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

Module 1
Panorama des menaces SSI

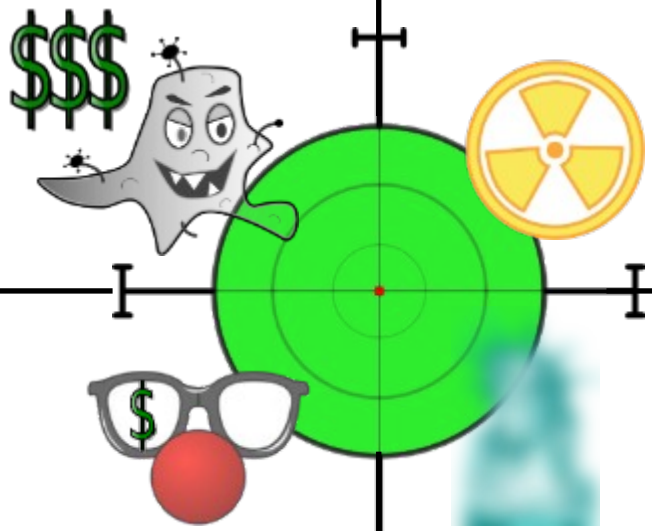
Module 2
Les règles élémentaires de protection

Janvier 2015 – Guilhem BORGHESI

Les menaces sur Internet

Crime organisé

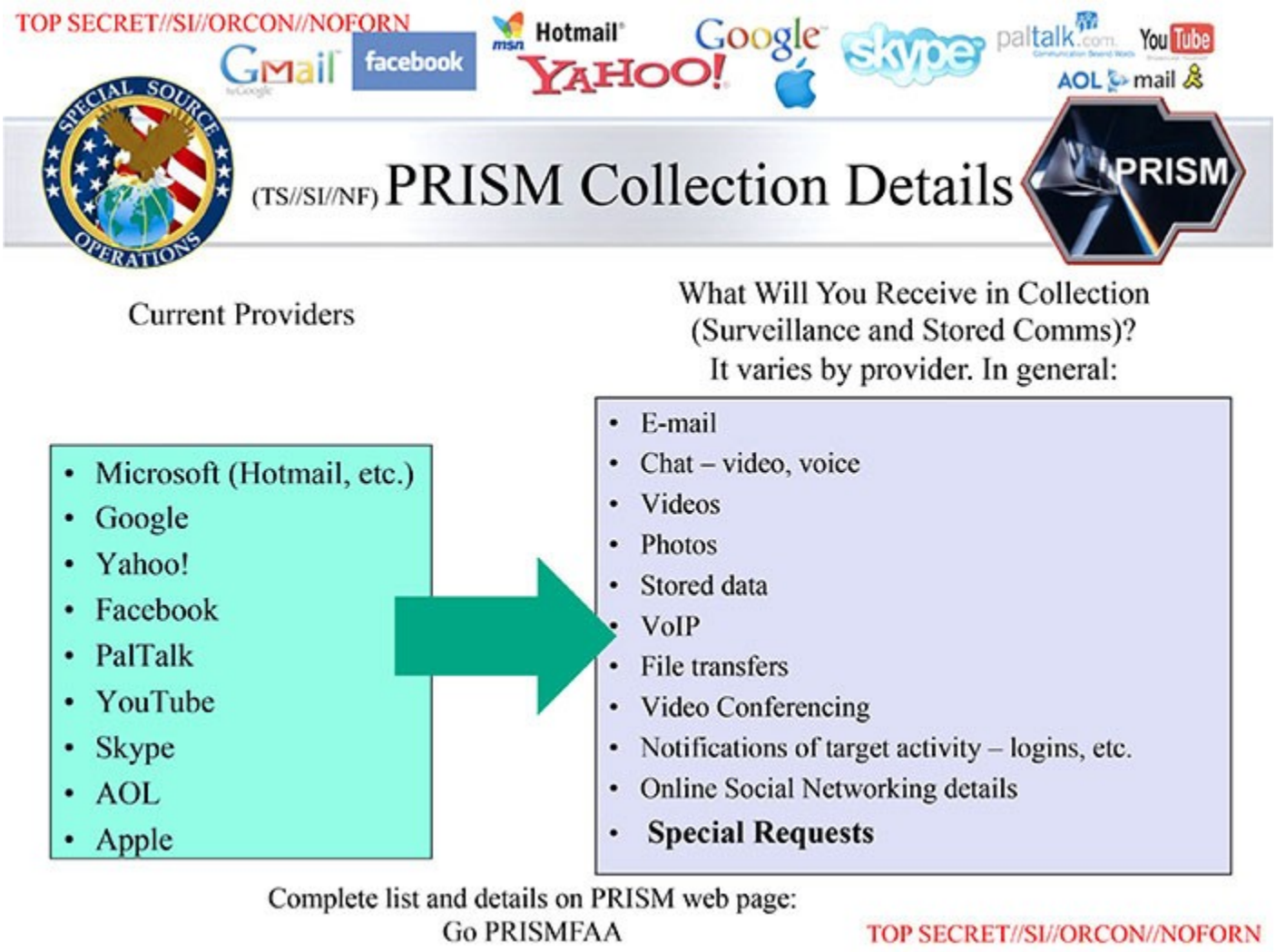
Services d'États



Petits génies

Hacktivistes

Les services d'États



Collecte de données et de métadonnées

Les services d'États

Le Monde

9 juin –> 21 octobre 2013

Le Monde : **306 articles** citent Edward Snowden

