Pôle technologies et industrie

cifom CPLN

Prescription et normes de sécurité

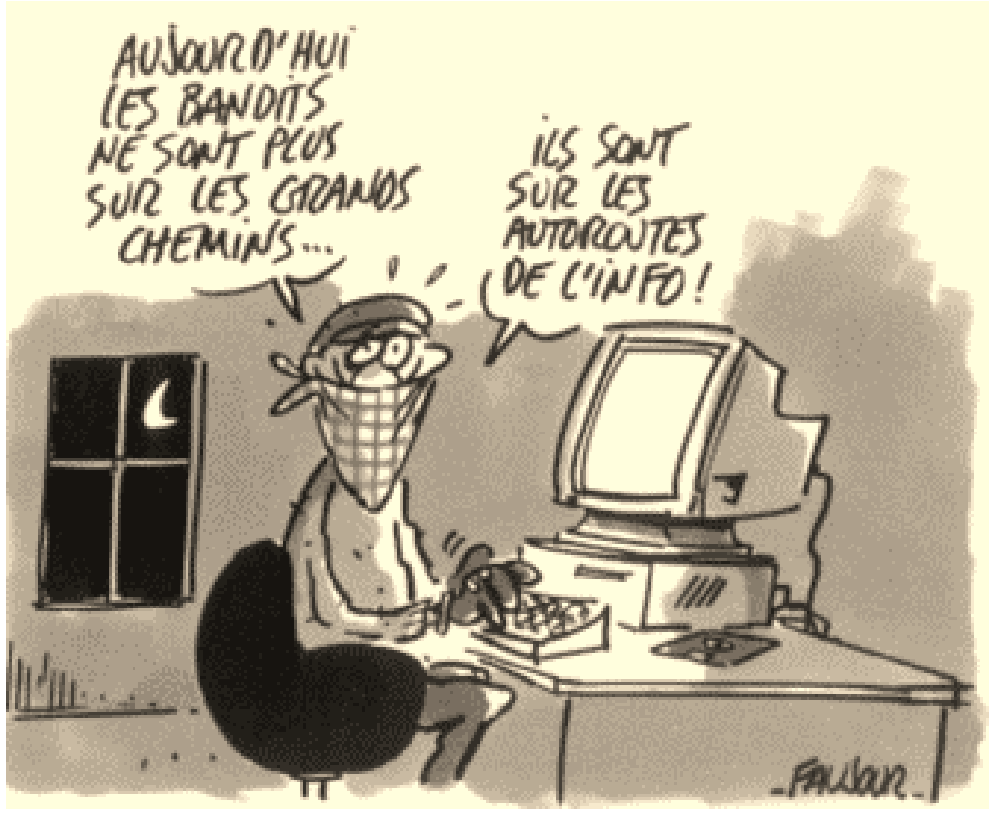
ICT-214 – Instruire les utilisateurs dans leur comportement avec des moyens informatiques

214_07_11_Th_Prescriptions_Normes_de_securite.pptx

JBL 06.04.2022 d'après MAG-MD

Objectifs :

- Expliquer aux utilisateurs les prescriptions et normes de sécurité dans le cadre d'un comportement responsable avec les informations dans un environnement de moyens informatique.



Importance et valeur de l'information

L'information constitue une part importante de la richesse d'une entreprise. Cela peut même constituer la richesse de l'entreprise :

- Banques → Clients et structures de leurs avoirs
- Industrie pharmaceutique → Formules des médicaments
- Etc…

L'enjeu de la sécurité des informations

Confidentialité

- *L'information n'est pas rendue disponible ni divulguée à des personnes, entités, ou des processus non autorisés.*

Intégrité

- *Exactitude et complétude (exhaustivité) de l'information.*

Disponibilité

- *L'information est accessible et utilisable à la demande par une entité autorisée.*

Traçabilité

- *Si les données sont altérées, possibilité de garder une trace de toutes les modifications à des fin d'analyse et de remédiation de la faille de sécurité*

Importance de l'image

- Toute atteinte aux données peut se traduire en perte de l'image de marque de la société si le problème est divulgué au dehors.

