansi@ansi.tn **www.ansi.tn**