Une équipe de 10 journalistes travaillent sur l'histoire du programme PRISM et la surveillance de la France par les services secrets US

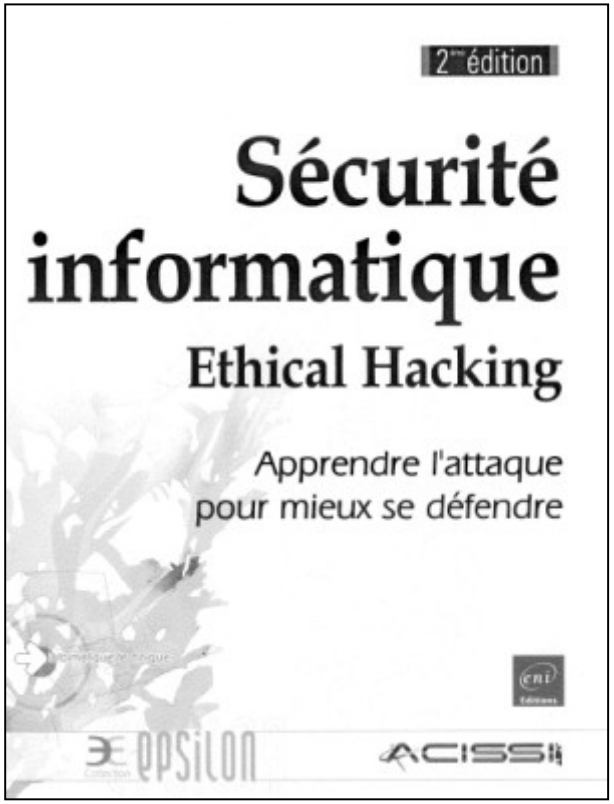
Editorial du 21 octobre

« Les *"révélations Snowden"* ne visent pas à affaiblir les sociétés démocratiques mais à les consolider, à éveiller les consciences sur les risques que comportent pour nos valeurs ce gigantesque ratissage de données permettant de lire dans nos vies, nos contacts, nos opinions, comme à livre ouvert. »

Le Crime organisé (Botnet Wadelac, démantelé en 2009)

Le Crime organisé (virus CryptoLocker, encore actif)