Conséquences légales, notion de responsabilité

- **L'entreprise a une responsabilité :**
  - vis-à-vis de ses clients, de la société (lois, droits d'auteurs), de ses employés (contrat de travail, respect de la sphère privée), de ses partenaires…
- **L'utilisateur a une responsabilité :**
  - qu'il soit employé de l'entreprise ou pas
- **Le service informatique a une responsabilité :**
  - vis-à-vis de l'entreprise (pérennité et protection des données, disponibilité du service selon les SLA), des utilisateurs, des ayant-droits, des partenaires, des fournisseurs (utilisation des services dans le cadre contractuel autorisé) …
- **Le hacker enfreint des lois et pourrait avoir à en répondre.**

La cybercriminalité: Phénomène en constante augmentation

- ***« Depuis 2004, le « chiffre d'affaire » de la cybercriminalité a dépassé celui du trafic de drogues illégales »***

  - Valérie McNiven, conseillère cybercriminalité, Trésor américain

- Il s'agit d'une vraie guerre !
- Pour bien conseiller les utilisateurs dans leur comportement, vous devez savoir comment procèdent les ennemis de l'entreprise.

  - ***« Connais ton ennemis et connais-toi toi-même »***

Profil des «ennemis»

- Aujourd'hui, les attaques sont de moins en moins menées par des pirates néophytes (*script kiddies*) et de plus en plus par des hackers aux connaissances avancées (*black hat ou white hat*).

- Les attaques sont aussi souvent internes :
- Employés mécontents,
- Espionnage,
- Résultat de l'incompétence.

- Votre entreprise doit clairement avoir dans ses objectifs de se protéger.

- Cela passe par une information et une formation des utilisateurs.

Pôle technologies et industrie

cifom

Les risques sur internet

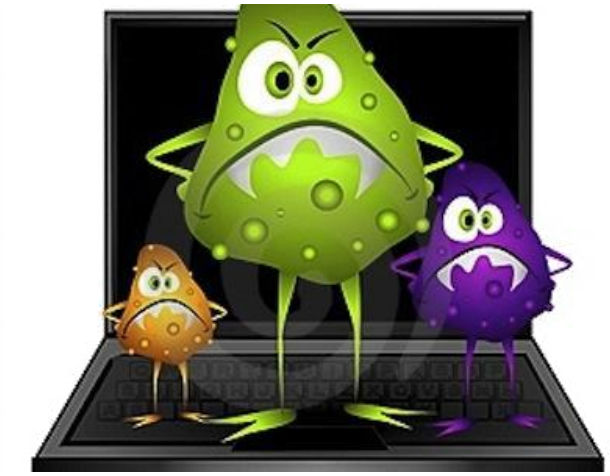
- Il est important de comprendre les risques de façon à mettre en place la protection adaptée et déterminer les comportements à conseiller à vos utilisateurs.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI

- Le site internet de MELANI s'adresse aux particuliers ainsi qu'aux PME en Suisse.

Les virus



- Ils se composent d'instructions programmées qui disent à l'ordinateur les actions à exécuter.

- Ils s'installent dans un "programme hôte" qui peut être une application (p. ex. un logiciel téléchargé) ou un document (p. ex. un fichier Word ou Excel).

Pôle technologies et industrie

cifom

Les virus

- **Conséquences et dangers :**
  - Modification et effacement des données
  - Changement affectant les contenus affichés à l'écran et apparition de messages inattendus.

- **Contre-mesures:**
  - Logiciels antivirus.
  - Faire preuve de prudence avec le courrier électronique.
  - Prendre ses précautions en naviguant sur internet.

Les vers (worms)

- Instructions programmées qui prescrivent à l'ordinateur les actions à exécuter.

- Ils utilisent les lacunes de sécurité ou des erreurs de configuration des systèmes d'exploitation ou des applications, pour se propager d'ordinateur à ordinateur.

Les vers (worms)

- **Conséquences et dangers :**
  - Accès non autorisé à l'ordinateur
  - Effacement de données
  - Espionnage de données confidentielles
  - Envoi de pourriels
- **Contre-mesures :**
  - Mises à jour des logiciels
  - Logiciels antivirus
  - Pare feu
  - Supprimer tout partage des espaces disques

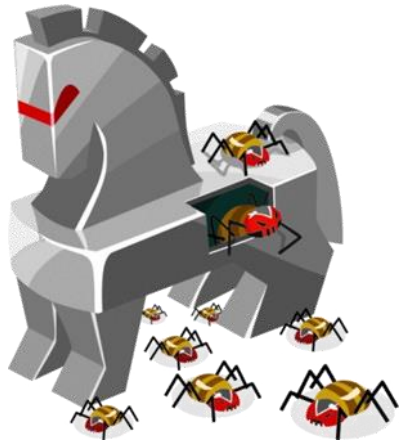
Les chevaux de Troie

- Programmes qui, de manière larvée, exécutent des action préjudiciables tout en se présentant à l'utilisateur comme des applications ou des fichiers utiles.
- Se présentent sous différentes formes :

