Les dix commandements de l'administrateur

I- Étant utilisateur avant d'être administrateur, ses commandements, tu suis.

II- Avec précaution, la première fois dans l'établissement, ta machine, tu connectes.

III- Les sauvegardes de tes données personnelles, fréquemment, tu fais.

IV- Avec retenue, les droits d'administrateur, tu utilises.

V- Sans discernement, le prêt de ta machine à un tiers, tu évites.

VI- Avec assiduité, des avis de sécurité, connaissance, tu prends.

VII- Les mises à jour de sécurité, régulièrement, tu appliques.

VIII- La lutte contre les virus et autres troyens, sans relâche, tu mènes.

IX- Des logiciels de contournement de politique de sécurité, jamais, tu ne te sers.

X- Les services ouverts sur ta machine, drastiquement, tu limites.

Administrateur de Ressources Informatiques

Tes Dix Commandements

ENS DE LYON

ENS DE LYON

Utilisateur de Ressources Informatiques

Tes Dix Commandements

Les dix commandements de l'utilisateur

I- En informatique comme ailleurs, la réglementation légale, tu suis.

II- Des ressources numériques de l'établissement, un usage mesuré, tu fais.

III- Ton sésame (identifiant/mot de passe), toujours, tu préserves.

IV- A un tiers, une application en ton nom, jamais, tu ne remets.

V- A un usage personnel, les ressources mises à disposition, tu limites.

VI- Les mesures de sécurité informatique du site, jamais, tu ne contournes.

VII- Les services informatiques, des anomalies de fonctionnement, tu avertis.

VIII- La traçabilité de ton activité électronique, dans le cadre légal, tu acceptes.

IX- Les comportements à risques, toujours, tu évites.

X- L'identité d'une autre personne, en aucun cas, tu n'usurpes.

"Utiliser ou tout l'art d'user sans abuser !"

I- L'informatique est l'univers de l'immatériel, mais les règles qui gouvernent son usage sont bien réelles. Certaines de ces règles sont de simples recommandations, comme la Nétiquette ou RFC 1855 : elles forment un "savoir-vivre ensemble" dans ces usages. D'autres règles sont des lois, que nul n'est censé ignorer : un simple manquement à la réglementation se traduit par des peines, elles aussi, bien réelles (par exemple, 15k€ d'amende et 1 an d'emprisonnement pour une usurpation d'identité). A ces lois spécifiques s'ajoutent toutes les autres lois sur l'atteinte à la vie privée, la diffamation, l'injure, la provocation de mineurs, l'apologie de crimes, l'incitation à la consommation de substances illicites, la contrefaçon, etc... Si utiliser des ressources numériques ou en mettre à disposition est un droit, il reste cependant encadré de devoirs à respecter.

II- Comme toutes les ressources, les ressources numériques mises à la disposition sont limitées. Si elles ne le semblent pas, c'est parce que des ressources matérielles et logicielles sont correctement proportionnées pour un usage courant et administrées par des personnels dévoués. L'exploitation abusive par quelques individus de ces ressources peut mettre en péril son usage pour tous ses autres usagers légitimes.

III- Le couple identifiant et mot de passe permet à l'utilisateur de s'identifier (pour accéder à des ressources) et s'authentifier (pour s'assurer qu'il est bien celui qu'il prétend être). Ce sésame est donc comparable à une carte de paiement avec son numéro et son code secret ou un véhicule et sa clé de contact. De la même manière que vous êtes responsable de ce qu'une personne accomplit avec votre véhicule ou avec votre carte de paiement, vous êtes responsable de l'usage de votre identifiant et mot de passe.

IV- Les applications informatiques sont mises à disposition dans le cadre de fonctions particulières : leur usage doit se limiter de la même manière que pour un véhicule, un logement ou un équipement de fonction.

V- La règlementation autorise l'usage de ressources professionnelles à des fins personnelles. Cependant, cet usage doit être mesuré : l'activité professionnelle ne doit pas en être dégradée.

VI- Une infrastructure informatique est un savant équilibre, aussi complexe à obtenir qu'une bonne santé chez un être vivant. De la même manière que nous sommes attentifs à notre santé (en veillant à notre alimentation, à notre activité physique), nous limitons nos contaminations en évitant les comportements "à risques". Il en va de même pour l'édifice informatique : l'usage de certains outils doit se limiter au "praticien" informatique ; de même, limiter son exposition à la contagion virale informatique passe par un comportement de bon sens.