Les petits génies



Les petits génies

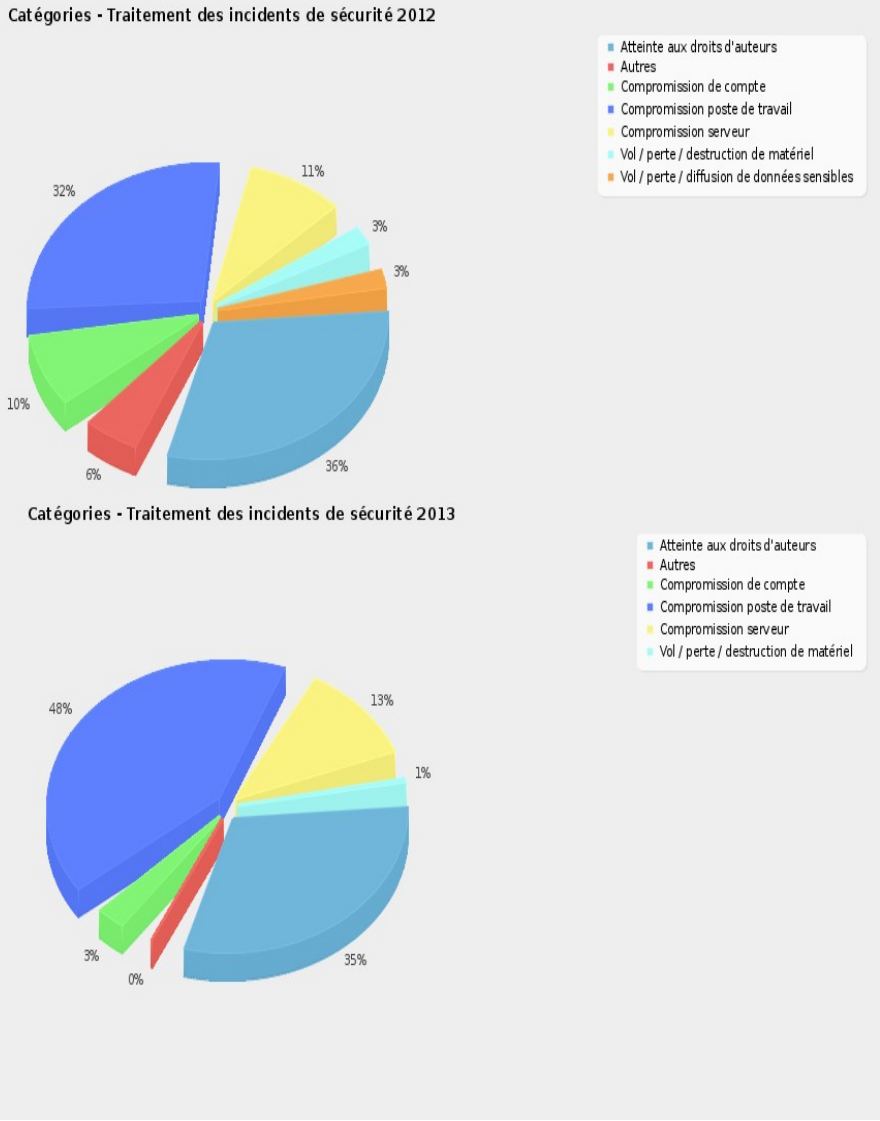
AUTRICHE - Arrestation d'un adolescent soupçonné d'avoir attaqué les serveurs de 259 sociétés en trois mois : âgé de 15 ans, il a été arrêté par la police autrichienne qui l'accuse de défigurations de sites Internet et d'exfiltrations de données sensibles. Il a utilisé plusieurs **logiciels largement diffusés sur internet** dont certains logiciels d'anonymisation.

(*Kurier* du 13/04/12, *ZDNet* du 17/04/12)

Et chez nous,ça donne quoi tout ça ?

