

Sensibilisation aux menaces Internet
&
Formation aux bonnes pratiques pour les
utilisateurs (BPU) de systèmes informatiques

Module 1
Panorama des menaces SSI



Module 2
Les règles élémentaires de
protection

LES 10 REGLES pour protéger son poste informatique

P. 2



Obligations légales

 Règle 1 – Respect des chartes informatiques

La protection technique du poste de travail



  Règle 2 - Sauvegarde systématique et quotidienne des données

  Règle 3 - Utilisation d'un pare-feu et d'un antivirus, mises à jour régulières des systèmes et logiciels

  Règle 4 - Limitation des droits « administrateurs », utilisation d'un compte « standard » au quotidien

Un comportement avisé de l'utilisateur

 Règle 5 - Protection des ordinateurs portables contre les accès illégitimes et le vol

  Règle 6 – Utilisation de mots de passe robustes, personnels et différents en fonction des usages

  Règle 7 – Se méfier des clés USB et autres matériels amovibles

  Règle 8 - Utilisation prudente d'Internet (navigation, téléchargement, services en ligne, vie privée)

  Règle 9 - Attitude prudente vis à vis des messages reçus

 Règle 10 – Ordinateur infecté : ça arrive(ra) à tout le monde, pas de panique



Obligations légales

Règle 1 – Respect des chartes informatiques

La protection technique du poste de travail



Règle 2 - Sauvegarde systématique et quotidienne des données

Règle 3 - Utilisation d'un pare-feu et d'un antivirus, mises à jour régulières des systèmes et logiciels

Règle 4 - Limitation des droits « administrateurs », utilisation d'un compte « standard » au quotidien

Un comportement avisé de l'utilisateur



Règle 5 - Protection des ordinateurs portables contre les accès illégitimes et le vol

Règle 6 – Utilisation de mots de passe robustes, personnels et différents en fonction des usages

Règle 7 – Se méfier des clés USB et autres matériels amovibles

Règle 8 - Utilisation prudente d'Internet (navigation, téléchargement, services en ligne, vie privée)

Règle 9 - Attitude prudente vis à vis des messages reçus

Règle 10 – Ordinateur infecté : ça arrive(ra) à tout le monde, pas de panique



Université de Strasbourg Chartre des bons usages des moyens numériques

<http://services-numeriques.unistra.fr/services-osiris/cert-osiris/charte-des-bons-usages-des-moyens-numeriques-de-luniversite-de-strasbourg.html>

- ▶ **Un document principal** 🧑🧑
→ fournissant un cadre de référence général.
- ▶ **Un guide pratique de l'utilisateur** 🧑🧑
→ précisant les modalités d'application des règles énoncées dans la charte.
- ▶ **Une annexe juridique** 🧑🧑
→ présentant les références juridiques sur lesquelles s'appuie la charte.



CNRS Chartre pour l'usage de ressources informatiques et de services Internet

<http://www.dgdr.cnrs.fr/BO/2007/03-07/415-bo0307-dec070007dAj.htm>





Circulaire Rocard du 17 juillet 1990 :

« Un fonctionnaire auteur ou responsable de reproduction illicite devra seul supporter les condamnations pénales encourues même s'il n'a pas agi dans son intérêt personnel »





« Vie privée résiduelle »

- L'adresse mèl est présumée « professionnelle »
- La vie privée ne peut nuire à la continuité du service (code d'accès)
- Risque ou évènement particulier :

– Arrêt du 17 mai 2005

Sauf risque ou évènement particulier, l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels qu'en présence de ce dernier ou celui-ci dûment appelé

CNIL  Article CNIL L'accès à la messagerie d'un salarié en son absence 26 mars 2012
<http://www.cnil.fr/linstitution/actualite/article/article/lacces-a-la-messagerie-dun-salarie-en-son-absence/>

Correspondant informatique et liberté (CIL) de l'Université : cil@unistra.fr

CIL CNRS : www.cil.cnrs.fr info.contact@cil.cnrs.fr





Quelques textes importants

- Code de la propriété intellectuelle
<http://www.legifrance.gouv.fr/affichCode.do?idSectionTA=LEGISCTA000006161658&cidTexte=LEGITEXT000006069414&dateTexte=20111102>
- Loi informatique et libertés, droits du citoyen
<http://www.cnil.fr/vos-droits/vos-droits/>
- Guide "Informatique et Libertés" pour l'enseignement supérieur et la recherche *Édition 2011*
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_AMUE_2011.pdf

Mise en place d'un annuaire des diplômés

Diffusion des résultats d'examen et des notes sur internet

Utilisation de la photographie d'une personne

Enquêtes statistiques portant sur le devenir professionnel et le suivi de cohortes d'étudiants

Mise à disposition ou accès à des ressources numériques via des dispositifs de « fédération d'identités »

Utilisation du téléphone sur le lieu de travail

Mise en place des espaces numériques de travail (ENT)

Dura lex, sed lex



LES 10 REGLES pour protéger son poste informatique

P. 8



Obligations légales

Règle 1 – Respect des chartes informatiques

La protection technique du poste de travail

Règle 2 - Sauvegarde systématique et quotidienne des données

Règle 3 - Utilisation d'un pare-feu et d'un antivirus, mises à jour régulières des systèmes et logiciels

Règle 4 - Limitation des droits « administrateurs », utilisation d'un compte « standard » au quotidien

Un comportement avisé de l'utilisateur

Règle 5 - Protection des ordinateurs portables contre les accès illégitimes et le vol

Règle 6 – Utilisation de mots de passe robustes, personnels et différents en fonction des usages

Règle 7 – Se méfier des clés USB et autres matériels amovibles

Règle 8 - Utilisation prudente d'Internet (navigation, téléchargement, services en ligne, vie privée)

Règle 9 - Attitude prudente vis à vis des messages reçus

Règle 10 – Ordinateur infecté : ça arrive(ra) à tout le monde, pas de panique



LES 10 REGLES pour protéger son poste informatique

P. 9



Obligations légales

Règle 1 – Respect des chartes informatiques

La protection technique du poste de travail

Règle 2 - Sauvegarde systématique et quotidienne des données

Règle 3 - Utilisation d'un pare-feu et d'un antivirus, mises à jour régulières des systèmes et logiciels

Règle 4 - Limitation des droits « administrateurs », utilisation d'un compte « standard » au quotidien

Un comportement avisé de l'utilisateur

Règle 5 - Protection des ordinateurs portables contre les accès illégitimes et le vol

Règle 6 – Utilisation de mots de passe robustes, personnels et différents en fonction des usages

Règle 7 – Se méfier des clés USB et autres matériels amovibles

Règle 8 - Utilisation prudente d'Internet (navigation, téléchargement, services en ligne, vie privée)

Règle 9 - Attitude prudente vis à vis des messages reçus

Règle 10 – Ordinateur infecté : ça arrive(ra) à tout le monde, pas de panique



Sauvegarder, c'est mettre en lieu sûr des informations pour les récupérer en cas de nécessité (vol, défaillance matérielle, effacement par virus ou par erreur).

En cas de vol ou de défaillance technique, la sauvegarde est **le seul moyen de recouvrer ses données**.

- Utiliser un logiciel de sauvegarde
 - Suivre les préconisations des CSSI et ASR de votre unité.
 - Préférer une solution globale à une solution individuelle (... ou les deux)
- Choisir un support adéquat
 - Espace de sauvegarde centralisé : NAS, serveur, ...etc.
 - Stockage individuel : disque externe, DVD, ...etc.
- Sélectionner les données à sauvegarder
 - Réfléchir aux données essentielles et critiques.
- Programmer une sauvegarde quotidienne

- *Vérifier la bonne exécution de la sauvegarde*
- *Vérifier la lisibilité des supports de sauvegarde*



Règle 2 - Sauvegarde systématique et quotidienne des données

- La règle
- Les bonnes pratiques
- Les outils

P. 12



Plan de sauvegarde interne

Quels supports, quels outils, automatisation ?
Restauration ?

