Aix-Marseille Université

GUIDE RESUME DES BONNES PRATIQUES INFORMATIQUES POUR LES UTILISATEURS

V04

25/02/2016

Table des matières

Ce guide résumé des bonnes pratiques est destiné à tous les utilisateurs au sein d'AMU. Il n'est pas exhaustif mais les recommandations qu'il contient permettront d'éviter la majorité des problèmes couramment rencontrés.

En environnement professionnel habituel

Règles générales

● Lire la charte informatique de votre établissement.
● Connaitre les usages et les ressources disponibles de votre structure (département / laboratoire / service) : un intranet est disponible à cet effet au sein d'AMU.
● Connaître votre CSSI (Correspondant Sécurité des Systèmes d'Informations), si vous travaillez dans un laboratoire ou une structure de recherche.
● En cas d'incident : créez un ticket de demande d'intervention et pour les laboratoires et organismes de recherche : « invitez » votre CSSI sur ce ticket.

Règles de sécurité appliquées

● Ne jamais donner son nom de connexion (login)/mot de passe, même pour dépanner quelqu'un.
● Ne pas noter son nom de connexion / mot de passe sur un document papier (exemple : un post-it collé sur le bureau, l'écran ou sous le clavier).
● Ne pas copier de données professionnelles sur des médias externes (clés USB, disques dur externes, etc.) car ils peuvent être perdus, copiés ou volés. En cas de nécessité de cette action de copie sur support externe, celui-ci doit être chiffré au moyen d'un logiciel dédié (validé par l'établissement).
● Si vous travaillez dans une structure de recherche : s'assurer que vos sauvegardes sont effectuées (volumétrie, périodicité, mode de restauration, etc.).
● Lors de la réception d'un courriel vous demandant des informations personnelles/professionnelles ou vous invitant à suivre un lien internet, ne pas cliquer sur :
- un lien internet présent dans le corps du texte,
- une image présente ou à charger,
- un fichier attaché, joint au courriel,
sauf à avoir la certitude de son expéditeur.
Cela évitera le vol de données personnelles/professionnelles, ainsi que beaucoup de virus.

Règles particulières

● Ne pas utiliser d'outils propriétaires de type Gmail, Yahoo, Skype, Dropbox, etc. pour des échanges professionnels.
● En général, des outils similaires sont proposés dans votre environnement numérique de travail (messagerie, calendrier, échange de fichier, AMUBox etc.).
● Dans les structures de recherches, les CSSI sont invités à consulter le site gouvernemental du Portail de la Sécurité Informatique : http://www.securite-informatique.gouv.fr

Si vous administrez des machines (laboratoires notamment) :

Règles fondamentales

Sous Windows

● Activez les mises à jour automatiques de sécurité avec Windows Update.
● Ne travaillez pas avec le compte « Administrateur », mais créez un utilisateur doté de droits limités (avec option données privées).
● Activez le firewall de Windows.
● Installez un antivirus.
● Séparez les données utilisateurs, des données systèmes.
● Effectuez des sauvegardes régulières.

Sous Linux & Mac

● Activez les mises à jour automatiques de sécurité et d'application.
● Activez le firewall Linux ou Mac déjà installé.
● Ne travaillez pas avec le compte « Administrateur », mais créez un utilisateur doté de droits limités (avec option données privées).
● Effectuez des sauvegardes régulières.

Les modalités de sauvegarde pour éviter la perte de données

Les sauvegardes peuvent être réalisées sous plusieurs formes :

● En « local » :
  - Une copie de fichier est effectuée sur une deuxième disque dur interne (ou « partition » différente de l'unique disque dur),
  - Sur support externe à l'ordinateur :
    - Clé USB,
    - Disque dur externe,
    - Serveur de sauvegarde situé dans le laboratoire (NAS)

● En « central » :
  - Sur un dossier partagé sur un serveur administré par le service informatique,
  - Sur la plateforme de sauvegarde « AMUBox », mise en place par l'établissement.
    Ce dispositif demeure être le plus sûr.

Autres règles

● Mettez à jour les applications.
● Vérifiez que les mises à jour de votre antivirus s'effectuent régulièrement.

