Séminaire annuel
Commission informatique

FÉDÉRATION FRANÇAISE
NATATION

Toulouse
30 sept. / 2 oct. 2016

Sommaire

La sécurité informatique

2ème partie

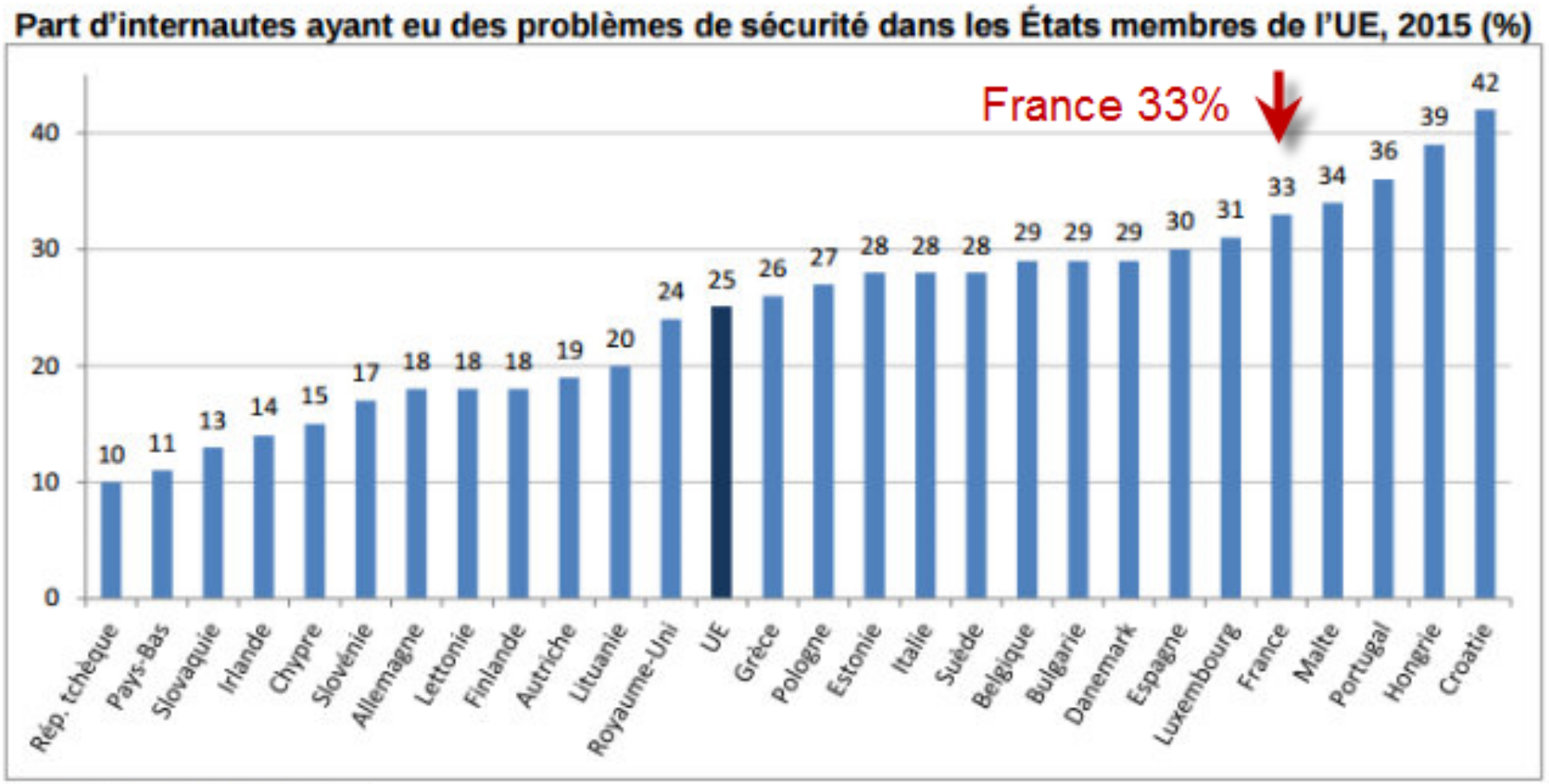
Bilan, tendances et enjeux de la sécurité informatique

Le constat

En 2015, le nombre d'incidents en Cybersécurité dans le monde a augmenté de 38 %, +51 % en France selon l'étude "The Global State of Information Security Survey 2016" réalisée par PWC. Cette année des exemples éloquents ont émaillé l'actualité, symptômes d'une escalade de l'ampleur des risques auxquels sont exposés des pans entiers de notre activité au quotidien.