❑ Programmes téléchargés sur Internet

❑ Fichiers musicaux ou vidéos (MP3, MPEG)

❑ Fichiers attachés au courriels



Les chevaux de Troie

- **Conséquences et dangers :**
  - Accès illicites aux données confidentielles
  - Accès non autorisé à l'ordinateur
  - Envoi de pourriels depuis votre ordinateur

- **Contre-mesures :**
  - Logiciels antivirus
  - Pare-feu
  - Faire preuve de prudence avec le courrier électronique
  - Prendre ses précautions en naviguant sur l'internet

Les logiciels espions et publicitaires (spyware, adware)

- Les logiciels espions collectent des informations à l'insu de l'utilisateur, sur :

❑ Ses habitudes en matière de navigation (surf)

❑ Les paramètres du système utilisé

Les logiciels espions et publicitaires (spyware, adware)

- **Conséquences et dangers:**
  - ❑ Espionnage de données confidentielles (p. ex. des mots de passe)
  - ❑ Mise en danger des données privées
  - ❑ Publicité non sollicitée
- **Contre-mesures:**
  - ❑ Pare-feu
  - ❑ Faire preuve de prudence avec le courrier électronique
  - ❑ Prendre des précautions en naviguant sur l'Internet

Le social Engineering (subversion psychologique)

- Est aussi connu sous le nom de « manipulation sociale ».

- Ce type d'attaque permet d'accéder à des données confidentielles ou conduire la victime à exécuter certaines actions spécifiques en exploitant :

- La serviabilité de l'utilisateur
- La bonne foi de l'utilisateur
- L'insécurité de l'utilisateur

Le social engineering (subversion psychologique)

- **Conséquences et dangers :**
  - Divulgation d'informations confidentielles
  - Escroquerie
  - Diffusion de virus et de chevaux de Troie
- **Contre-mesures :**
  - Attention en transmettant des informations
    Ne transmettez pas, même par téléphone, des informations confidentielles (p. ex. nom d'utilisateur, mot de passe, etc. Un fournisseur de services sérieux ne vous demandera jamais votre mot de passe.

Hameçonnage (Phishing)

- Fait appel à la bonne foi, la crédulité ou la serviabilité de leur victime en leur envoyant des courriels avec des adresses d'expéditeurs falsifiées.
- Ces courriels signalent p. ex. à la victime que les informations concernant son compte et ses données d'accès (p. ex. nom d'utilisateur et mot de passe) ne sont plus d'actualités ou ne sont plus sécurisées, les invitant à les modifier à l'aide d'un lien indiqué dans le courriel.

Hameçonnage (Phishing)

- **Conséquence et dangers :**

- Grâce aux données acquises frauduleusement, l'escroc peut effectuer des transactions bancaire au nom de l'utilisateur, la victime, ou placer des offres dans les enchères en ligne.

- **Contre-mesures :**

- Ne jamais cliquer sur des liens figurant dans des messages électroniques ou des sites censés donner accès au site recherché
- On évitera absolument d'ouvrir d'autres sites Internet en cours de session e-banking.

Les lacunes de sécurité

- Les programmes sont composés d'instructions qui indiquent à l'ordinateur les actions à exécuter.

- **Conséquences et dangers :**

- Les erreurs de programmation, au niveau de la sécurité, peuvent permettre d'accéder de manière non autorisée aux données et aux systèmes. Ce sont ces erreurs que l'on appelle lacunes de sécurité ou vulnérabilités.

Les lacunes de sécurité

- Contre-mesures :
- Mises à jour fréquentes des programmes
- Stratégie à deux navigateurs et autres possibilités

Les canulars (Hoax)

- Se présentent sous forme de courriels annonçant de nouveaux virus.
- Presque toujours de fausses annonces (canulars ou hoax).
- Les canulars sont toujours conçus sur le même modèle. Ils signalent l'apparition d'un nouveau virus dangereux résistant même à un logiciel anti-virus récent.