Règles de confidentialité

● Utilisez des mots de passe d'au moins 8 caractères (avec majuscules, chiffres et caractères spéciaux).
● Utilisez l'option de chiffrage du disque lors de l'installation du système (directement sous Linux par exemple ou avec une puce TPM sous windows).
● Chiffrez les données (en cas de perte ou de vol).
Sur internet :
● Ne donnez pas d'information personnelle, car ce que vous publiez sur Internet y demeure et votre identité n'est jamais vraiment secrète.
● Ne donnez jamais vos identifiants/mots de passe.
● Lors de l'utilisation d'ordinateurs partagés, une fois la navigation terminée, effacez les données du cache internet.
● Apprenez à reconnaître un site fiable à son adresse (URL). Si elle contient une faute d'orthographe ou des chiffres, si son nom n'est pas en rapport avec l'objet du site web auquel vous souhaitez accéder, il peut s'agir d'un site de phishing/hameçonnage qui cherche à subtiliser des informations confidentielles. Les mêmes recommandations s'appliquent aux **contenus des courriels** qui vous poussent à cliquer sur un lien, pour accéder à un site web.
● N'inscrivez votre numéro de carte bleue que sur des sites réputés fiables et quand le cadenas en bas à droite de votre écran est fermé, indiquant un site sécurisé avec le protocole https. **Privilégiez l'utilisation de E-cartes bleues** (lorsque cela est possible).

En déplacement

Vous trouverez ci-dessous une version simplifiée du "Passeport aux voyageurs" édité par l'ANSSI.

Règles de base

● Respectez les règles de sécurité de votre organisme.
● Prenez connaissance de la législation locale.
● Utilisez de préférence du matériel dédié aux missions (ordinateurs, téléphones, supports amovibles, etc.), contenant le minimum d'informations.
● Sauvegardez les données que vous emportez.
● Evitez de partir avec vos données sensibles. Récupérez-les en accédant au réseau de votre organisme avec une liaison sécurisée.

Pendant la mission

● Gardez vos appareils, supports et fichiers avec vous. Ne les laissez pas dans un bureau ou dans une chambre d'hôtel.
● Utilisez un logiciel de chiffrement pendant le voyage.
● Ne communiquez pas d'information confidentielle en clair sur votre téléphone mobile ou tout autre moyen de transmission de la voix.
● Pensez à effacer l'historique de vos appels et de vos navigations (données en mémoire cache, cookies, mot de passe d'accès aux sites web et fichiers temporaires).
● En cas d'inspection ou de saisie par les autorités, informez votre organisme, fournissez les mots de passe et clés de chiffrement, si vous y êtes contraint par les autorités locales.
● En cas de perte ou de vol d'un équipement ou d'informations, informez votre organisme et demandez conseil au consulat avant toute démarche auprès des autorités locales.
● N'utilisez pas les équipements qui vous sont offerts avant de les avoir fait vérifier par votre service de sécurité. Ils peuvent contenir des logiciels malveillants.
● Evitez de connecter vos équipements à des postes ou des périphériques informatiques qui ne sont pas reconnus de confiance.
● Attention aux échanges de documents (par exemple : par clé USB lors de présentations commerciales ou lors de colloques). Emportez une clé destinée à ces échanges et effacez les fichiers dès lors qu'ils ne vous sont plus utiles.

Avant votre retour de mission

● Transférez vos données sur le réseau de votre organisme avec une connexion sécurisée. Puis effacez-les ensuite de votre machine.
● Effacez l'historique de vos appels et de vos navigations.

Après la mission

● Changez les mots de passe que vous avez utilisés pendant votre voyage.
● Analysez ou faites analyser vos équipements.
● Ne connectez pas les appareils à votre réseau avant d'avoir fait au minimum un test anti-virus et anti-espiogiciels.

Pour en savoir plus

Liens utiles

● ANSSI (Agence Nationale de la Sécurité des Systèmes d'informations)
http://www.ssi.gouv.fr/
● Portail de la Sécurité Informatique http://www.securite-informatique.gouv.fr/
● CERTA, Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques, http://www.certa.ssi.gouv.fr/

Exemples de logiciels utiles et gratuits :

- TrueCrypt (version 7.1a) : logiciel de chiffrage pour Windows et Linux.
- FileZilla : logiciel de transfert de fichier (FTP, SFTP, SSH, etc...).
- OpenVPN : client VPN pour Windows et Linux.
- Putty : pour accéder à des serveurs Linux de façon sécurisée.
- Thunderbird : client de messagerie.
- Firefox : navigateur web.
- OpenOffice : suite bureautique compatible avec tous les systèmes.
- Ccleaner : nettoyeur de fichiers temporaires, notamment.