Autre problème: L'infrastructure HARDWARE du réseau Internet se fragilise et a de plus en plus de difficultés à absorber le flux et le volume des données échangées.

Le constat



Roumanie: donnée non disponible.
Les données sources sont consultables ici.

Source: Le Figaro 8/02/2016

La cybercriminalité en 2016

- Trois catégories

1) Les atteintes directes à des systèmes informatiques en perturbant leur fonctionnement, tels que les attaques par déni de services (DDoS), destinées à faire tomber, par saturation, un serveur à distance.

2) Réaliser des actes illicites en utilisant les outils numériques (escroqueries, vols de données bancaires ou personnelles, espionnage industriel, atteinte à la propriété intellectuelle, sabotage, accès frauduleux, fraudes, usurpation d'identité, phishing, création de PC zombies, contamination d'autres postes informatiques ou d'autres serveurs, exploitation de failles…)

3) Modifier le contenu d'un espace numérique pour y déposer ou diffuser des contenus illicites (pédopornographie, racisme, xénophobie, fanatisme).

Quelques différences !

- Un hacker (bidouilleur, fouineur)

• Personne qui, par jeu, goût du défi ou souci de notoriété, cherche à contourner les protections d'un logiciel, à s'introduire frauduleusement dans un système ou un réseau informatique et à découvrir les failles.

*'**Crackers** "* sont un genre de hackers spécialisés dans le contournement des protections anticopies des logiciels.

*"**Phreakers** "*, ce sont également des hackers, spécialistes, eux, de la téléphonie. Ils inventent des systèmes qui permettent de téléphoner gratuitement ou de modifier le contenu des téléphones mobiles ..

- Un pirate informatique (casseur)

• Personne qui contourne à des fins **malveillantes** ou même détruit les protections d'un logiciel, d'un ordinateur ou d'un réseau informatique.

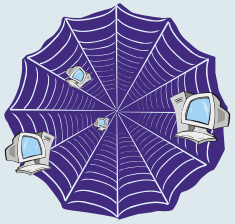
Les 2 sont des génies de l'informatique, et lorsqu'ils ne changent pas de catégorie, l'un bidouille pour progresser, l'autre pour casser.

Constatation et craintes au niveau mondial

Deux questions se posent:

1 - Le réseau INTERNET fera t-il, dans un proche délai, l'objet d'une gigantesque attaque permettant de le neutraliser ?

Aujourd'hui, les conditions techniques peuvent être rassemblées pour effectuer ce type d'action.