< à compléter par l'entité en charge des sauvegardes >



- La règle
- Les bonnes pratiques
- Les outils

P. 13



Utilisez les espaces de stockages
partagés internes **ET**
les outils de sauvegarde préconisés
localement



Évitez les outils de « cloud public » :

Dropbox, Gdrive, iCloud ...

*Préférez le dépôt de vos données sur un
espace de stockage **privé et maîtrisé***



Time Machine

<http://www.apple.com/fr/findouthow/mac/#backup>



Sbackup

<http://doc.ubuntu-fr.org/sbackup>



SyncBackSE

<http://www.01net.com/telecharger/windows/Utilitaire/sauvegarde/fiches/31511.html>



Sauvegarde Windows intégrée (w7)

<http://windows.microsoft.com/fr-FR/windows7/Back-up-your-files>



LES 10 REGLES pour protéger son poste informatique

P. 14



Obligations légales

Règle 1 – Respect des chartes informatiques

La protection technique du poste de travail

Règle 2 - Sauvegarde systématique et quotidienne des données

Règle 3 - Utilisation d'un pare-feu et d'un antivirus, mises à jour systèmes et logiciels

Règle 4 - Limitation des droits « administrateurs », utilisation d'un compte « standard » au quotidien

Un comportement avisé de l'utilisateur

Règle 5 - Protection des ordinateurs portables contre les accès illégitimes et le vol

Règle 6 – Utilisation de mots de passe robustes, personnels et différents en fonction des usages

Règle 7 – Se méfier des clés USB et autres matériels amovibles

Règle 8 - Utilisation prudente d'Internet (navigation, téléchargement, services en ligne, vie privée)

Règle 9 - Attitude prudente vis à vis des messages reçus

Règle 10 – Ordinateur infecté : ça arrive(ra) à tout le monde, pas de panique



Règle 3 - Pare-feu, antivirus, mises à jour régulières des systèmes et logiciels

- La règle
- Les bonnes pratiques
- Les outils

P. 15

①



PAREFEU

Mon poste est connecté à Internet
↔
Internet est connecté à mon poste

protège contre les connexions
NON SOLLICITÉES

ne protège pas contre les
connexions SOLLICITÉES



②



ANTIVIRUS

Des centaines de fichiers et de programmes pénètrent sur mon poste, via le navigateur Web, la messagerie, les chats

protège contre les
menaces CONNUES

ne protège pas contre les
menaces INCONNUES



③



MISES À JOUR

Les systèmes d'exploitation et les logiciels comportent des dizaines de failles de sécurité corrigées au fur et à mesure par les éditeurs

empêche l'exploitation par un
malware des failles CORRIGÉES

n'empêche pas l'exploitation des
failles nouvelles ni des failles
inconnues



①

PAREFEU

Distinguer le réseau domestique (local) et le réseau public (internet)

Ne pas répondre systématiquement **OUI** aux messages du pare-feu

②

ANTIVIRUS

Mises à jour quotidienne des bases de signature et du moteur de l'antivirus

Analyses régulières et complètes des disques

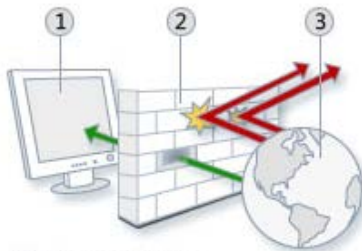
③

MISES À JOUR

Système :
Mises à jour automatiques

Logiciels :
Mises à jour automatiques

Désactiver les programmes qui ne sont pas indispensables au bon fonctionnement du poste de travail.



- ① Votre ordinateur
- ② Votre pare-feu
- ③ Internet



Règle 3 - Pare-feu, antivirus, mises à jour régulières des systèmes et logiciels

- La règle
- Les bonnes pratiques
- Les outils

P. 17



①

PAREFEU



< à remplir >



< à remplir >



< à remplir >

②

ANTIVIRUS

< à remplir >

③

MISES À JOUR

< à remplir >

< à remplir >

Si un équipement ne peut pas être mis à jour (OS obsolète, drivers introuvables...) :
Isoler l'équipement du réseau



- La règle
- Les bonnes pratiques
- Les outils



①

PAREFEU



Intégré
[Windows7](#) [Windows8](#)



[Coupe-feu applicatif](#)

②

ANTIVIRUS

Avast!
<http://www.avast.com/fr-fr/index>

③

MISES À JOUR

Windows Update (OS)
Paramétrage de chaque logiciel
(Java, Flashplayer, Acrobat...)



Règle 3 - Pare-feu, antivirus, mises à jour régulières des systèmes et logiciels

- La règle
- Les bonnes pratiques
- Les outils

P. 19

Outils de diagnostic



Tester la version des logiciels installés – *Secunia Personal Software Inspector*

<http://www.01net.com/telecharger/windows/Utilitaire/systeme/fiches/42855.html>

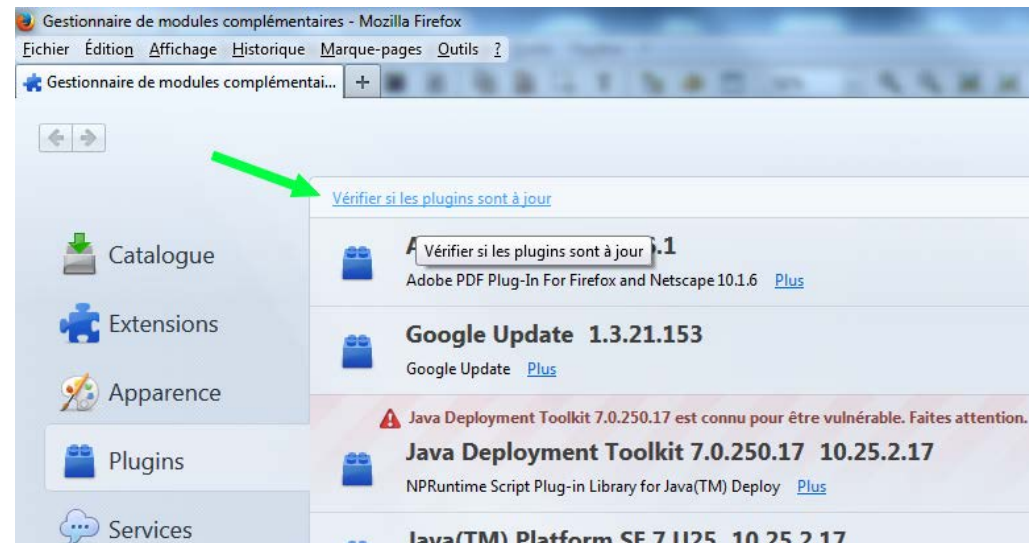


Navigateur : test des modules complémentaires

Intégré à FF

Tester les ports ouverts de sa machine

<http://nmap.online-domain-tools.com/>



- La règle
- Les bonnes pratiques
- Les outils

P. 20

Windows XP :

fin de vie **AVRIL 2014**

<http://windows.microsoft.com/fr-fr/windows/products/lifecycle>



« Patch Tuesday »

Le deuxième mardi de chaque mois, Microsoft met à disposition de ses clients les derniers patches de sécurité pour ses logiciels



LES 10 REGLES pour protéger son poste informatique

P. 21



Obligations légales

Règle 1 – Respect des chartes informatiques

La protection technique du poste de travail

Règle 2 - Sauvegarde systématique et quotidienne des données

Règle 3 - Utilisation d'un pare-feu et d'un antivirus, mises à jour systèmes et logiciels

Règle 4 - Limitation des droits « administrateurs »

Un comportement avisé de l'utilisateur

Règle 5 - Protection des ordinateurs portables contre les accès illégitimes et le vol

Règle 6 – Utilisation de mots de passe robustes, personnels et différents en fonction des usages

Règle 7 – Se méfier des clés USB et autres matériels amovibles

Règle 8 - Utilisation prudente d'Internet (navigation, téléchargement, services en ligne, vie privée)

Règle 9 - Attitude prudente vis à vis des messages reçus

Règle 10 – Ordinateur infecté : ça arrive(ra) à tout le monde, pas de panique



UTILISER DES DROITS MINIMUMS POUR LES ACTIVITÉS COURANTES

(navigation, messagerie, téléchargement, réseaux sociaux, etc.)