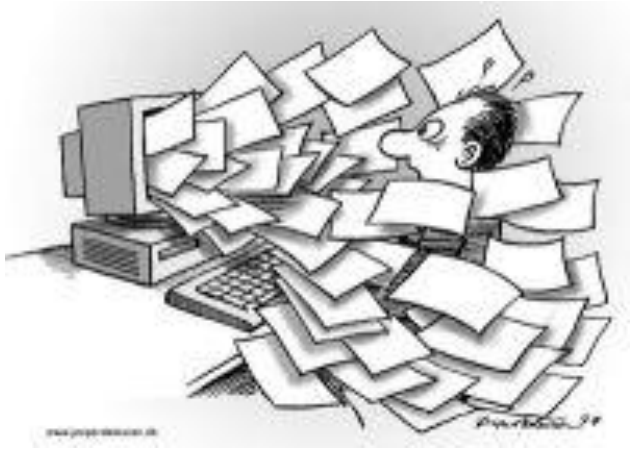
Exemple de canular

Les canulars (Hoax)

- **Conséquences et dangers :**
  - Suivre les mesures proposées dans le canular peut entraîner la perte de données ou la mise hors usage de l'ordinateur.
  - Panique potentielle et trafic de données inutile
  - Surcharge de l'infrastructure nécessaire aux courriels

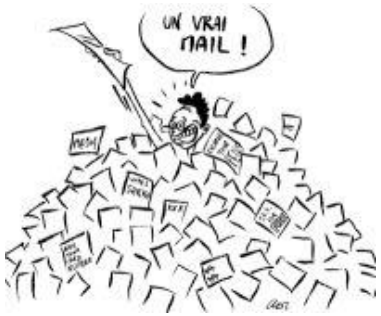
- **Contre-mesures :**
  - Ne pas exécuter les instructions du courriel
  - Consulter d'autres sources
  - Aviser l'expéditeur qu'il s'agit d'un canular

Les pourriels (spam)



- La notion de pourriel (spam) englobe tous les messages électroniques indésirables et les chaînes de courriels.
- La personne qui envoie de tels messages est appelée polluposteur (**spammer**), tandis que l'on parle de pollupostage (**spamming**) pour l'action proprement dite.
- Selon plusieurs études, les pourriels représenteraient déjà plus de **60 %** du courrier électronique au plan mondial et la tendance est à la hausse.

Les pourriels (spam)



- **Conséquences et dangers :**
  - Perte de temps
  - Très grosse charge pour l'infrastructure IT de l'entreprise
- **Contre-mesures :**
  - Faire preuve de prudence avec le courrier électronique
  - Pas d'adresses électronique courte
  - Filtres proposés par les programmes de messagerie
  - Filtre anti-pourriel
  - Utilisation des copies aveugles lors de l'envoi d'e-mail à plusieurs destinataires

Les cookies

- Petits fichiers texte qui s'installent sur l'ordinateur du visiteur lorsque ce dernier consulte une page Internet (témoins de connexion) , dans le but de lui simplifier la tâche.

- Exemple : il faut parfois dans certains services en ligne s'annoncer à l'aide d'un nom d'utilisateur et du mot de passe correspondant.

Les cookies

- **Conséquences et danger :**

❑ Mise en danger de la sphère privée. Lors d'une connexion, enregistrement du comportement du visiteur du site. Etablissement du profil client.

- **Contre-mesures :**

❑ Restriction des témoins de connexion. Paramétrage du navigateur.

❑ Acceptation de témoins de connexion uniquement pour des site spécifiés.

❑ Recours à des outils qui effacent les témoins de connexion.

Le chat et messagerie instantanée

- Le « chat » désigne un moyen de communiquer sur Internet en temps réel avec d'autres utilisateurs.

- Les discussion se font non en parlant mais en écrivant.

Le chat et messagerie instantar

- **Conséquences et danger :**
  - ❑ Préserve l'anonymat pour agir de manière illégale (p.ex. pédophilie).
  - ❑ Introduction de virus ou de vers sur votre ordinateur.
  - ❑ Risque de cliquer sur un lien ou à entrer des commandes inconnues.
- **Contre-mesures :**
  - ❑ Mises à jour des programmes.
  - ❑ Suppression des partages des espaces disques.
  - ❑ Précautions à prendre en « chattant ».

Wireless LAN

- Un WLAN (Wireless Local Area Network) est un réseau local sans fil.
- Dans un tel réseau, les ordinateurs portables, agendas électroniques (PDA), communiquent sans fil avec un point d'accès WLAN, relié à Internet ou à un réseau local.