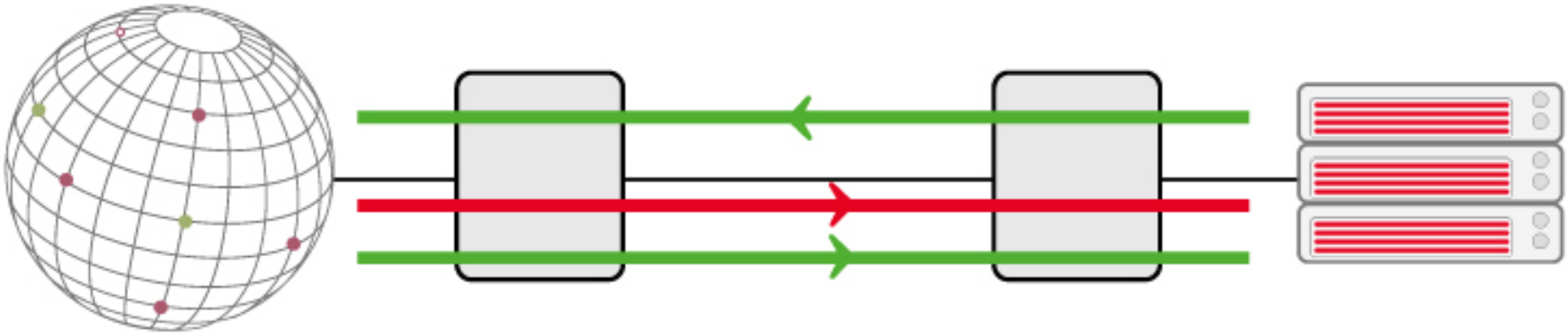


2 - L'infrastructure en place du réseau INTERNET résistera-elle longtemps au flux toujours plus important des données le parcourant (vidéo, TV, web, blogs, Téléphones IP, messagerie, etc…)?

Aujourd'hui, l'accroissement des données est compensé par l'évolution des techniques de compression de données, mais jusqu'à quand?

N°1 des attaques en 2016 : les attaques DDoS

- DDoS:= attaque par déni de services
- L'attaque DDOS cible en priorité les entreprises et les grandes organisations.

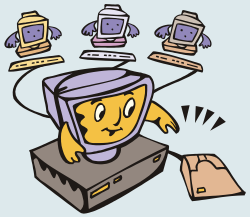


Les chances d'être confronté à une attaque DDoS sont importantes et les tentatives nombreuses.

Une attaque DDoS vise à rendre un serveur, un service ou une infrastructure indisponibles en surchargeant la bande passante du serveur, ou en accaparant ses ressources jusqu'à épuisement.

Lors d'une attaque DDoS, une multitude de requêtes sont envoyées simultanément, depuis de multiples points du Net. L'intensité de ce "tir croisé" rend le service instable, ou pire, indisponible.

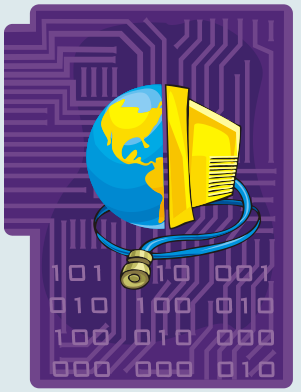
La tendance : Évolution du ‘Piratage’’



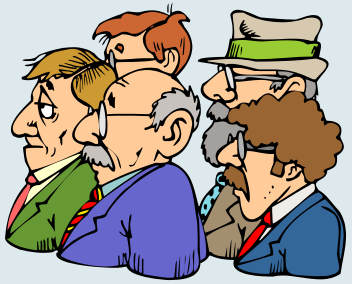
- Les attaques sont de plus en plus sophistiquées, elles s’appuient souvent sur un réseau de machines, elles sont dirigées, elles mettent en place un ensemble de modules distincts, (virus backdoor) pour accéder à la machine, (virus rootkit) pour s’approprier le cœur de la machine en silence, ensuite mise en place du virus final (distribution de spyware, vol de ressources, PC ZOMBI, stockage illicite, etc…). La combinaison de ces multiples techniques rend difficile la neutralisation et l’éradication complète de ces attaques.
- L’évolution montre également une tendance au regroupement des ‘hackers’ en communauté organisée (Expl: Anonymous’) avec une tendance d’infiltration visant les gouvernements et les milieux politiques.

- Autre tendance: Le piratage ‘hardware’ (modification, déverrouillage, desimlocage de matériels, etc..), semble en recul par rapport au piratage ‘Software’ (modification de logiciels)

.



La tendance : Évolution des cibles



Les Blogs et Réseaux sociaux

• L'évolution du web à permis progressivement aux internautes de ,s'approprier Internet, de participer à la mise à jour des informations et de partager de plus en plus de données numériques à caractère privée (photos, vidéo, etc..) au travers de blogs personnels, de réseaux sociaux (Facebook, Instagram, Twitter) ou de points centraux de diffusion (YouTube, Dailymotion).

•Tous les réseaux sociaux fonctionnent sur le même principe,: on crée son profil (infos personnelles, photos, centres d'intérêt), on donne son avis, on se dévoile et l'on invite ses <<amis>> à nous rejoindre.