OBJECTIFS

- Cloisonner les utilisateurs, les applications et le système
- Limiter les risques de propagation
- Ne pas exposer les autres comptes présents sur le même ordinateur
- Protéger le système d'exploitation
- Eviter les erreurs de manipulation

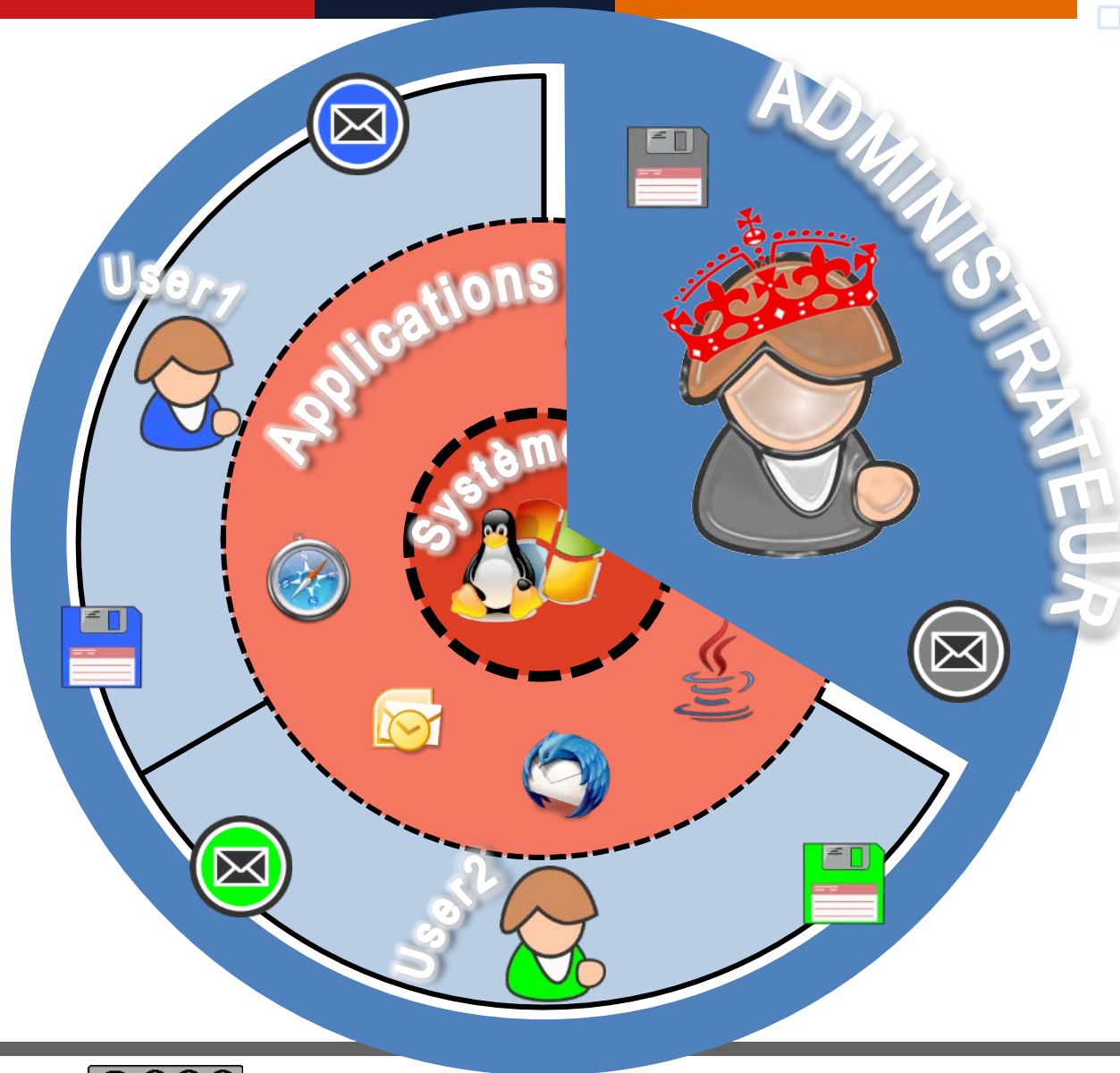
RISQUES

- Blocage complet de l'ordinateur
- Vol d'informations personnelles et/ou confidentielles
- Désactivation des mécanismes de protection (parefeu, antivirus, etc.)
- Utilisation de l'ordinateur pour commettre des méfaits (spam, warez, etc.)

Règle 4 - Limitation des droits « administrateurs »

- La règle
- Les bonnes pratiques
- Les outils

P. 23



- Création d'un **compte standard** pour chaque utilisateur
- Utilisation par défaut de ce compte standard **avec droits limités** au quotidien
- La plupart des systèmes d'exploitation (Windows, Linux, MacOS) permettent d'utiliser le mode *Administrateur* depuis une session *Utilisateur*.
- Le mot de passe du compte *Administrateur* doit être **ROBUSTE** (risque d'élévation de privilèges)

- La règle
- Les bonnes pratiques
- Les outils

Ne s'applique pas dans le cas d'un DOMAINE avec gestion centralisée des comptes



Sous Windows :

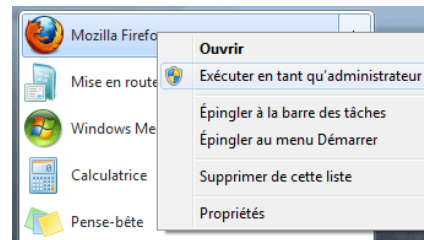
Pour gérer les comptes, créer des utilisateurs, vérifier des droits

- Panneau de configuration
- Ou exécuter : `mmc compmgmt.msc`



Comptes d'utilisateurs

Pour exécuter ponctuellement une opération avec les droits administrateur :



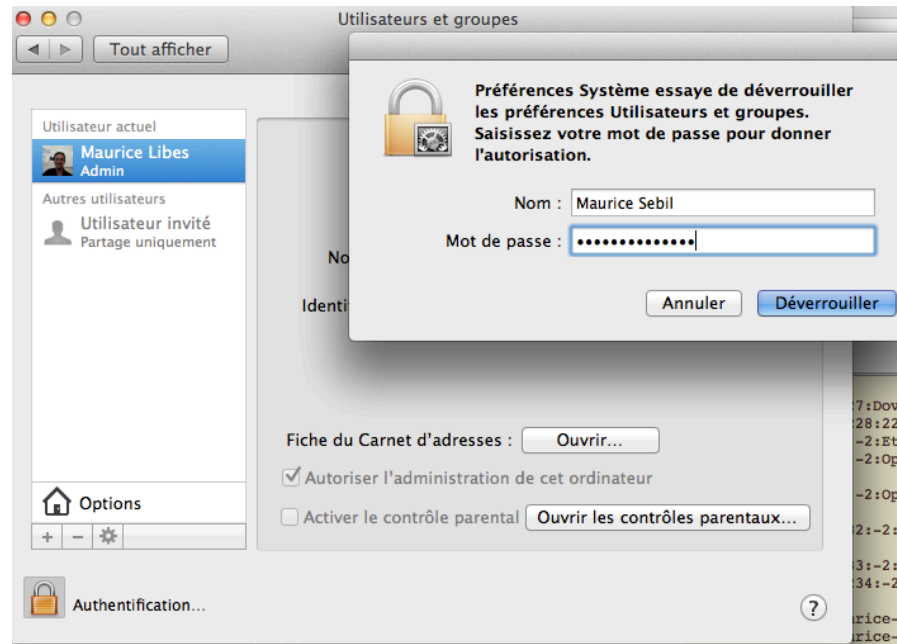
Sous Linux et MacOS X :

- Utiliser la commande « `sudo` » pour passer occasionnellement en mode administrateur.