VII- Un incident informatique est comme un incendie de forêt : plus tôt il est pris en charge, meilleure sera sa résolution. En effet, des pannes peuvent être précédées de signes avant-coureurs qu'un utilisateur pourra rencontrer mais qu'un administrateur ne constatera pas dans sa supervision des systèmes. Avertir les informaticiens des anomalies est souvent salutaire.

VIII- La traçabilité est une obligation légale. La qualité des informations à conserver s'est étendue avec la nouvelle loi Loppsi 2. Tout comme dans la production alimentaire, la traçabilité informatique permet de conserver des traces des actions sur les systèmes. Elles permettent, en cas de problème, de remonter plus facilement à la source et mieux cibler les responsabilités des uns ou des autres.

IX- Les campagnes de santé nous invitent à des comportements "sains" en matière d'alimentation, de dépense physique ou autre. Il en va de même en informatique : laisser sa session ouverte, partir en laissant son portable sans cadenas, installer n'importe quel logiciel, répondre aux requêtes de hameçonnage sont des comportements à risques, donc à proscrire.

X- L'usurpation d'identité est un délit, désormais puni, même sans préjudice financier.

"A grand pouvoir, grande responsabilité !"

Question : suis-je un administrateur ?

- je connecte mon smartphone ou mon propre ordinateur sur le WiFi de l'établissement ;
- j'utilise mon propre ordinateur dans mon unité d'accueil (laboratoire, département, plate-forme) ;
- je connecte mon propre ordinateur dans la résidence ;
- je peux installer des logiciels sur un poste mis à ma disposition et connecté au réseau ;
- j'administre une machine connectée au réseau.

En cas de réponse affirmative à l'une de ces propositions, alors oui, sans conteste, je suis un administrateur.

I- Les commandements de l'administrateur sous-tendent l'application tacite de tous les commandements de l'utilisateur. Les administrateurs disposant de droits étendus, leurs devoirs le sont aussi.

II- Connecter sa machine personnelle au réseau du site n'est pas un acte anodin. Toutes les actions de votre machine seront détectées comme provenant du site. Il est donc préférable, avant de connecter son équipement sur une prise avec fil, d'en informer le personnel informatique, de proximité ou des services centraux. Ces derniers doivent pouvoir vérifier rapidement que votre machine ne risque pas de mettre en péril la sécurité informatique du site.

III- La charge de l'administration d'une machine commence par la conservation des données qui y sont stockées. Il convient de s'assurer que des sauvegardes ont lieu, que ces dernières sont également réalisées ailleurs. Il est également préférable qu'un archivage (permettant de retrouver l'état des données à un instant précis) soit également réalisé.

Charte Informatique
http://intranet.ens-lyon.fr/adminsite/objetspartages/liste_fichiergw.jsp?OBJET=DOCUMENT&CODE=1283870185487&LANGUE=0

IV- Le compte administrateur est semblable au capot d'un véhicule : le conducteur peut l'ouvrir pour des opérations de maintenance, mais il le referme après. Il évite ainsi, en son absence, que les organes vitaux de son véhicule ne soient endommagés par les intempéries ou par des mains aux intentions contestables. Limiter donc l'usage du compte de l'administrateur est mère de sûreté.

V- Le prêt de sa machine équivaut au prêt de son véhicule personnel : il engage sa responsabilité pleine et entière. Justifier a posteriori qu'un tiers a utilisé sa machine pour commettre des actes illicites est difficile. La prudence s'impose donc.

VI- Régulièrement, des avis de sécurité sont diffusés par le RSSI de l'établissement ou des listes associées aux logiciels dont vous administrez les services. Il convient d'y prêter une attention particulière et de tenir compte de leur caractère critique.

VII- Les systèmes d'exploitation et certains logiciels proposent des mises à jour, souvent là pour combler des trous de sécurité. Il convient de les appliquer (sauf contre-ordre) rapidement.

VIII- Les virus et les chevaux de Troie sont les principaux artisans des problèmes informatiques. L'usage d'outils antivirus reste une des meilleures protections mais son efficacité dépend de son actualité : mettre à jour son antivirus est aussi important que l'installer.

IX- Des outils servent à tester ou contourner les règles de sécurité d'un site. Leur utilisation équivaut à une agression. Un tel comportement ne correspond pas à un usage "loyal" des ressources mises à disposition.

X- Par défaut, les machines offrent des services aux autres machines. Offrir un service, c'est risquer la possibilité d'une compromission si une faille affecte le service mis à disposition. Il est donc raisonnable, principe de précaution oblige, de les limiter au strict nécessaire.

<emmanuel.quemener@ens-lyon.fr>