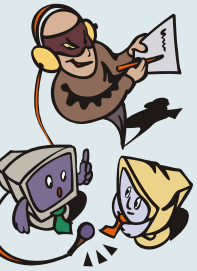
• Tout se partage: vidéos, sons, photos, diaporama, CV, savoir, potins, sentiments, etc.

Problème: Cela en fait des cibles attrayantes pour organiser la fuite d'informations privées, exploitées en arrière plan à des fins commerciales ou frauduleuses

La tendance : La boucle infernale

La tendance : Évolution des cibles (suite)

Les Blogs : Une belle cible



- **Les blogs personnels ont remplacés les sites personnels**
  - Pour créer un site personnel, il fallait un minimum de connaissance en programmation HTML, le site était figé, c'était l'équivalent d'une publication dans un magazine (Web 1.0)
  - L'arrivée des langages PHP et Flash ont permis de développer des sites modèles interactifs et personnalisables, les BLOGS (Web 2.0)
  - Dynamiques, interactifs, très faciles à mettre en œuvre ces sites de nouvelle génération permettent d'avoir un retour et des avis sur les thèmes abordés et d'entamer un dialogue avec les visiteurs du blog.
  - Les évolutions web 3.0, 4.0 et 5.0 ont permis de faciliter les échanges et d'introduire des 'assistants personnels' afin que le stockage et le partage d'infos sur Internet soient facilités (cloud)

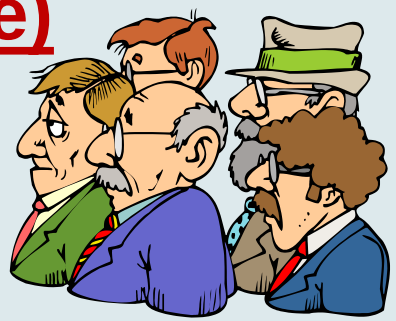
Problèmes liés à cette nouvelle tendance:

La facilité d'utilisation et de mise en ligne d'informations ont banalisé et dégradé la qualité des informations disponibles. On trouve de tout et l'on peut donner son avis sur n'importe quoi.

Attention : Les blogs servent souvent de refuge aux enfants qui traversent une crise d'adolescence. Se sentant incompris, ils trouvent par ce biais le moyen de s'exprimer librement et de refaire le monde à leur image.

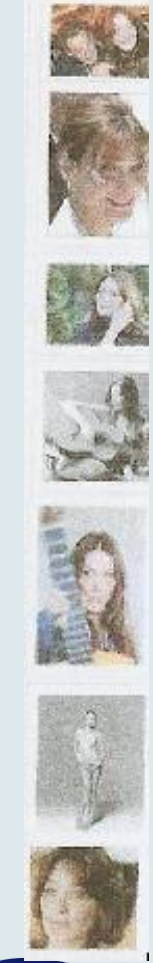
Attention au dérapage (diffamation, suicide, actes répréhensibles, etc…)

La tendance : Évolution des cibles (suite)



Les réseaux sociaux:

Une mine de renseignements personnels



•**Risque pour l'individu** : **l'e-réputation.**

•ATTENTION: Les amis d'aujourd'hui ne seront pas forcément ceux de demain. (expl: affaire Manaudou,) .

•**Risque pour l'individu : Mauvaises rencontres**

•Les adolescents se dévoilent trop sur les sites communautaires. On ne sait pas qui se cache derrière un pseudo (pédophilie, détournement de mineur, etc..)

•**Risque pour l'individu : Usurpation d'identité**

•Lorsque vous aurez tout dit de votre vie privée, il sera facile a un <<ami>> de se faire passer pour vous et de commettre des méfaits sur le Net en votre nom.