Incidents de sécurité 2012 et 2013

	2013	2012
Droits d'auteur	180	79
Compromission de compte	17	22
Compromission de poste de travail	247	71
Compromission serveur	68	24
Vol/perte/destruction matériel	4	6
Vol/perte/destruction données sensibles	0	6
Autres	1	22
Total	517	222



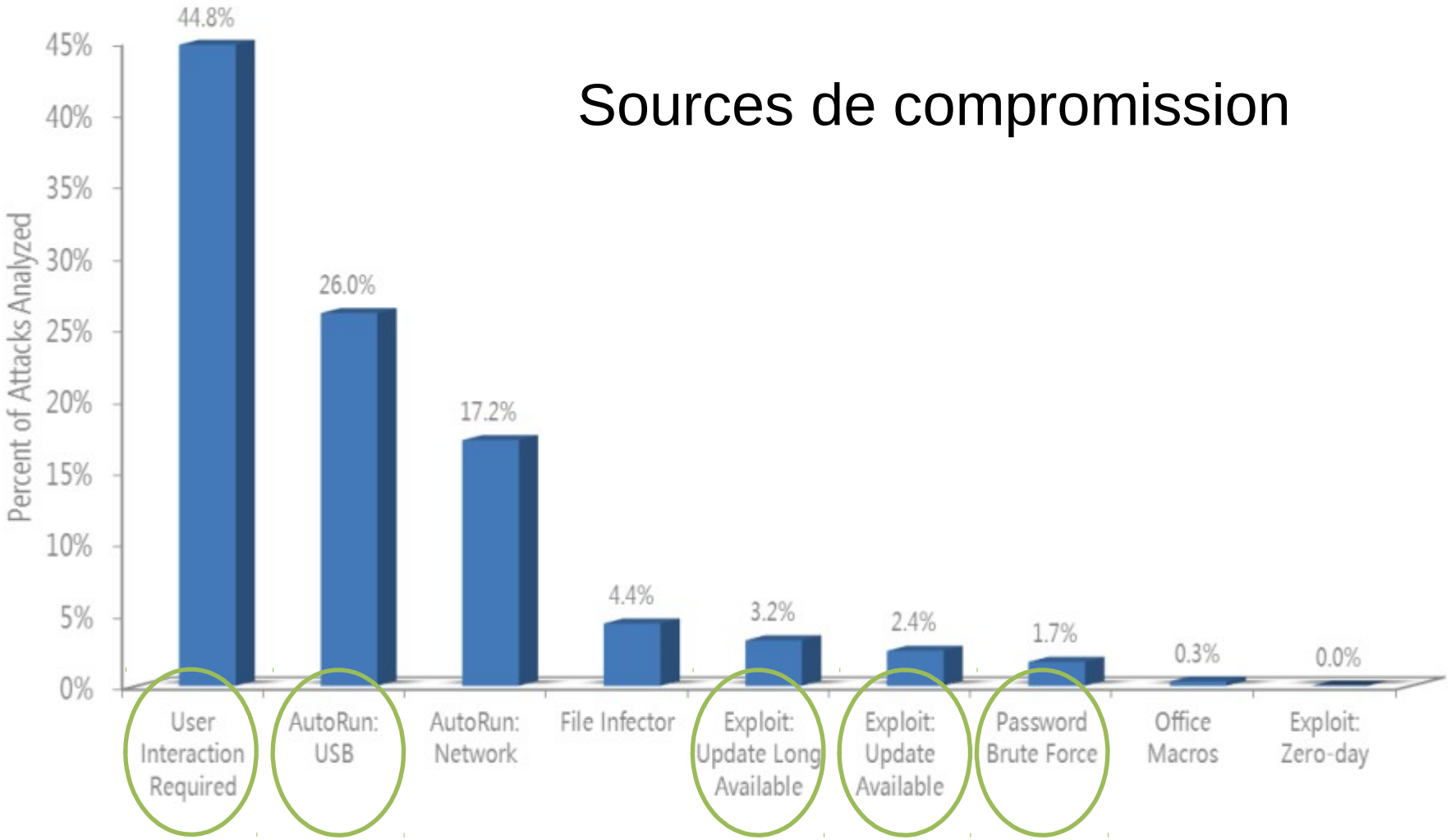
Des exemples concrets à l'Université

- Téléchargement de films par des étudiants
- Hébergement d'images illégales par un personnel d'université
- Perte de toutes les données d'un doyen en Sciences Humaines
- Réinstallations régulières de postes infectés
- Diffamation d'un étudiant par courrier électronique anonyme
- Blocage de tous les mails UdS après une campagne de phishing

Nous sommes tous concernés !

