Ressources informatiques à l'ENS sécurité des données : Découverte / présentation des possibilités et conseils d'utilisation

Présentation SSI
Présentation NPS
Présentation DGNUM

Les acteurs des systèmes d'informations (enseignement)

- Une organisation sectorisée
  - Le Centre de Ressources Informatique (CRI)

    → login fourni par le CRI
  - Le pôle Numérique Pédagogique et Scientifique (NPS)

    (ex Service de Prestation Informatique (SPI))

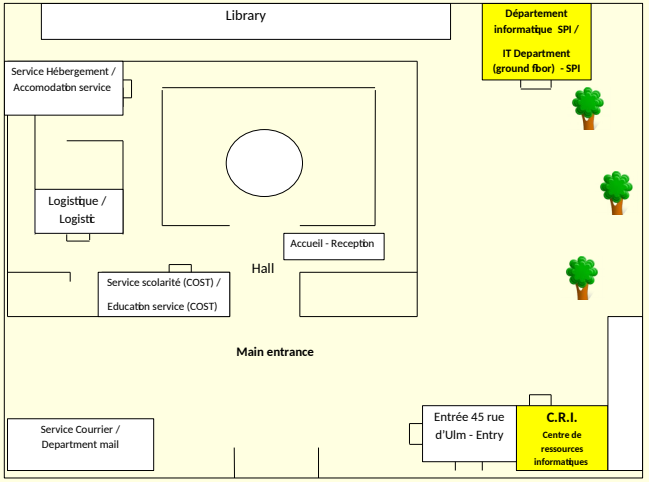
    → login fourni par le NPS
  - Les plateformes informatiques dans les départements

    → login fourni par les départements

Le centre de ressources informatiques (CRI)

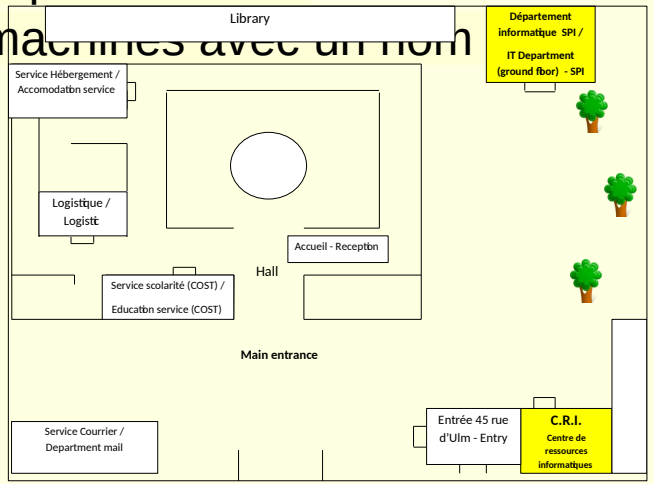
- Responsable : Christophe Ngo
- Gestion du réseau, des services/applications adminstratifs
  - Réseau Wifi Eduroam avec identificant : loginCRI@ens.psl.eu
  - Réseau Wifiens portail captif avec authentification via navicateur web (login CRI)
  - Réseau filaire : fournir l'adresse Mac pour l'identification
  - Plateforme pédagogique Moodle : https://moodle.psl.eu
  - ~~GPS : https://gps.ens.psl.eu~~
  - Pegasus : https://ens-etud.helvetius.net/pegasus
  - Dossier de scolarité normalienne (DSN)
  - Services RENATER utilisant SSO (Single Sign-On)
- Localisation : Pavillon Pasteur (derrière la loge du 45)
  - Ouverture au public :
    - Période normale : lundi, mardi, jeudi, vendredi 10h-12h 14h-16h
    - Période de rentrée : lundi – vendredi 9h30-12h 13h-17h
- Contact : assistance-cri@ens.psl.eu

  → à privilégier, la plupart des traitements se font à distance
- Web : https://intranet.ens.psl.eu/fr/services-administratifs/centre-de-ressources-informatiques



Le pôle Numérique édagogie Scientifique (NPS)

- Responsable : Jean-Marc Notin
- Gestion des services/applications pédagogiques/associatifs
  - Messagerie (clipper)
    - Adresse générique : prenom.nom@ens.psl.eu
    - connexion avec login NPS via imap/smtp ou webmail
  - Salles informatiques élèves libre-service (machines avec un nom bateau)
  - Cloud, Visioconférences,...
- Bâtiment Rataud (fond de la cour Pasteur au 45)
- Contact : nps@ens.psl.eu
- Web : https://www.spi.ens.psl.eu

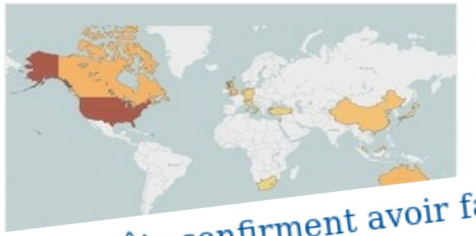


L'insécurité informatique...
Ce n'est pas de la fiction!