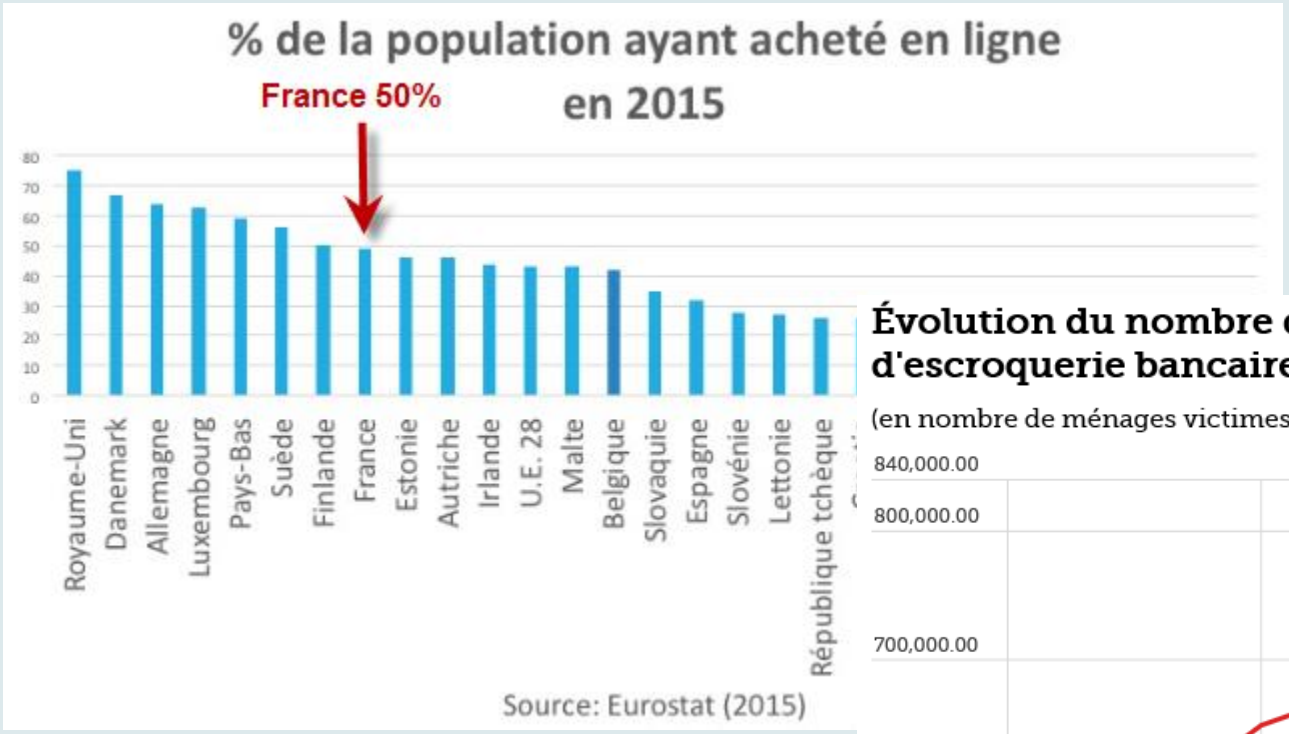
•**Risques pour l'individu et l'entreprise**: : diffusion involontaire de données sensibles, atteinte à la réputation, contre publicité.