Que faire ?

Sources de compromission



Que faire ?

Tous les internautes sont exposés en permanence à des menaces

La majorité des compromissions est due à une mauvaise manipulation

Il faut donc sensibiliser à **l'application des Bonnes Pratiques Utilisateur (BPU)**

Module 2
Les règles élémentaires de protection

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

Mai 2014 – Guilhem BORGHESI

LES 10 REGLES pour protéger son poste informatique

Obligations légales

Règle 1 – Respect des chartes informatiques

La protection technique du poste de travail *(par la DI sur vos postes)*

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 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 – Prudence sur Internet

Règle 9 – Prudence avec la messagerie

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

LES 10 REGLES pour protéger son poste informatique

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 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 - Prudence sur Internet

Règle 9 – Prudence avec la messagerie

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

Réseau OSIRIS

Charte OSIRIS

https://services-numeriques.unistra.fr/services-osiris/cert-osiris/charte-osiris.html

Université de Strasbourg

Charte 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.

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

  – Arrêt du 17 mai 2005

  Sauf risque ou événement 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

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 »

http://www.cnil.fr/vos-droits/vos-droits/

- Guide “Informatique et Libertés” pour l’enseignement supérieur et la recherche (*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

Obligations légales

Règle 1 – Respect des chartes informatiques

La protection technique du poste de travail *(par la DI sur vos postes)*

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 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 - Prudence sur Internet

Règle 9 – Prudence avec la messagerie

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

Règle 2 - Sauvegarde systématique et quotidienne des données

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**.

Évitez les outils de « cloud public » *:*
Dropbox, Gdrive, iCloud ...
Préférez le dépôt de vos données sur un espace de stockage ***privé et maîtrisé***

UNIVERSITÉ DE STRASBOURG

Seafile™

La sauvegarde est prise en charge par la DI sur vos postes

LES 10 REGLES pour protéger son poste informatique

Obligations légales

Règle 1 – Respect des chartes informatiques

La protection technique du poste de travail *(par la DI sur vos postes)*

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 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 - Prudence sur Internet

Règle 9 – Prudence avec la messagerie

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

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

Ces 3 éléments sont pris en charge par la DI sur vos postes

LES 10 REGLES pour protéger son poste informatique

Obligations légales

Règle 1 – Respect des chartes informatiques

La protection technique du poste de travail *(par la DI sur vos postes)*

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 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 - Prudence sur Internet

Règle 9 – Prudence avec la messagerie

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

Règle 4 - Limitation des droits « administrateurs »