- La règle
- Les bonnes pratiques
- Les outils

Sous Mac OS :



LES 10 REGLES pour protéger son poste informatique

P. 27



Obligations légales

Règle 1 – Respect des chartes informatiques

La protection technique du poste de travail



Règle 2 - Sauvegarde systématique et quotidienne des données

Règle 3 - Utilisation d'un pare-feu et d'un antivirus, mises à jour régulières des systèmes et logiciels

Règle 4 - Limitation des droits « administrateurs », utilisation d'un compte « standard » au quotidien

Un comportement avisé de l'utilisateur

Règle 5 - Protection des ordinateurs portables contre les accès illégitimes et le vol

Règle 6 - Utilisation de mots de passe robustes, personnels et différents en fonction des usages

Règle 7 - Se méfier des clés USB et autres matériels amovibles

Règle 8 - Utilisation prudente d'Internet (navigation, téléchargement, services en ligne, vie privée)

Règle 9 - Attitude prudente vis à vis des messages reçus

Règle 10 - Ordinateur infecté : ça arrive(ra) à tout le monde, pas de panique



Un comportement avisé de l'utilisateur

Kevin Mitnick :

« You could spend a fortune purchasing technology and services... and your network infrastructure could still remain vulnerable to old-fashioned manipulation ».

LES 10 REGLES pour protéger son poste informatique

P. 29



Obligations légales

Règle 1 – Respect des chartes informatiques

La protection technique du poste de travail



Règle 2 - Sauvegarde systématique et quotidienne des données

Règle 3 - Utilisation d'un pare-feu et d'un antivirus, mises à jour régulières des systèmes et logiciels

Règle 4 - Limitation des droits « administrateurs », utilisation d'un compte « standard » au quotidien

Un comportement avisé de l'utilisateur

Règle 5 - Protection des ordinateurs portables contre les accès illégitimes et le vol

Règle 6 - Utilisation de mots de passe robustes, personnels et différents en fonction des usages

Règle 7 - Se méfier des clés USB et autres matériels amovibles

Règle 8 - Utilisation prudente d'Internet (navigation, téléchargement, services en ligne, vie privée)

Règle 9 - Attitude prudente vis à vis des messages reçus

Règle 10 - Ordinateur infecté : ça arrive(ra) à tout le monde, pas de panique



Tous les ordinateurs portables doivent être chiffrés
+ les postes particulièrement sensibles



Les vols (ou pertes) se produisent souvent dans les transports en commun, lors des déplacements en France ou à l'étranger, mais également dans ses propres locaux.



Le chiffrement d'un ordinateur, d'une clé USB ou d'un disque externe rend les données illisibles et inexploitable en cas de vol du matériel.

L'accès aux données chiffrées se fait via un mot de passe. Il est indispensable de disposer d'un **mot de passe ROBUSTE** et d'une **procédure de recouvrement** en cas d'oubli de ce mot de passe.

La négligence est la principale cause du vol

Anticiper la perte

- 1- **chiffrement** des ordinateurs portables pour éviter la fuite d'informations
- 2- **sauvegarde régulière** pour restaurer les données perdues

Dans les transports

- *Ne pas oublier son matériel ... nombre de disparitions d'ordinateur résultent d'un simple oubli*
- *Garder ses matériels à portée de main*
- *Ne pas laisser son matériel sans surveillance (en particulier dans les trains)*
- *Mettre un signe distinctif sur l'appareil et sa housse pour le surveiller plus facilement et éviter les échanges volontaires ou involontaires (à l'aéroport par exemple)*

PASSEPORT DE CONSEILS AUX VOYAGEURS

http://www.securite-informatique.gouv.fr/IMG/pdf/Passeport-de-conseils-aux-voyageurs_janvier



Tous les ordinateurs portables doivent être chiffrés
+ les postes particulièrement sensibles

Le chiffrement d'un ordinateur, d'une clé USB ou d'un disque externe rend les données illisibles et inexploitable en cas de vol du matériel.

L'accès aux données chiffrées se fait via un mot de passe. Il est indispensable de disposer d'un **mot de passe ROBUSTE** et d'une **procédure de recouvrement** en cas d'oubli de ce mot de passe.

[CNRS/RSSI-FSD : Recommandations pour la protection des données et le chiffrement](#)



- La règle
- Les bonnes pratiques
- Les outils

Windows :

Chiffrement du disque entier ou d'un conteneur avec TrueCrypt.

MacOS X : FileVault (intégré à MacOSX).

Chiffrement d'un répertoire.

Chiffrement du disque entier à partir de Mac OS X Lion.

Linux : Dm-crypt (intégré au système de la plupart des distributions Linux Debian, Ubuntu, ...etc.).

Chiffrement du disque entier **dès l'installation du poste.**

Clé USB chiffrée : Par exemple Ironkey ou Datashur

CNRS/DSI/RSSI juin 2012 - François MORRIS

[Chiffrement des portables](#)

[Mise en oeuvre et utilisation](#)



Se rapprocher de votre ASR pour être formé sur l'utilisation de ces outils de chiffrement.



LES 10 REGLES pour protéger son poste informatique

P. 35



Obligations légales

Règle 1 – Respect des chartes informatiques

La protection technique du poste de travail



Règle 2 - Sauvegarde systématique et quotidienne des données

Règle 3 - Utilisation d'un pare-feu et d'un antivirus, mises à jour régulières des systèmes et logiciels

Règle 4 - Limitation des droits « administrateurs », utilisation d'un compte « standard » au quotidien

Un comportement avisé de l'utilisateur

Règle 5 - Protection des ordinateurs portables contre les accès illégitimes et le vol

Règle 6 - Utilisation de mots de passe robustes, personnels et différents

Règle 7 - Se méfier des clés USB et autres matériels amovibles

Règle 8 - Utilisation prudente d'Internet (navigation, téléchargement, services en ligne, vie privée)

Règle 9 - Attitude prudente vis à vis des messages reçus

Règle 10 - Ordinateur infecté : ça arrive(ra) à tout le monde, pas de panique



Tout système informatique doit être protégé.

Chaque utilisateur doit s'authentifier nominativement pour protéger ses données et permettre un contrôle des accès auprès de ce système informatique.

Authentification simple : elle ne repose que sur un seul élément, habituellement un mot de passe

Authentification forte : elle repose sur plusieurs facteurs

Exemple :

- Mot de passe + certificat personnel
- Mot de passe + code de confirmation reçu par SMS
- Banque (*grille de codes + mot de passe + confirmation mail*)
- Impôts (*n° fiscal + n° de télé-déclarant + revenu fiscal de référence*)




L'authentifiant est la clé d'accès à l'information, cette clé doit être **strictement personnelle** et suffisamment complexe pour ne pas pouvoir être trop facilement découverte.







La robustesse d'un mot de passe dépend :

1. De sa longueur.
2. De la capacité de le deviner facilement (présence dans un dictionnaire).
3. De la combinaison de différents types de caractères utilisés.
4. Du nombre de caractères utilisables.



Les attaques sur les mots de passe :



-  Force brute : toutes les combinaisons sont essayées (en direct ou sur l'empreinte).
-  Ingénierie sociale : obtention du mot de passe par ruse (phishing, usurpation d'identité).
-  Vol : 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.