Dans l'actualité

Les pirates du Département d'Indre-et-Loire diffusent les informations volées

Posted On 23 Août 2022 By : Damien Bancal Comment: 1 Tag: Département d'Indre-et-Loire, piratage, touraine, vice

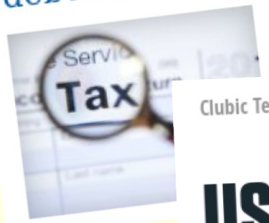


LE 24 AOUT 2018 / SÉCURITÉ

Cobalt Dickens : 76 universités visées par des attaques par usurpation

Une deuxième attaque [illegible] par le groupe de pirates [illegible] de bibliothèques en ligne

Les impôts confirment avoir fait face à une vague de piratages au début de l'été



Sécurité - Le ministère de l'Économie et des Finances a confirmé hier qu'une vague de piratage avait été détectée sur son service impots.gouv.fr en juin. Celle-ci a affecté un peu plus de 2000 contribuables, mais le ministère assure que la situation

Trump confirme une cyber attaque à l'encontre d'une entreprise Russe

Le Président Américain, Donald Trump, a confirmé une cyber attaque à l'encontre d'une

Clubic Tech > Sécurité informatique

Par Dimitri PAVLENKO
le dimanche 03 septembre 2017

USA : des pacemakers rappelés pour risque de piratage

CYBERATTAQUE CYBERSÉCURITÉ LOI

Cyberattaque contre la Commission électorale britannique : Une menace prévisible pour les démocraties modernes

La fragilité croissante des systèmes d'information dans les démocraties modernes a été mise en évidence une fois de plus alors que la Commission électorale britannique a récemment divulgué avoir été victime d'une cyberattaque complexe.

Damien Bancal 21 août 2023

=> Il faut se protéger...

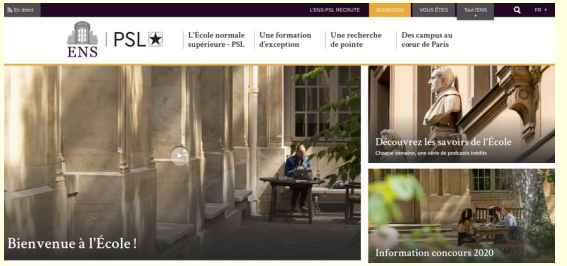
L'insécurité informatique... ce n'est pas de la fiction!

- De nombreux incidents avec des conséquences souvent graves...
  - Un vol d'identifiants (login/mot de passe) peut permettre au délinquant l'envoi de spams, l'usage indélicat d'un compte, l'accès aux données de l'utilisateur, le piratage de site web, du vol d'argent,...
  - Un vol d'ordinateur, c'est aussi un vol de données qui peuvent être exploitées (usurpation d'identité pour souscription de crédits, chantage, faux appels au secours,...)
  - Une machine infectée par un virus peut induire des conséquences graves : altération ou destruction de données (ex : cryptolocker), plate-forme d'attaque (botnet),...
  - Le téléchargement illégal (P2P, loi Hadopi,...) peut conduire à de lourdes amendes...
  - L'usurpation d'identité peut conduire son auteur devant les tribunaux et est très difficile à vivre par la victime…
  - L'espionnage peut coûter cher...

=> Il faut se protéger...

La politique de sécurité des systèmes d'information à l'ENS

- Un patrimoine humain, culturel, immobillier,...
- Des collaborations ou contrat de recherche avec d'autres entités,…
- et beaucoup d'autres «actifs» :
  - recherche donnant lieu à publication, à brevet, à prix Nobel,…
  - support de cours,…
  - données nominatives, données sensibles,…



=> Un environnement professionnel à protéger

- Une organisation structurée.
- La PSSI en vigueur a été signée par le conseil d'administration le 14 avril 2010. Elle a été révisée en 2016.
- Une charte des bons usages des systèmes d'information existe depuis plus de 30 ans et évolue régulièrement

Se protéger : la SSI

→ De nombreuses lois (CNIL 1978, Godfrain 1988, ..., Hadopi, Lopsi 2, RGPD)

→ Des règles à appliquer ou Politique de Sécurité des Systèmes d'Informations (PSSI de l'État, juillet 2014)

→ Des brigades spécialisées de police et de gendarmerie (BEFTI, OCLCTIC,...)