OBJECTIFS

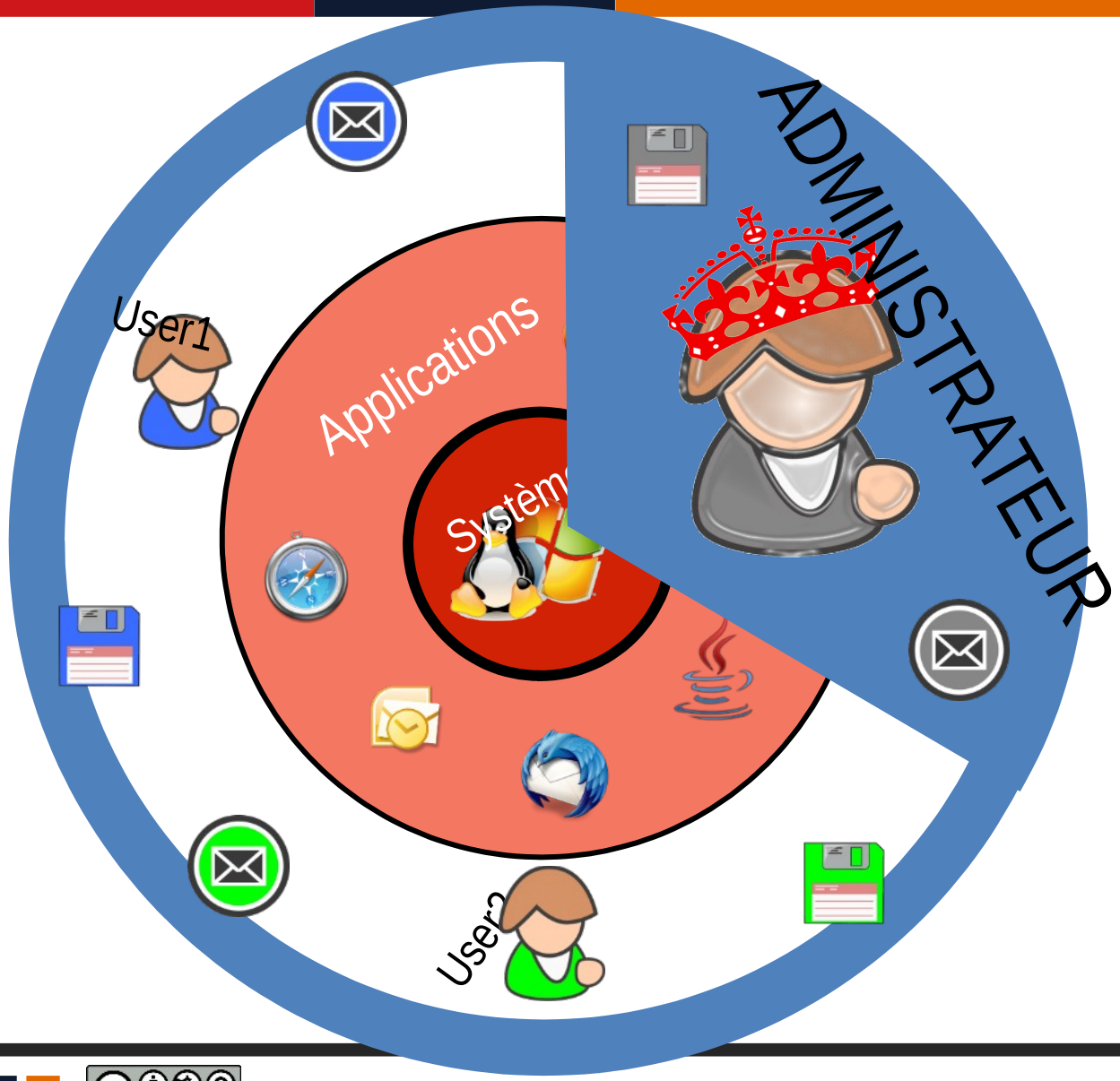
- Cloisonner les utilisateurs, les applications et le système
- Limiter les risques de propagation de virus
- Ne pas exposer les autres comptes présents sur le même ordinateur
- Protéger le système d'exploitation
- Éviter les erreurs de manipulation

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.)

La DI vous fournit un compte « standard » et non pas « administrateur »

Règle 4 - Limitation des droits « administrateurs »



LES 10 REGLES pour protéger son poste informatique

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 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 – Prudence sur Internet

Règle 9 – Prudence avec la messagerie

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

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

- *Ne pas laisser son bureau ouvert sans surveillance*
- *Protéger l'écran de veille par un mot de passe*
- *Ne pas écrire le mot de passe (écran, clavier)*
- *Ne pas laisser accéder à votre ordinateur à d'autres personnes (que vos collègues ou la DI)*

Les ordinateurs portables ou ordiphones sont également concernés !

Anticiper la perte

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

Conseils

- *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-2010.pdf

LES 10 REGLES pour protéger son poste informatique

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 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 - Prudence sur Internet

Règle 9 – Prudence avec la messagerie

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

Tout accès à un système informatique doit être protégé.
Chaque utilisateur doit s'authentifier nominativement pour protéger ses données et permettre un contrôle des accès.