Wireless LAN

- **Conséquences et danger :**
  - Peur entraîner un accès au réseau local si la configuration est irréfléchie.
  - Un cryptage insuffisantes connexions WLAN permet à des tiers de lire des données.
- **Contre-mesure :**
  - Protection de la page administration
  - Bloquer l'envoi de l'identification du réseau
  - Restriction d'accès aux terminaux
  - Enclencher le cryptage
  - Recours à des protocoles sûrs

Bluetooth, Handy, PDA

- Autrefois, le téléphone portable ne servait qu'à téléphoner.
- Aujourd'hui il s'est mué en appareil multifonction, véritable assistant numérique.
- Tous ces appareils ont une fonction Bluetooth

Bluetooth, Handy, PDA

- **Conséquences et danger :**

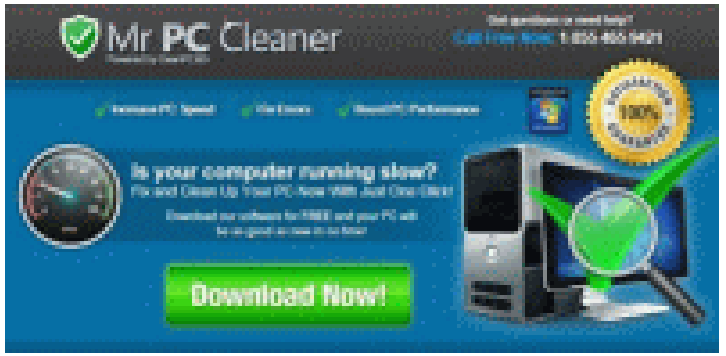
- Possibilité de lecture non autorisée de l'agenda, du carnet d'adresse, voire des message SMS enregistrés.
- Possibilité d'activation cachée d'appels ou envoi de SMS.
- Risque de propagation de vers affectant le bon fonctionnement du portable.

Bluetooth, Handy, PDA

- **Contre-mesures**

- N’activez le Bluetooth qu’en cas de besoin.
- Recours au Bluetooth uniquement dans un contexte sécurisé.
- Mode « discoverable » de l’appareil Bluetooth activé uniquement si nécessaire.
- Utiliser les options de sécurité.

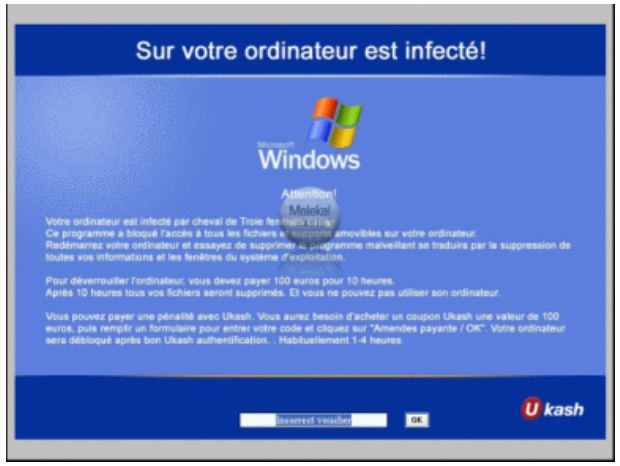
Les rogues



- Les rogues sont de faux logiciels de sécurité.
- Exemple : Le rogue Security Tool
- Faux logiciel anti-spyware.
- S'installe sans permission et vous incite à un logiciel "frauduleux" pour soit disant désinfecter votre ordinateur.

- A ne pas faire !

Les RamsonWare



- Logiciel qui prend en otage des données personnelles.
- Pour ce faire, il chiffre des données personnelles puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de de les déchiffrer.

Le Spear phishing

- Variante plus subtile du phishing.
- Vise une ou quelques cibles pour exfiltrer des données sensibles.
- Le but est de collecter des informations afin de personnaliser un email comportant une pièce jointe avec un extension trompeuse ou un lien.

Le Spear phishing

http://halls-of-valhalla.org/beta/news/research-to-prevent-spear-phishing-attacks,113/

- **Contre-mesures :**

- ❑ S’assurer de la fiabilité de l’expéditeur.
- ❑ Ne pas cliquer sur des pièces jointes ou des liens avant d’être convaincu de l’authenticité de l’expéditeur.
- ❑ S’assurer de la pertinence de la destination des hyperliens.
- ❑ Vérifier l’intitulé parfois trompeur des liens affichés.
- ❑ Ne jamais communiquer de données sensibles sur des sites.