→ Des spécialistes de la sécurité des systèmes d'informations (ANSSI, CERTs,…)

De nombreuses lois

- CNIL (1978), révisé en 2004
- La loi sur les droits d'auteur : 4 juillet 1985
- La loi Godfrain sur la fraude informatique : 5 janvier 1988
- La loi sur la francophonie (1994)
- Les lois sur la cryptographie
- la LSQ (2001), la LEN (2003)
- la DAVDSI (juin 2006)
- Les lois Hadopi (juin 2009) et Hadopi2 (octobre 2009)
- La Loppsi (2011)
- La loi sur la circulation des données et le savoir (2016)
- Le Réglement Général de la Protection des Données (2018)
- et toutes les lois non spécifiques !

Se protéger : la SSI

→ De nombreuses lois (CNIL 1978, Godfrain 1988, ..., Hadopi, Lopsi 2, RGPD)

→ Des règles à appliquer ou Politique de Sécurité des Systèmes d'Informations (PSSI de l'État, juillet 2014)

→ Des brigades spécialisées de police et de gendarmerie (BEFTI, OCLCTIC,...)

→ Des spécialistes de la sécurité des systèmes d'informations (ANSSI, CERTs,…)

Les CERTs

- CERT : Computer emergency response team
  - Organismes assistant les utilisateurs des réseaux sur le plan de la sécurité informatique afin de traiter les incidents et de les prévenir.
- L'ENS connectée via le réseau Renater est adhérente de fait au CERT-Renater.
  - Répondre et traiter les requêtes qui nous sont transmises sous peine d'exclusion du réseau et autres poursuites éventuelles
    - Identification de machines infectées par des virus
    - Localisation de trafic «atypique»
    - Signalement de machines piratées ou de machines «attaquantes»
    - ...

Une organisation de la SSI à l'ENS

- **AQSSI :**
  - Frédéric Wolf (Directeur)
- **FSD (Fonctionnaire sécurité défense):**
  - Myriam Fadel (DGS)
- **DPD (Délégué à la protection des données)**
  - Gwendoline Joly-Jagot
- **RSSI :**
  - Pierre Vincens et Jean-Marc Notin
    - → web : http://www.ssi.ens.fr
    - → courriel : rssi@ens.psl.eu
- **CSSIs au niveau des unités.**

→ **Comité de pilotage de la SSI**

→ **Collaboration avec le CNRS, l'INSERM, Sorbonne Université,... (COCSSI)**

PSSI et charte

- Des dispositions adaptées à l'environnement
    - Professionnel à vocation de recherche et d'enseignement
    - Connexion performante à travers les réseaux RENATER (impose un usage professionnel)
    - Évolution régulière en fonction du contexte
- Tout utilisateur de SI à l'ENS doit les respecter
    - Suspension temporaire de l'usage des ressources à titre conservatoire
    - Renvoi vers des procédures disciplinaires ou judiciaires

=> RÉPONDRE RAPIDEMENT aux requêtes des RSSIs

Des obligations légales

- Obligation de répondre aux injonctions gouvernementales et aux requêtes judiciaires

From: Isabelle XXX <XXX@recherche.gouv.fr>
Date: Thu, 7 Jul 2005 19:24:30 +0200
Subject : Information du COSSI aux ministères
A la suite des attentats à Londres et compte tenu de la nature de la menace, [...] mesures [...] dans le cadre du plan VIGIPIRATE porté au niveau rouge.
Les mesures SSI actuellement activées sont les suivantes : ...

Charte 4.1, 4.3, 4.4, 4.8, 4.9, 4.12, 3

Le Rézo dans les chambres

- Le «rézo»
  - Couvre l'ensemble des hébergements de l'ENS («turnes» de Jourdan, Montrouge et Ulm)
- Règles d'usage
  - La charte de bon usage des systèmes d'informations et la PSSI s'y appliquent comme partout ailleurs
  - Usage «professionnel» imposé par le contrat qui lie l'ENS à RENATER
    - Les usages personnels doivent rester marginaux
      - 90Go en 1 jour de trafic Netflix n'est pas marginal !
- Comment faire ?
  - S'enregistrer en se connectant avec les identifiants du NPS (clipper) à: **https://www.eleves.ens.fr/rezoweb**