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 :

- De sa longueur : 8 caractères minimum
- De la capacité de le deviner facilement : pas un mot du dictionnaire
- De la combinaison de différents types de caractères utilisés :
  - Caractères normaux, spéciaux, majuscules et chiffres.

Les attaques sur les mots de passe :

- Force brute : toutes les combinaisons sont essayées.
- 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.

*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 ans) 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.)*
- *Idéalement, **ne pas laisser** les navigateurs ou autres logiciels **mémoriser** vos mots de passe*

LES 10 REGLES pour protéger son poste informatique

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 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 - Prudence sur Internet

Règle 9 - Prudence avec la messagerie

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 ou de vol,
- au transport de virus en tout genre,
- une détérioration plus rapide.

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, …*

LES 10 REGLES pour protéger son poste informatique

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 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 - **Prudence sur Internet**

Règle 9 - Prudence avec la messagerie

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

Le navigateur est **LA plate-forme d'échange** avec Internet

Chaque **CLIC** génère une ou plusieurs interactions entre internet et l'ordinateur

Le navigateur conserve les informations de visite de pages web :

- 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.

Navigation *

Téléchargements *

Services gratuits *

Pour les achats sur Internet, il faut privilégier les sites de confiance

Qu'est-ce qu'un site de confiance ?

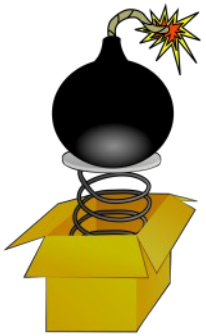
- Le site web utilise-t-il le protocole sécurisé *https* ?
- Le site web appartient-il à une entreprise connue ?
- L'entreprise est-elle clairement identifiée et localisée (voir *mentions légales*) ?
- Est-il possible de contacter quelqu'un par téléphone ou par courrier ?

Navigation *
Téléchargements *
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.



- Éviter les téléchargements illicites (logiciels craqués, œuvres protégées…)
- Éviter les installations de petits logiciels gratuits (jeux, utilitaires, ...)

- Privilégier les logiciels préconisés par la DI

UNIVERSITÉ DE STRASBOURG

Navigation *
Téléchargements *
Services gratuits *

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 *
Téléchargements *
Services gratuits *

- 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 (google, yahoo, microsoft, apple, ...)