-  *Un mot de passe correct doit comporter au **minimum 10 caractères**, préférez les « **pass-phrase** »*
-  *Il est recommandé d'**utiliser des mots de passe différents** suivant le contexte et la sensibilité : accès professionnels, accès privés, banques, etc.
Comme cela est humainement très difficile, il est conseillé d'utiliser un outil de gestion des mots de passe tel que [Keepass](#).*
-  ***Un mot de passe doit rester personnel** : pas de mot de passe partagé entre plusieurs utilisateurs.*
-  *Un mot de passe devrait être **changé périodiquement** tous les 6 mois à 1 an en fonction de la sensibilité du système ou des données à protéger.*
-  *Un mot de passe doit être changé dès que l'on soupçonne sa compromission (vol ou perte du PC, divulgation à un tiers, etc.)*
-  *Ne pas laisser les navigateurs ou autres logiciels mémoriser vos mots de passe, ils sont faillibles*

Règle 6 - Utilisation de mots de passe robustes, personnels et différents

- La règle
- Les bonnes pratiques
- Les outils

P. 39

- Une pass-phrase doit être suffisamment complexe :
 -  Longueur minimum 10 caractères
 -  Caractères spéciaux, majuscule et chiffres

Mot de passe	robustesse	Attaque brut force	commentaire
manganese	36 %	0 s	
25manganese	52 %	22 mn	Rajout de chiffres
25=manganese	70 %	3 ans	Rajout caractère spécial « = »
25 = manganese	84 %	174 000 ans	Rajout caractère spécial <espace>
25 = Manganese	91 %	16 millions ans	Rajout Majuscule
25 = Manganèse	100 %	3 milliards ans	Rajout caractère spécial « è »

Exemple 1 : Le sport, j'aime ça (robustesse = 100 %)
Exemple 2 : Le Racing en Ligue1 (robustesse = 100 %)
Exemple 3 : Le roi, c'est Gauss (robustesse = 100 %)



Règle 6 - Utilisation de mots de passe robustes, personnels et différents

- La règle
- Les bonnes pratiques
- Les outils

P. 40

Stockage des mots de passe

Windows, Linux et MacOS X:

<https://www.projet-plume.org/fr/fiche/keepass>



Title	User Name	Password
clé recouvrement SSI		*****
SSI Latitude E6500 SN:8F2104J		*****
SPS Latitude E6400 SN:J0XC04J	Permanence	*****
SL Latitude E6500 SN:3XHCQ4J	Claudine Castomi	*****
SPV Latitude D630 SN: DHWXR3J	Marie Weiss	*****
DIR Latitude E6220 SN:3XKWWP1	Gaëlle Bujan	*****
SPRH Latitude E6520 SN:88CAFS1	yves magassouba	*****
SPV Latitude E6520 SN:J9Z3FS1	Christine Brunel	*****
SFC Latitude E6520 SN:99Z3FS1	Jean-Marie Burgio	*****
SCOM Latitude E6320 SN:HDH9FS1	Michele Bauer	*****
SL Latitude E6320 SN:JFH9FS1	Hugues Schoenfeld	*****
SSI latitudeD420 CNRS_3G-2 SN : BSR2N2J	voyageur 3G	*****
SSI latitudeD630 CNRS_3G-1 SN : 294P43J	voyageur 3G	*****
DIR Latitude E4300 SN:536XH4J	ex Jean-Marie Burgio	*****
SMP Latitude E4300 SN:5XW1P4J	eric.simon	*****
SFC Latitude E4300 SN:J58DB4J	Jerome BERGER	*****
SPS Latitude E4300 SN:CFDZL4J	Kevin Geiger	*****
SPV Latitude E6400 SN:JT63F4J	Jean-Pierre Vraux	*****
SL Latitude E6500 SN:2XHCQ4	Frederic Schott	*****
SL Latitude E4300 SN:GK84P4J	futut Hugues Schoenfeld	*****
SPRH Latitude E6320 SN:65NFGV1	doris.pflumio	*****
SPV Latitude E6230 SN 8SRSGV1	Marie Weiss	*****
SSI Latitude E6520 SN 99Z3FS1	ex Yves Magassouba	*****



LES 10 REGLES pour protéger son poste informatique

P. 41



Obligations légales

Règle 1 – Respect des chartes informatiques

La protection technique du poste de travail



Règle 2 - Sauvegarde systématique et quotidienne des données

Règle 3 - Utilisation d'un pare-feu et d'un antivirus, mises à jour régulières des systèmes et logiciels

Règle 4 - Limitation des droits « administrateurs », utilisation d'un compte « standard » au quotidien

Un comportement avisé de l'utilisateur

Règle 5 - Protection des ordinateurs portables contre les accès illégitimes et le vol

Règle 6 - Utilisation de mots de passe robustes, personnels et différents en fonction des usages

Règle 7 - Se méfier des clés USB et autres matériels amovibles

Règle 8 - Utilisation prudente d'Internet (navigation, téléchargement, services en ligne, vie privée)

Règle 9 - Attitude prudente vis à vis des messages reçus

Règle 10 - Ordinateur infecté : ça arrive(ra) à tout le monde, pas de panique



Les supports amovibles (disques, clé USB, ...) sont des média à utiliser avec prudence.

Ils doivent **seulement** être utilisés que pour **transférer les données** et non pas comme un moyen de stockage permanent, car le **risque de perte de données est important**.

Ces média sont sujets plus que les autres à :

- des risques de perte, ...de vol...
- une détérioration plus rapide que des matériels professionnels.

Ils ne faut pas les utiliser pour stocker des informations sensibles :

- *sujets ou notes d'examens, données privées, dossiers de carrière,*
- *mots de passe, codes bancaires, ...*

Si la clé USB est utilisée pour transporter des données sensibles, il est indispensable de chiffrer son contenu.

Désactiver l'exécution automatique des clés USB sur les vieilles version de Windows :
<http://support.microsoft.com/kb/967715/fr>



1- Clés auto-chiffrantes

IronKey D80 Flash Drive 4 GB



Prix : 50 €

iStorage datAshur AES 256 bits 4 GB
(avec clavier intégré)



Prix : 60 €

2- utiliser des conteneurs chiffrés avec TrueCrypt



LES 10 REGLES pour protéger son poste informatique

P. 45



Obligations légales

Règle 1 – Respect des chartes informatiques

La protection technique du poste de travail



Règle 2 - Sauvegarde systématique et quotidienne des données

Règle 3 - Utilisation d'un pare-feu et d'un antivirus, mises à jour régulières des systèmes et logiciels

Règle 4 - Limitation des droits « administrateurs », utilisation d'un compte « standard » au quotidien

Un comportement avisé de l'utilisateur

Règle 5 - Protection des ordinateurs portables contre les accès illégitimes et le vol

Règle 6 - Utilisation de mots de passe robustes, personnels et différents en fonction des usages

Règle 7 - Se méfier des clés USB et autres matériels amovibles

Règle 8 - Utilisation prudente d'Internet (navigation, téléchargement, vie privée)

Règle 9 - Attitude prudente vis à vis des messages reçus

Règle 10 - Ordinateur infecté : ça arrive(ra) à tout le monde, pas de panique



Règle 8 - Utilisation prudente d'Internet (*navigation, téléchargement, services gratuits*)

- La règle
- Les bonnes pratiques
- Les outils

P. 46

Le navigateur est **LA plate-forme d'échange** entre Internet et l'ordinateur.







Chaque **CLIC** génère une ou plusieurs interactions internet ↔ ordinateur :
Exécution de code, chargement d'une page ou de fichiers, envoi d'information
... de manière légitime (**ou pas**) ... de manière visible (**ou pas**)



NAVIGATION 
TELECHARGEMENTS 
SERVICES GRATUITS 



Le navigateur conserve tout un tas d'informations lors de la visite de pages web et lors des téléchargements :

-  Pages visitées
-  Saisies dans les formulaires et la barre de recherche
-  Mots de passe (chiffrés)
-  Liste des téléchargements
-  Cookies
-  Fichiers temporaires ou tampons (*plusieurs centaines de Mo !*)

Ces informations sont potentiellement accessibles à tous les sites web visités, certains services gratuits s'en servent ouvertement.

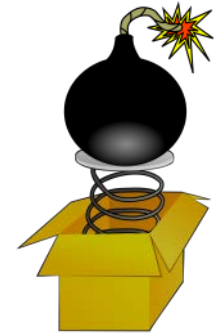
La « navigation privée » permet d'effacer systématiquement toutes ces informations.