La charte du bon usage des systèmes d’informations

—

Points importants

Protéger physiquement ses équipements

- Un ordinateur, un smartphone,... cela peut être volé !
    - Un vol par mois identifié impactant la communauté de l'ENS
        - Dans l'ENS
        - Dans un lieu public : restaurant, cinémas,…
        - Dans les transports : sacoche sur un vélo
        - Chez soi

    → Attacher les équipements, fermer les portes
- Attention aussi aux pertes et maladresses
    - Oubli dans un avion, un train,…
    - Clé USB dans la machine à laver

→ Outre la perte de l'équipement, c'est aussi une perte des données et une divulgation potentielle d'information

Environnement de travail

- Utiliser un ordinateur, un smartphone,... dans le métro, le train, dans une salle de travail collective,…
    - Risque du voisin curieux
        - Vision du contenu de votre écran
        - Collecte des informations que vous tapez sur le clavier (mots de passe, informations bancaires,...)
        - « Piratage » de votre connexion bluetooth, wifi,…
        - ...

→ **Utiliser un filtre de confidentialité pour écran**

→ **Désactiver les connexions inutiles**

→ **Ne pas accéder à des données confidentielles**

Maîtriser l’accès aux systèmes de gestion de l’information

- L’accès à l’information, aux moyens de traitement de l’information doit être contrôlé sur la base des exigences d’exploitation et de sécurité et des besoins « métier ».
- L’utilisation des ressources informatiques à l’École est soumise à autorisation préalable, concrétisée par l’ouverture d’un compte ou le droit de connecter un ordinateur sur le réseau (2.1).
- **Les autorisations d'accès sont strictement personnelles (2.2).**

→ Une personne ne peut en aucun cas céder ses droits à un tiers.

=> Tout accès doit être authentifié.

→ Utilisation d’identifiants type login / mot de passe

Identification et authentification

- Identification : annoncer qui je suis
  - Forme directe en donnant un login
  - Forme indirecte via des composants associées à l'utilisateur :
    - Adresse internet : ATTENTION prenom.nom@ens.psl.eu sera différent de prenom.nom@ens.fr
    - Cookies
    - ...
- Authentification : prouver qui je suis
  - solution classique : le mot de passe
  - Mot de passe à usage unique (OTP)
  - Utilisation de chiffrement asymétrique (clé privé/clé publique)

Les vols de mot de passe...

- Vol de puissance de calcul (Ex : Minage de bitcoins)
- Vol de données (Ex : accès aux mails, clouds, services,...)

- De nombreuses méthodes
  - Vol d'ordinateurs, de supports de données (disque, clé USB)
    - Exploitation des données par les voleurs ou receleurs
  - Virus (keylogger)
    - Écoute sur des réseaux peu sécurisés
      → être vigilant notamment dans les lieux publics (4.14)
    - Piégeage (faux serveurs web, faux réseaux wifi,...)
    - Hameçonnage (phishing)

=> en cas de suspicion de vol, changer le mot de passe rapidement.

Identifiants et SSI (4.1)

- Ils ne doivent pas être enregistrés sans protection.
  - En effet, quid si machine volée ?
  - Ne pas utiliser les outils de stockage de mots de passe en ligne (ex : Lastpass,…).
    - Un outil pour les stocker : Keepass
- Ils ne doivent être communiqués à personne :
  - ni à un(e) petit(e) ami(e), à une personne de la famille, . . .
  - en réponse à un courriel, serveurs Web (phishing),
  - à un serveur. Ex. : relève du courrier par Gmail, Hotmail, …
- Les mots de passe doivent être différents pour chque groupe de serveurs ou services :
  - Éviter la propagation du risque en cas de vol !

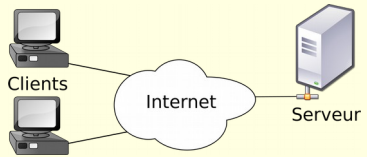
Un bon mot de passe...

- Il doit être robuste (plus de 500 scans SSH, IMAP,... par jour!)
- Ce n'est pas un mot présent dans un dictionnaire, un prénom, un nom, une date de naissance...
- Composé de lettres majuscules, minuscules, de chiffres et de caractères spéciaux

  → Attention à l'accessibilité des caractères spéciaux non disponibles sur certains claviers
- Le plus long possible (12 caractères ou plus)

  → Une méthode : à partir d'une phrase fétiche, conserver la n^{ième} lettre de chaque mot, mixer avec le nombre de lettres d'un mot sur deux, …