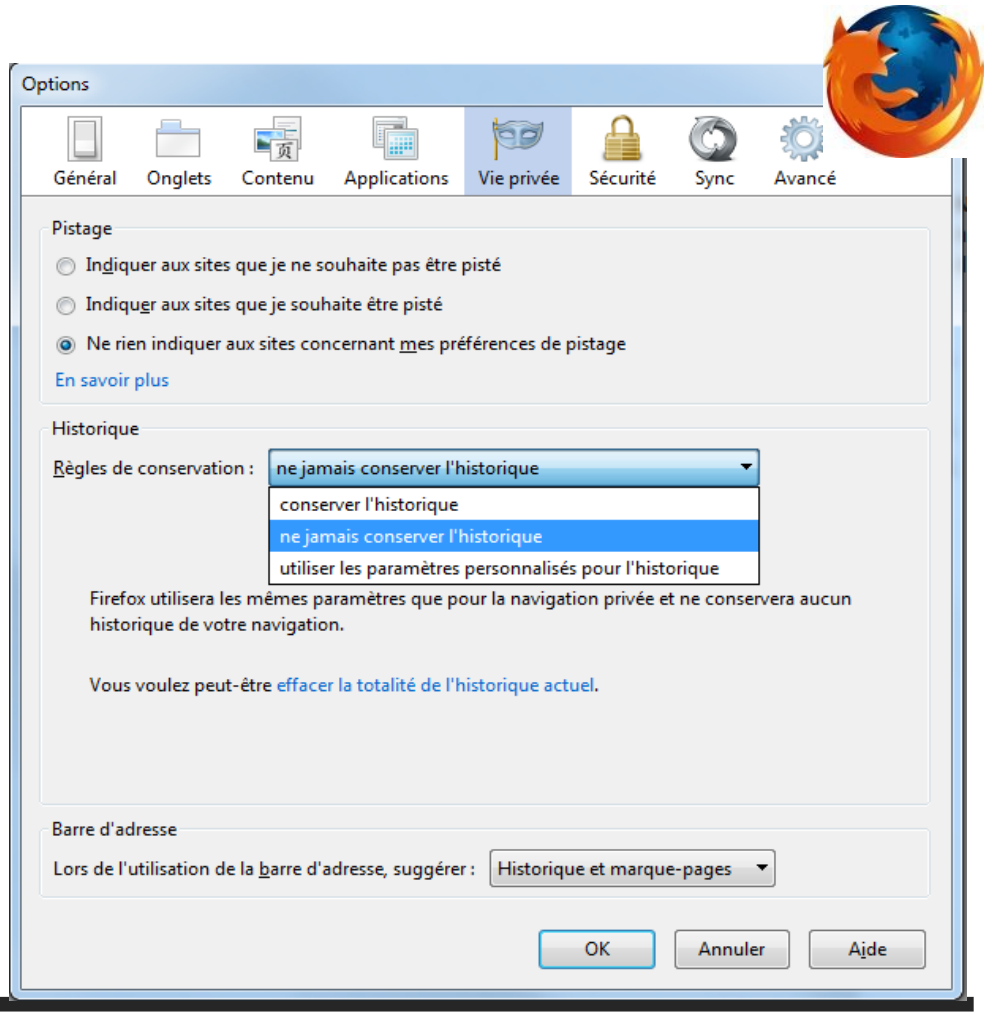
Données stratégiques (recherche, finance, RH…)
Données de valorisation
Données scientifiques
Données d'enseignement (sujets, relevés de note…)
Données à caractère personnel (CNIL)

Navigation *
Téléchargements *
Services gratuits *

Passer en mode de navigation privée

Navigation privée

En savoir plus… *la navigation privée*
Navigation privée Firefox
Navigation privée Chrome
*InPrivate : n*avigation privée Internet Explorer



Il existe des modules pour sécuriser la navigation

Modules complémentaires

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/

A propos des ActiveX et des Javascript
http://www.securite-informatique.gouv.fr/gp_article74.html

LES 10 REGLES pour protéger son poste informatique

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 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 - Prudence sur Internet

Règle 9 – Prudence avec la messagerie

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

N'importe qui peut envoyer un mail dans votre boite 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 :

- Message contenant un lien frauduleux pour aboutir à une infection

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.

- Demandes d'informations confidentielles, soit en réponse au mail soit via un lien sur un formulaire

Banques, EDF, CAF, service informatique

- Exécution d'une pièce jointe malveillante

Fichiers PDF, PowerPoint, images jpg

- Canulars ou chaînes de diffusion d'informations non vérifiées

Catastrophes naturelles, disparition de personnes et autres

Utiliser son esprit critique et son discernement !

- 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.

LES 10 REGLES pour protéger son poste informatique

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 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 - Prudence sur Internet

Règle 9 - Prudence avec la messagerie

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

La seule chose certaine c'est qu'un jour vous serez infectés !

Quelques signes cliniques d'une infection

- Blocage de l'ordinateur
- Ouverture intempestive de fenêtres
- Alerte du pare-feu
- 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 inexpliquées ou consommation de mémoire anormale
- Activité réseau intempestive

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

P. 49

Correspondant informatique

Support Informatique

CERT OSIRIS

UNIVERSITÉ DE STRASBOURG

cert-osiris@unistra.fr

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

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

- Débranchant le poste compromis du réseau
- Sauvegardant les données importantes
- Effectuant le nettoyage nécessaire avec les outils adéquats
- Et ensuite, on espère que cela aura suffit...

Conclusion

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

Questions / réponses

Merci de votre attention !