NAVIGATION 
TELECHARGEMENTS 
SERVICES GRATUITS 





Télécharger un logiciel ou un fichier (*pdf, zip, mp3, avi, mov,...*),
c'est introduire un élément inconnu sur l'ordinateur.



Ouvrir un fichier (*ou installer un logiciel*), c'est faire confiance à son contenu.

Faire confiance au contenu, c'est faire confiance au fournisseur.

Faire confiance au fournisseur, c'est ... faire confiance au fournisseur.

L'utilisation à des fins professionnelles des services « gratuits » sur Internet (messagerie électronique, hébergement de sites web, stockage de données,...) suscite *de sérieuses réserves*

"La vie privée est devenue une sorte de monnaie d'échange. Elle nous sert à payer les services en ligne. Google ne fait rien payer pour Gmail. En lieu et place, il lit vos emails et vous envoie des publicités en fonction des mots-clés trouvés dans votre correspondance privée".

Dan Lyons, éditorialiste à Newsweek

SERVICES GRATUITS

« SI C'EST GRATUIT,
C'EST **TOI** LE PRODUIT »



NAVIGATION 

TELECHARGEMENTS 

SERVICES GRATUITS 

Règle 8 - Utilisation prudente d'Internet (*navigation, téléchargement, vie privée*)

P. 50

- La règle
- Les bonnes pratiques
- Les outils

- 📁 Maintenir à jour la version du navigateur
- 📁 Maintenir à jour les versions des extensions et des plugins
- 📁 Utiliser la fonction « Navigation privée »
- 📁 Installer les modules complémentaires WOT, NoScript
- 📁 Désactiver le module « Java Deployment Toolkit »
- 📁 Eviter les pratiques à risque : téléchargements illicites, « frénésie du clic », darkweb...
- 📁 RAPPEL : pas de session *ADMINISTRATEUR*















NAVIGATION 
TELECHARGEMENTS 
SERVICES GRATUITS 

CERT-OSIRIS



[Vérifier si les plugins sont à jour](#)

 Catalogue	 Adobe Acrobat 10.1.6.1 Adobe PDF Plug-In For Firefox and Netscape 10.1.6 Plus
 Extensions	 Google Update 1.3.21.153 Google Update Plus
 Apparence	 Java Deployment Toolkit 7.0.250.17 est connu pour être vulnérable. Faites attention. Plus d'informations
 Plugins	 Java Deployment Toolkit 7.0.250.17 10.25.2.17 NPRuntime Script Plug-in Library for Java(TM) Deploy Plus
 Services	 Java(TM) Platform SE 7 U25 10.25.2.17 Next Generation Java Plug-in 10.25.2 for Mozilla browsers Plus



- La règle
- Les bonnes pratiques
- Les outils



Mikko Hypponen

@mikko

Suivre





Do you have Java plugin in your browser?
You're vulnerable. Unless you run J2SE 1.x
from the 1990s. And you shouldn't.
seclists.org/fulldisclosure...

Répondre Retweeter Favori

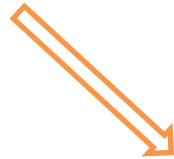
NAVIGATION

TELECHARGEMENTS
SERVICES GRATUITS



-  Sélectionner des sites de confiance pour vos téléchargements
-  Eviter les téléchargements illicites (logiciels craqués, œuvres protégées...)
-  Analyse antivirus en « temps réel » de tous les fichiers téléchargés
-  **RAPPELS** : pas de session *ADMINISTRATEUR*, antivirus à jour

- Utiliser la messagerie professionnelle pour la réception de vos mails professionnels
- Envoyer vos messages professionnels vers des adresses professionnelles
- Utiliser les services de stockage, d'échange, d'hébergement web, etc. de votre établissement, de vos tutelles ou d'un partenaire de confiance
- Pas de données « **sensibles** » dans le cloud public (google, yahoo, microsoft, apple, free...)



Données stratégiques (recherche, finance, RH...)
Données de valorisation
Données scientifiques
Données d'enseignement (sujets, relevés de note...)
Données à caractère personnel (CNIL)





Les conseils du Professeur GORIFA pour se protéger des logiciels de surveillance



- N'échangez aucune information sur aucun réseau social
- Ne parlez à aucun tiers ni sur Facebook, ni sur Twitter, ni même GooglePlus, si d'aventure vous vous y risquez
- Résilier vos abonnements internet et téléphone dans les plus brefs délais
- Vendez votre téléphone et votre ordinateur sur Ebay
- Éloignez vous de toutes possessions matérielles
- Fuyez vos amis** qui pourraient rapporter tous vos faits et gestes sur d'autres réseaux sociaux.
- Achetez un chien, désactivez l'option 4G
- Louez une grotte

NAVIGATION

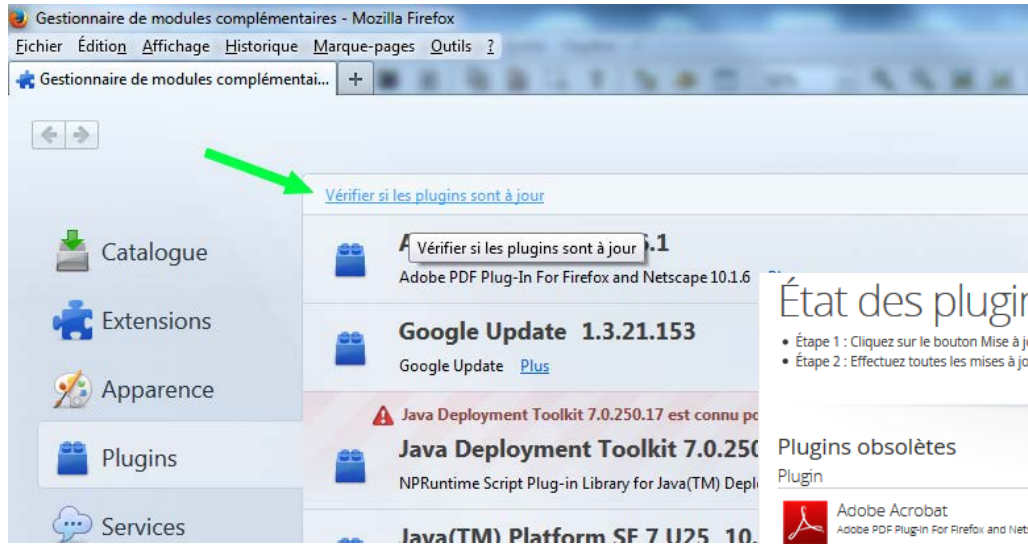
TELECHARGEMENTS

SERVICES GRATUITS

Règle 8 - Utilisation prudente d'Internet (*navigation, téléchargement, vie privée*)

- La règle
- Les bonnes pratiques
- Les outils

P. 55



Vérification des mises à jour des plugins

État des plugins

- Étape 1 : Cliquez sur le bouton Mise à jour pour mettre le plugin à jour.
- Étape 2 : Effectuez toutes les mises à jour recommandées avant de redémarrer votre navigateur.

Plugins obsolètes

Plugin	État	Action
Adobe Acrobat Adobe PDF Plug-In For Firefox and Netscape 10.1.6	vulnérable	Mettre à jour maintenant
VLC Web Plugin VLC media player Web Plugin 2.0.6	vulnérable	Mettre à jour maintenant

Plugins inconnus

Plugin	État	Action
Microsoft Office 2010 The plugin allows you to open and edit files using Microsoft Office applications	inconnu	Rechercher
Google Update Google Update	inconnu	Rechercher

Ces plugins sont à jour

Plugin	État	Action
Java Deployment Toolkit 7.0.250.17 NPRuntime Script Plug-in Library for Java(TM) Deploy	10.25.2.17	Plugin à jour
Java(TM) Platform SE 7 U25 Next Generation Java Plugin 10.25.2 for Mozilla browsers	10.25.2.17	Plugin à jour
Shockwave Flash Shockwave Flash 11.0 r800	11.8.800.94	Plugin à jour



NAVIGATION 
TELECHARGEMENTS 
SERVICES GRATUITS 



- La règle
- Les bonnes pratiques
- Les outils

Modules complémentaires



WOT – évalue la fiabilité des sites web

<https://addons.mozilla.org/fr/firefox/addon/wot-safe-browsing-tool/?src=hp-dl-featured>



NoScript – blocage préventif de scripts java basé sur une liste blanche

<https://addons.mozilla.org/fr/firefox/addon/noscript/>



Adblock Plus – blocage des bandeaux publicitaires

<https://addons.mozilla.org/fr/firefox/addon/adblock-plus/?src=search>



Ghostery – blocage des mouchards, des systèmes de mesure d'audience, des widgets

<https://addons.mozilla.org/fr/firefox/addon/ghostery/>

Web of trust : fonctionne sur le modèle du crowdsourcing (info donnée par la foule) et vous indique si un site est sûr en fonction de l'avis d'autres internautes. Si vous débarquez sur un site réputé être un nid de scripts malveillants, WOT vous affichera une alerte avant que la page ne se charge.