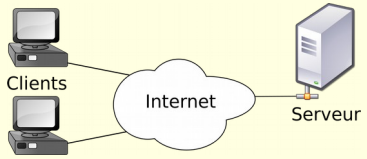
Le modèle client-serveur



- Serveur :
  - Le fournisseur du service: espace de données, affichage, mail, web, tchat,...
- Client :
  - L'utilisateur du service :
- Connexion :
  - Le lien entre le client et le serveur

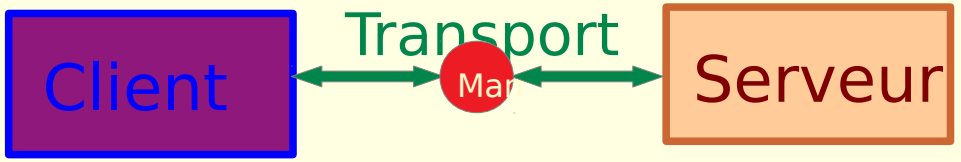
→ **Un modèle efficace mais des risques associées**

Des risques liés au modèle client-serveur

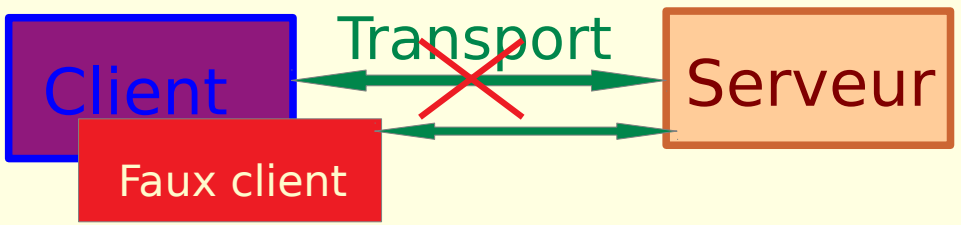


- Faux serveur :
  - Ex : URL modifiée crns.fr au lieu de cnrs.fr

- Interception lors du transport
  - Ex : Man in the middle



- Vol de session client
  - Ex : vol de cookies



Des échanges sûrs…

- **Utilisez des protocoles sécurisés pour vos connexions** (accès à un terminal distant, échanges de fichiers, web, courriel, wifi,…) afin de transmettre le flux de données sans divulgation et garantir la confidentialité des échanges.
  - Protocoles : https, imaps, smtps, ...
  - Outils : ssh, x2go, vpn, ...
- **Vérifiez que le service utilisé est bien celui souhaité, que c'est le bon interlocuteur.**
  - En vérifiant l'identité du serveur (ex : site.co au lieu de site.com)
  - En activant la vérification des certificats (ou en ne la désactivant pas) pour authentifier le serveur

    → ATTENTION : il existe de faux réseaux wifi « eduroam ». S'il n'y a pas de vérification des certificats, quand vous passez à proximité d'un tel réseau, une connexion peut tenter de s'établir et vous exposer à un vol d'identifiant, à une attaque

    → Ne pas outrepasser sans une justification sérieuse les alertes concernant des certificats invalides.

    → **Soyez vigilant**

Le courrier électronique à l'ENS

- Toute personne à l'ENS à une adresse canonique sous la forme :
  - prenom.nom@ens.psl.eu (alias : prenom.nom@ens.fr)

    → cette adresse est virtuelle. Les courriels sont redirigés vers un serveur où se trouve la vrai boîte dans un des domaines de l'ENS
- En tant qu'élèves, vous disposez d'une ou plusieurs boites pour gérer votre courrier :

  → sur le serveur élèves (clipper) : login@clipper.ens.psl.eu (alias : login@clipper.ens.fr)

  → sur un ou des serveurs d'autres départements
- Un outil comme Thunderbird permet de gérer efficacement plusieurs boîtes de courriel. Il existe des outils équivalents sur smartphone (Mail, K9Mail,... sur Android).

  → Le courriel ENS est d'usage systématique, y compris pour des informations importantes. Il faut le lire !

Attention au «Phishing»

«Les utilisateurs doivent être vigilants lors de toute saisie d'informations personnelles sur Internet, notamment avec la multiplication des courriers d'hameçonnage (phishing). L'Ecole ne pourra être tenue responsable des dommages subis lors de telles divulgations d'informations.» (8.3)

Bonjour,
Nous avons récemment déterminé que plusieurs ordinateurs se sont connectés à votre compte. Par conséquent, celui-ci a été limité. Pour rétablir votre accès, vous devez mettre à jour des informations en vous connectant sur notre **site de gestion** et suivre les instructions indiquées.
Cordialement,

Un «Phishing» stressant

→ Stresser le destinataire est une technique classique

- Modifier à sa guise l'adresse d'expéditeur est aussi simple que sur un courrier papier. Attention à l'usurpation d'identité !
  - → Ne jamais payer en cas de demande de rançon, en cas de menaces diverses
  - → Mettre un cache devant sa webcam

Salut
Comme vous l'avez peut-être remarqué, je vous ai envoyé un e-mail depuis votre compte de messagerie.
Cela signifie que j'ai un accès complet à votre compte de messagerie.
Je t'observe depuis quelques mois maintenant. Le fait est que vous avez été infecté par un cheval de Troie via un site pour adultes que vous avez visité.
Si vous n'êtes pas familier avec cela, je vais vous expliquer.
...

