La sécurité, c'est uniquement un problème technique

Je sauvegarde tous mes fichiers dans le cloud : simple, pratique et gratuit

Même au travail, je préfère utiliser ma messagerie privée, c'est plus pratique

Pas de risque, j'ai un antivirus

ATTENTION ! IDÉES REÇUES

Je n'ai aucune information sensible

Mon compte est «Administrateur», facile et pratique

Mon mot de passe, c'est le sigle du labo : simple à trouver et pratique à retenir

Ma vie privée sur internet ? Je n'ai rien à cacher...

L'ARNAQUE 2.0...

«Vous acceptez nos conditions et reconnaissez avoir lu et compris notre politique d'utilisation des données»

SERVICES GRATUITS...

« Si c'est gratuit, c'est TOI le produit »

CERT OSIRIS

Informations détaillées, conseils et outils

http://cert-osiris.unistra.fr

Contact et déclaration d'incident

votre CSSI : .....

(à défaut : cert-osiris@unistra.fr)

Conception et réalisation : CERT-OSIRIS
Version novembre 2013

C'est facile, c'est utile

DIX RÈGLES PRATIQUES

pour protéger votre vie numérique

cnrs

UNIVERSITÉ DE STRASBOURG

Les 10 règles d'or

RÈGLE N° 1 — Obligations légales

RESPECT DES CHARTES INFORMATIQUES

Lisez attentivement les chartes relatives à vos établissements de rattachement (Université, CNRS, autres)

RÈGLE N° 2 — Protection technique

SAUVEGARDE SYSTÉMATIQUE DES DONNÉES

Dupliquez quotidiennement vos données,
stockez les supports en lieu sûr
Une sauvegarde vous sera nécessaire pour récupérer vos informations en cas de vol ou de panne matérielle

RÈGLE N° 3 — Protection technique

UTILISATION DES OUTILS DE PROTECTION

Utilisez un **antivirus** et activez les mises à jour automatiques
Activez le **pare-feu**
Activez les **mises à jour automatiques** du système d'exploitation et des logiciels

RÈGLE N° 4 — Protection technique

LIMITATION DES DROITS «ADMINISTRATEURS»

Utilisez par défaut un compte «**Standard**» pour naviguer sur internet et lire vos mails
Une infection virale d'un compte «**Administrateur**» nécessite une réinstallation complète du poste

RÈGLE N° 5 — Comportement utilisateur

PROTECTION DES ÉQUIPEMENTS NOMADES

Chiffrez votre ordinateur portable, les données seront protégées en cas de vol
Activez le verrouillage automatique des téléphones
Activez le chiffrement des tablettes, des téléphones, des clés USB si l'équipement le permet

RÈGLE N° 6 — Comportement utilisateur

UTILISATION DE MOTS DE PASSE ROBUSTES

Vos mots de passe sont **les seuls remparts** pour les accès à votre messagerie, aux réseaux sociaux, à la banque en ligne, aux achats en ligne, etc.
Soignez-les : choix pertinent et stockage sécurisé

RÈGLE N° 7 — Comportement utilisateur

SE MÉFIER DE TOUT SUPPORT AMOVIBLE

Les **clés USB** sont un vecteur très utilisé pour le piratage des postes de travail
Une clé infectée peut compromettre un poste lors de son utilisation

RÈGLE N° 8 — Comportement utilisateur

UTILISATION PRUDENTE D'INTERNET

Navigateurs : activez les modules complémentaires pour renforcer votre protection et utilisez la navigation privée
Téléchargements : uniquement depuis des sites de confiance
Achats - Paiements : vérifiez la fiabilité du site
Publications : vous êtes auteur-responsable de tous les contenus que vous publiez et diffusez sur internet

RÈGLE N° 9 — Comportement utilisateur

UTILISATION PRUDENTE DE LA MESSAGERIE

Identifiez l'expéditeur avant d'ouvrir le message
Vérifiez les liens dans les courriels avant de cliquer
N'envoyez aucune **information sensible** par courriel

RÈGLE N° 10 — Comportement utilisateur

ORDINATEUR INFECTÉ : LES BONS RÉFLEXES

Contactez sans délai votre chargé de sécurité (CSSI), un incident mineur peut en cacher un autre plus grave
En cas d'infection avérée, changez de suite tous vos mots de passe