NAVIGATION 

TELECHARGEMENTS 
SERVICES GRATUITS 



- La règle
- Les bonnes pratiques
- Les outils

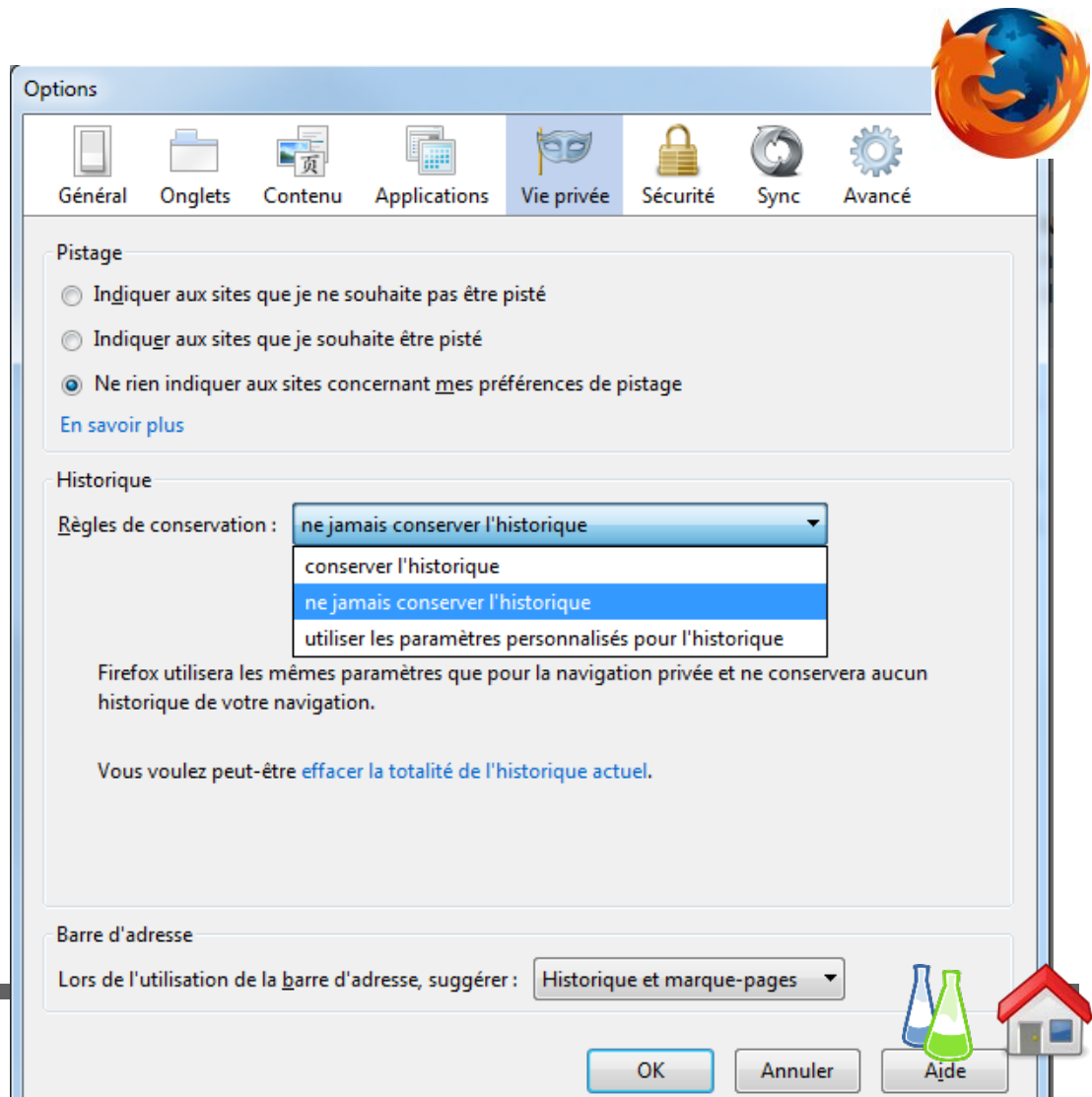
Navigation privée

En savoir plus... [la navigation privée](#)

[Navigation privée Firefox](#)

[Navigation privée Chrome](#)

[InPrivate : navigation privée Internet Explorer](#)



NAVIGATION 
TELECHARGEMENTS 
SERVICES GRATUITS 

Le module complémentaire WOT indique un niveau de crédibilité et de réputation des sites web

TÉLÉCHARGEMENT DE LOGICIELS

PLUME : 400 logiciels libres, classement thématique, avec fiche pédagogique

<https://www.projet-plume.org>



ACHATS

Le site web utilise-t-il le protocole sécurisé *https* ?

Le site web appartient-il à une entreprise connue ?

L'entreprise est-elle clairement identifiée et localisée (voir mentions légales) ?

Est-il possible de contacter quelqu'un par téléphone ou par courrier ?



NAVIGATION 

TELECHARGEMENTS 

SERVICES GRATUITS 

Utiliser les services recommandés par votre structure, par l'université, le CNRS ou tout autre partenaire de confiance (Renater...) :

- Stockage interne
- Service de messagerie de votre tutelle
- Hébergement de sites web
- Agenda de votre tutelle
- CNRS : messagerie, espaces collaboratifs, machines virtuelles
- Planification de rendez-vous [Studs](#)

En cas d'utilisation « ça va pas autrement, je n'ai aucune autre solution », chiffrer obligatoirement les échanges et les données stockées dans le Cloud (*voir règle 5 concernant le chiffrement*)

NAVIGATION 

TELECHARGEMENTS 

SERVICES GRATUITS 

LES 10 REGLES pour protéger son poste informatique

P. 60



Obligations légales

Règle 1 – Respect des chartes informatiques

La protection technique du poste de travail



Règle 2 - Sauvegarde systématique et quotidienne des données

Règle 3 - Utilisation d'un pare-feu et d'un antivirus, mises à jour régulières des systèmes et logiciels

Règle 4 - Limitation des droits « administrateurs », utilisation d'un compte « standard » au quotidien

Un comportement avisé de l'utilisateur

Règle 5 - Protection des ordinateurs portables contre les accès illégitimes et le vol

Règle 6 - Utilisation de mots de passe robustes, personnels et différents en fonction des usages

Règle 7 - Se méfier des clés USB et autres matériels amovibles

Règle 8 - Utilisation prudente d'Internet (navigation, téléchargement, services en ligne, vie privée)

Règle 9 - Attitude prudente vis à vis des messages reçus

Règle 10 - Ordinateur infecté : ça arrive(ra) à tout le monde, pas de panique



N'importe qui peut envoyer un mail dans votre boîte aux lettres et tenter d'abuser votre curiosité, votre gentillesse, votre crédulité, votre naïveté ou encore votre ignorance.