Procédures à risque pour gérer son courriel

- **Faire relever ses courriels par un serveur externe** (Google,…)
  - Cela conduit à fournir ses identifiants à un tiers (4.1)
- **Faire suivre son courrier vers un serveur externe**
  - Quelle est le niveau de confidentialité ?
    - Connaissez-vous la politique de filtrage des spams, est-elle fiable ?
    - Pouvez-vous savoir si vous êtes bien le seul à accéder à votre boîte ? Réfléchissez à son contenu !
  - Quel est le niveau de fiabilité ?
    - Les FAI ne s'engagent pas à vous garder !
    - En général, les FAI ne s'engagent à rien vis à vis de la perte de vos archives
  - ATTENTION aussi aux ping-pongs (A renvoie vers B qui renvoie vers A)

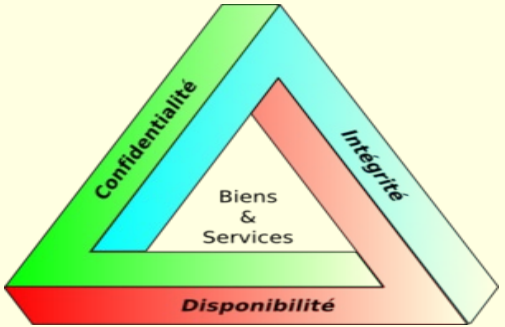
Vos données sont précieuses

- Cela peut être des années de travail telle qu'une thèse.
- Cela peut être des données nominatives.
- Cela peut être des données protégées par contrat.
- Cela peut être des données expérimentales coûteuses à obtenir
- …

  => Ne pas les divulguer (confidentialité)

  => Ne pas les perdre (disponibilité)

  => Ne pas les laisser se corrompre (intégrité)



Vos données privées…

- À vous de voir ce que vous mettez en ligne de votre vie privée.
  - Mais quid quand vous chercherez un travail, ou dans 20 ans ?
- À méditer : est-ce raisonnable de confier à un même prestataire vos courriels, votre carnet d'adresses, vos documents, vos photos, votre agenda, votre carnet de santé,...
  - tout cela protégé par un unique mot de passe, le mot de passe peut être volé
  - Les mécanismes de protection peuvent être défaillants
  - Le compte peut-être clos sans préavis
  - ...

Vos données professionnelles

- Elles vous engagent au titre de votre employeur vis à vis de collaborateurs, partenaires, clients,…

→ **Respecter les règles en vigueur**

- En terme de confidentialité, intégrité, disponibilité
  - Quid des conséquences en cas de divulgation de certains documents (vol de supports de données, erreurs de manipulation,...) ?
  - Attention aux informations cachées dans les fichiers (document conservant une trace des corrections,...)
  - Interception d'informations lors des communications ou du stockage externe

Echanges et stockages d'informations

- Des interrogations :
  - Comment transite l'information ?
    - L'échange se fait-elle via un ou des serveurs externes ?
    - Y-a-t-il chiffrement de bout en bout ou seulement entre le client et le serveur ?
  - Où et comment est stocké l'information ?
    - Qui y a accès ? Comment est-elle protégée de la perte, du vol ?
  - Quelles lois sont applicables ?
    - Chaque État a ses règles (ex : le Patriot Act, le Cloud Act aux USA)
- La PSSI de l'État, les PSSI des tutelles imposent des règles :
  - Circulaire du CNRS sur l'usage des services gratuit

    → Restriction ou interdiction d'usage de certains services tel que Skype, Blackberry, Google Desktop Toolbar, Time Machine (Apple), Gmail,...