Modes opératoires et fraudes les plus courants :

1. Message contenant un lien frauduleux pour aboutir à une infection de type *drive-by-download* :
pages Web qui tentent d'exploiter les failles des sécurité des navigateurs en installant et en exécutant automatiquement des programmes malveillants sur le poste de l'internaute.
2. Demandes d'informations confidentielles, soit en réponse au mail soit via un lien sur un formulaire (*ex : banques, EDF, CAF, service informatique*).
3. Exécution d'une pièce jointe malveillante (*fichiers PDF, PowerPoint, images jpg, ...etc.*).
4. Canulars ou chaînes de diffusion d'informations non vérifiées (*catastrophes naturelles, disparition de personnes et autres*).

- Avant de cliquer, passez la souris sur le lien pour vérifier l'adresse URL.
- Ne répondez jamais à une demande d'informations confidentielles (*phishing*).
- Ne cliquez JAMAIS sur les liens contenus dans des messages d'origine douteuse.
- N'ayez jamais une confiance aveugle dans le nom de l'expéditeur.
- N'ouvrez pas de pièces jointes d'expéditeurs non reconnus.
- Soyez vigilant lors de la transmission d'une adresse courriel sur Internet : créez une « *adresse poubelle* » pour vos activités sur Internet.

- **Utiliser son esprit critique et son discernement** : analyser la vraisemblance du contenu du message.
- **Ne communiquer aucune information sensible par messagerie ou par téléphone** (mot de passe, code bancaire, date et lieu de naissance).
- **Vérifier l'adresse du lien (URL) avant de cliquer.**

- Disposer d'un anti-virus à jour.
- **Rappel** : ne pas être connecté avec des droits Administrateur peut limiter les effets d'une possible infection.
- **Rappel** : utiliser les boîtes professionnelles pour l'envoi et la réception de mails

- Consulter les sites recensant les canulars (ex : hoaxbuster.com) avant de relayer une fausse information.

LES 10 REGLES pour protéger son poste informatique

P. 64



Obligations légales

Règle 1 – Respect des chartes informatiques

La protection technique du poste de travail



Règle 2 - Sauvegarde systématique et quotidienne des données

Règle 3 - Utilisation d'un pare-feu et d'un antivirus, mises à jour régulières des systèmes et logiciels

Règle 4 - Limitation des droits « administrateurs », utilisation d'un compte « standard » au quotidien

Un comportement avisé de l'utilisateur

Règle 5 - Protection des ordinateurs portables contre les accès illégitimes et le vol

Règle 6 - Utilisation de mots de passe robustes, personnels et différents en fonction des usages

Règle 7 - Se méfier des clés USB et autres matériels amovibles


Règle 8 - Utilisation prudente d'Internet (navigation, téléchargement, services en ligne, vie privée)

Règle 9 - Attitude prudente vis à vis des messages reçus

Règle 10 - Ordinateur infecté : ça arrive(ra) à tout le monde, pas de panique






« La **gravité** d'un événement de sécurité mesure l'**impact** réel de l'événement en fonction de la **criticité** du bien touché »



Types d'incident

- 1- Vol / perte / diffusion d'informations sensibles
- 2- Compromission de compte
- 3- Compromission poste de travail
- 4- Vol / perte / destruction de matériel chiffré
- 5- Atteinte aux droits d'auteurs

! ATTENTION !

-  Difficulté de perception
-  Tendance à minimiser l'impact
-  Rétablissement du service vs gestion de l'incident

Exemples traités par le CERT-OSIRIS

Gravité 1 :

Plusieurs vols d'ordinateurs non chiffrés

Données de recherche sur un site ftp privé et non protégé

Site intranet ouvert sur internet (erreur filtrage FW)

Intrusion et prise de contrôle total de l'ordinateur

Perte de téléphone

Tout vol ou perte d'un ordinateur ou d'un téléphone est un incident SSI !

Vol d'un ordinateur **non chiffré** = gravité 1
Vol d'un ordinateur **chiffré** = gravité 4

Détection d'un incident

Les compromissions ne sont pas souvent très visibles, tout comportement anormal d'un ordinateur mérite une attention particulière.

Qualification

La qualification d'un incident se fait après un diagnostic des symptômes, du système, des traces/logs des équipements réseaux, etc. Ne peut être réellement évaluée qu'une fois l'analyse terminée

Réaction / Traitement

Dépend du diagnostic et du type d'incident.

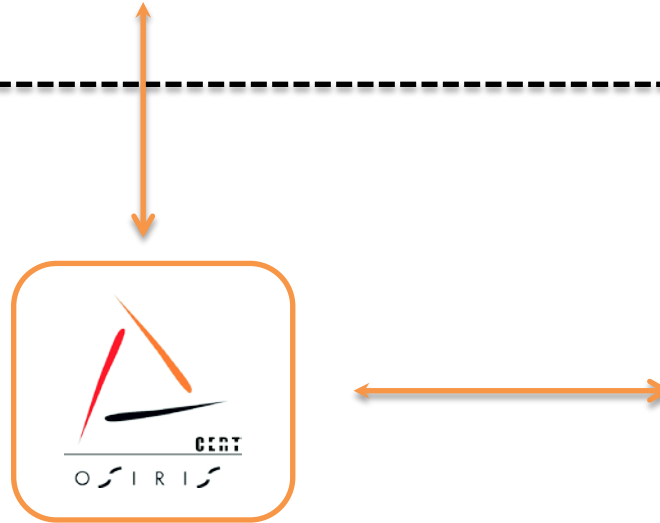
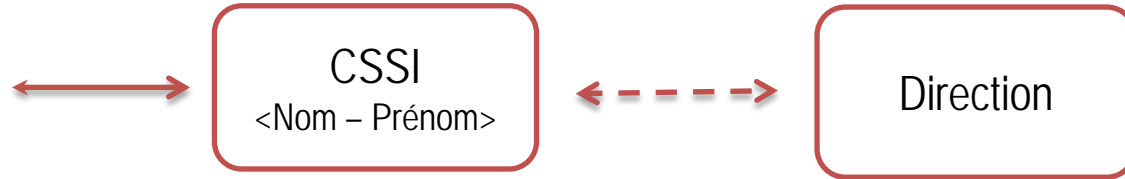
Exemple « Compromission d'un poste » : éradication ou réinstallation ou mise sous scellé et/ou dépôt de plainte, etc.

Une **prise en compte rapide** permet de circonscrire (= protéger les autres) et réagir efficacement par le choix d'un traitement adapté



Règle 10 - Ordinateur infecté : ça arrive(ra) à tout le monde, pas de panique

- La règle
- Les bonnes pratiques
- Les outils



cert-osiris@unistra.fr



Quelques signes cliniques d'une infection

- Blocage de l'ordinateur
- Ouverture intempestive de fenêtres
- Alerte du parefeu
- Présence et la disparition immédiate de boîtes de dialogue au démarrage
- Message d'erreur cyclique et récurrent
- Présence de **fichiers** inconnus (film, musique, etc.) sur le poste de travail
- Rapport de l'anti-virus
- Lenteurs inexplicables ou consommation de mémoire anormale
- Activité réseau intempestive



Si le compte compromis a les droits d'ADMIN
=> réinstallation complète du poste

Si non, on peut tenter d'éradiquer le malware :

- Débrancher le poste analysé du réseau
- Sauvegarder les données importantes en cas d'erreur de manipulation
- Se connecter avec un profil ADMIN
- Vérifier l'intégrité du cœur de Windows à l'aide de l'outil Rootkit [Rootkit Revealer](#)
- Vérifier les programmes en cours d'exécution à l'aide de l'outil [Process Explorer](#)
- Vérifier les programmes lancés automatiquement au démarrage de Windows ou d'une application à l'aide de l'outil [Autoruns](#)
- Vérifier l'activité réseau à l'aide de l'outil [Tcpview](#)
- Supprimer les programmes malveillants à l'aide d'outils dédiés ou par un système externe

<https://security.symantec.com/nbrt/overview.aspx?lcid=1033&origin=default>

« La sécurité est avant tout affaire d'état d'esprit, pas de produits.
Tous sont par essence faillibles. »

Eric Filiol