Recouvrir ses données en cas de perte

- La sauvegarde (3.4 et 4.10)
  - Disposer d'une copie à jour de ses données en un lieu différent de la source primaire
    - Vol d'un sac contenant le portable et le disque externe utilisé pour la sauvegarde
  - Vérifier que la sauvegarde est pérenne
    - Relire les données et vérifier qu'elles sont identiques et complètes
  - Utiliser des supports de sauvegarde fiables
    - Attention aux supports fragiles ou facilement égarable (clé USB)
  - En cas de recours à des prestataires externes
    - Ils doivent garantir contractuellement la confidentialité, l'intégrité et la disponibilité des données qui leur sont confiées.

Se protéger de l'usage abusif de ses données

- En cas de perte ou de vol de support de données, il faut se protéger de l'usage abusif de celles-ci.
  - Que contient comme données votre ordinateur portable,votre clé USB, votre smartphone?
  - Le chiffrement
    - Obligatoire pour les supports de données (ordinateur fixe ou portable, clé ou disque USB,...). (4.11) (CNRS 2013)
      - Circulaire J.M.Voltini du 16 janvier 2011 sur le chiffrement des disques pour les unités CNRS étendue en 2013 et rappel en 2019
        - Méthodologie :
          - Utilisation de disques chiffrants
          - Utilisation de chiffrement logiciel de disque ou création de container chiffré
        - Obligation de recouvrement
          - Une clé de déchiffrement doit être sauvegardée auprès d'un tiers

Protéger ses données en pratique

- Utiliser un chiffrement de surface pour les supports de données
  - Dmcrypt sous Linux (à mettre en œuvre lors de l'installation du système)
  - Filevault sur MacOS (il faut suffisamment d'espace disponible lors de l'activation)
  - Veracrypt (ou Bitlocker) sous Windows

    → activer aussi le chiffrement sur vos smartphones
- Stocker les données sensibles dans des containers chiffrés
  - Veracrypt (https://www.veracrypt.fr)
  - Zed (https://www.primx.eu/fr/zed-free/: version gratuite limitée)

Respect de la propriété intellectuelle

- sur les documents : images, textes, chansons
- sur des ressources : fontes
- sur les programmes : il existe des logiciels du domaine public, des sharewares, des logiciels commerciaux. Chacun a son modèle de pensée et son modèle économique. (6.1, 6.2)
- sur des bases de données (ex. : ressources bibliographiques) (6.3)

→ Télécharger plusieurs articles d'une revue dans un court laps de temps peut être interprété comme du pillage induisant une suspension de l'accès aux ressources bibliographiques

Téléchargement et P2P

- Des lois : Hadopi, Hadopi2,…
- Le trafic P2P (peer to peer)
  - Induit une forte consommation de bande passante
  - Est souvent associé à des échanges de contenu illégaux

    → circulaire Guyon de 2000 interdit le trafic P2P au sein de l'ENS
  - Exemples de programmes P2P : cacaoweb, *torrent,…
  - RAPPEL : la convention signée avec le réseau RENATER implique un usage professionnel !

Violation des droits

- Des sociétés sont mandatées par les majors pour rechercher les téléchargements illégaux et engager des actions

We are contacting you on behalf of The Cartoon Network, Inc.... Under penalty of perjury we assert that IP-Echelon Pty. Ltd. is authorized to act on behalf of The Cartoon Network, Inc., who is the copyright owner and/or owner of exclusive rights in such content identified below.
We have become aware that an individual has utilized the IP address 129.199.X.Y at the recorded date and time below to download, host, and/or facilitate the downloading and/or streaming of video content that is exclusively owned by The Cartoon Network, Inc.
...
As the owner of the IP address, we request that you immediately assist in removing and disabling access to the infringing material from your network.
...

Les codes malveillants…

- Une grande variété de formes possibles
  - Virus, vers, chevaux de Troie, spyware, ransomware, cryptolocker,…
  - Une grande variété de nuisances possibles
    - Vol d'informations, destruction de données, chantage,…
    - Prise de contrôle à distance,…
  - Une grande variété de cibles
    - Windows, MacOS, Linux et aussi les smartphones

Un faux message d'alerte...

Se protéger des malwares …

- Faire le nécessaire pour éviter l'introduction et la propagation de virus (4.9)

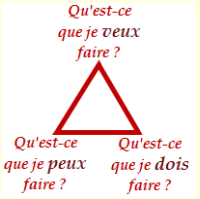
  → **Installer un antivirus et en mettre à jour régulièrement les règles.**

  → **Ne pas connecter de smartphones, tablettes,... sur un port USB d'un poste de travail "sensible" même pour le recharger.**

  → **Ne pas « surfer » depuis un équipement sensible.**

- Un outil de détection de trafic associé à des malwares
  - Des systèmes de détection d'intrusion sont en service en entrée des sites de l'ENS et du département de biologie.
    - **Tenir compte des alertes des RSSI ou CSSI que vous pouvez recevoir issues de ces systèmes**

L'éthique



- Dans ses échanges , nul ne peut s’exprimer au nom de l’École ou engager l’École sans y avoir été dûment autorisé. (9.1)
    - Utiliser l’adresse d’expéditeur adéquate pour vos mails (moi@ens.psl.eu est différent de moi@orange.fr)
- Chacun doit faire preuve de la plus grande correction à l’égard de ses interlocuteurs dans les échanges électroniques. (9.2)
- Compte tenu de la valeur juridique d’un courriel, chacun doit être vigilant sur le contenu des messages électroniques et s’assurer de leur conservation. (9.3)
- Il est rappelé que toute publication sur un site Internet hébergé dans l’École engage celle-ci. (9.5)
- L’usage à titre non professionnel d’une adresse de l’École (forums, blogs, ou toute autre publication sur Internet) doit être évité. (9.6)

- Les utilisateurs nomades se connectant en utilisant leurs identifiants « eduroam » ENS doivent respecter les règles imposées par le site d'accueil. (8.4)

Les attaques... (4., 8.)

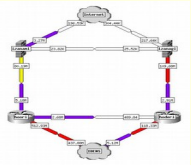
- Chacun est responsable de l'usage des ressources informatiques qu'il utilise
- N'utiliser que des ressources locales ou distantes autorisées (4.2, 8.1)
- Ne pas utiliser ou développer des programmes mettant sciemment en cause l'intégrité des SI. (4.3, 8.2)
- Signaler aux RSSIs/CSSIs en cas de découverte d'un tel programme (4.4)
- Ne pas exploiter les éventuels trous de sécurité, anomalies de fonctionnement, défauts de configuration (4.8)
- Prendre les mesures nécessaires pour ne pas introduire ou propager un virus (4.9)

L'usurpation d'identité

- Loi LOPPSI, du 14 mars 2011 :
  - Deux articles concernant l'usurpation d'identité numérique sont ajoutés à l'article 226-4 du code pénal,
    - «*Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende.* »
    - «*Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.* »
  - Dans la charte ENS
    - Les utilisateurs doivent s'abstenir de toute tentative de falsification d'identité. (4.6)

      → **Falsifier son adresse d'expéditeur d'un mail est une usurpation d'identité**

Les administrateurs



- Ils gèrent les machines et ont forcément des pouvoirs.
- Ils s’astreignent à confidentialité si la gestion, un besoin de sécurité nécessitent des investigations.
- Pour la sécurité, la métrologie, les systèmes génèrent des journaux nominatifs, ou indirectement nominatifs. (Accusé de réception CNIL 1118312).

Encore une fois, ce n'est pas de la fiction !

- Dernier avertissement CERT :
  - Septembre 2023.
- Dernier piratage :
  - Septembre 2023.
- Dernier vol de machine :
  - Juillet 2023.
- Dernier vol d'identifiants réussi :
  - Septembre 2023.
- Dernière réquisition judiciaire :
  - Février 2014.

Pour conclure, quelques règles…

- Ne pas oublier les règles de vie en société lors de l'usage d'un système d'information. Une information échappe vite à tout contrôle

  => les amis de mes amis sont ils mes amis ?

- Ne jamais communiquer ses identifiants à un tiers humain ou non
  - Attention au phishing (hameçonnage)
  - Utiliser des mots de passe résistants
  - Utiliser des moyens de communications sûrs (chiffrés!)
- Avoir un système d'exploitation et des logiciels mis à jour en terme de sécurité
- Installer un logiciel antivirus et mettre à jour régulièrement les signatures
- Chiffrer les données, notamment les données sensibles
- Avoir une sauvegarde récente de ses données
- Lire les contrats d'usage et licences des logiciels utilisés et vérifier qu'ils sont compatibles avec le besoin
- Privilégier l'usage des outils « professionnels » mis à votre disposition.
- Sécuriser physiquement ses équipements matériels (attacher son ordinateur,...)

En cas d’incident

→ Agir en fonction du type d'incident

- **Prendre des mesures d'urgence**
  - Isoler l'équipement du réseau
    - → sans arrêt de la machine sauf ransomware
  - changer les mots de passe
  - …
  - mais sans altérer pour analyse ultérieure
- **Alerter :**
  - prévenir les RSSIs (ou CSSI) si impact professionnel (matériel ou données)
    - → **tout vol doit être déclaré (4.13)**
  - prévenir les structures (banques, …)
  - …
  - dépôt de plainte notamment en cas de vol par le propriétaire