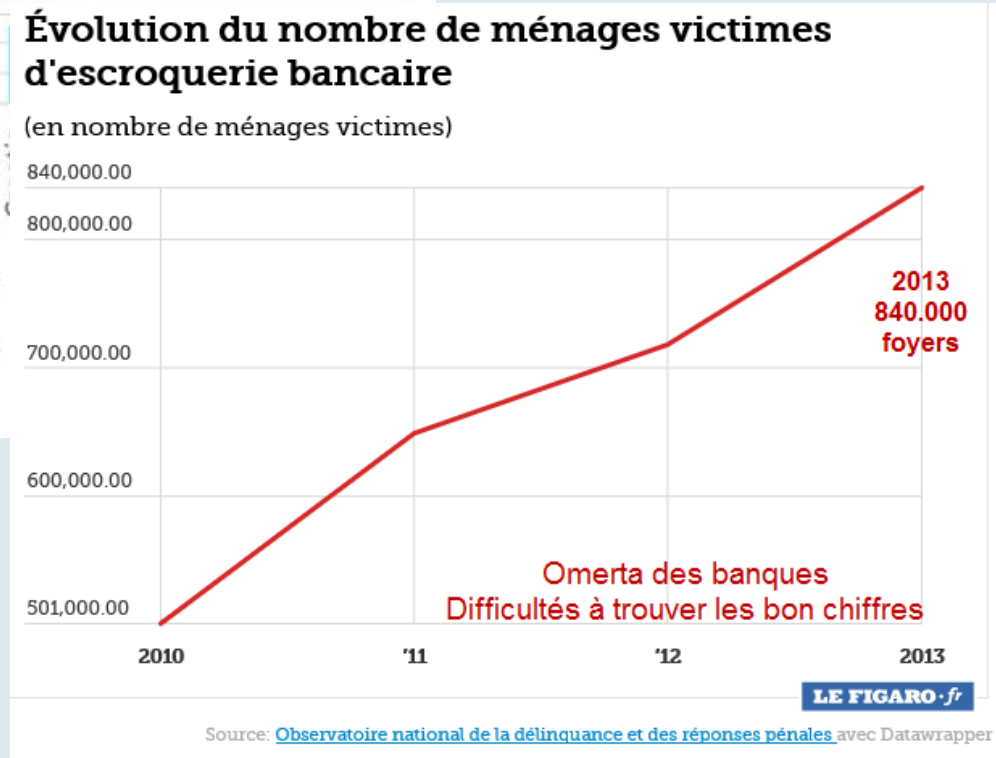
Problème lié à cette nouvelle tendance:

La <sphère privée> de chaque individu s'amenuise de jour en jour . D'autres individus s'expriment à notre sujet ou diffusent nos photos. Une fois diffusée, l'information devient indélébile. .

La tendance : Évolution des cibles (suite)

Le commerce en ligne





Arnaques bancaires :
Comment procèdent les escrocs

- **Vendeur malhonnête**
- **Logiciels espions**
- **Mails trompeurs**

Autres tendances : Les nouveaux risques

- Les smartphones

Attention: de plus en plus de données sont échangées via les smartphones. Ignorer au départ par les hackers les smartphones deviennent progressivement un terrain de jeu pour les nouveaux virus qui exploitent les failles de sécurité d'Android et des iphone.

- Plusieurs antivirus payants ou gratuits sont disponibles (clean master, Psafe, 360 security, etc...).
- Importance des mots de passe sur les Smartphones

- Le cloud

- Évitez de stocker des informations personnels sur les volumes en ligne. Ils font l'objet d'attaque répétées.

- Les montres connectées

- Les véhicules modernes

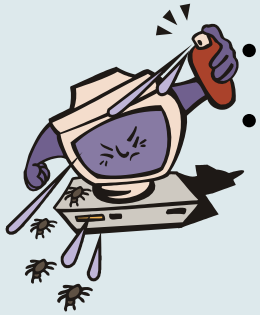
Autres tendances :

- **La contrefaçon d'antivirus**
- Cibles : les internautes privés
- Technique: Inciter les visiteurs à cliquer par des messages alarmistes . L'utilisateur teste. L'utilisateur achète. L'utilisateur est débité plusieurs fois du montant de l'achat. L'utilisateur a infecté sa machine.

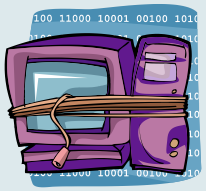
- **Les fausses loteries**
- Cibles : les internautes privés
- Technique: Avertir les internautes qu'ils ont gagné. Les inciter à cliquer sur le message pour récupérer leurs gains. Évidemment, il faut payer pour recevoir les gains.

- **La vente de services criminels en ligne**
- Cibles : les entreprises
- Offre: proposition d'éradication de la concurrence.

Autres tendances (suite) :



- **Le recel à l'insu de son plein gré**
- Cibles : Toutes machines sur le net
- Technique: exploitation des failles techniques des hébergeurs pour s'approprier des ressources appartenant à quelqu'un d'autre pour stocker des contenues illicites à son insu (les stros) ou pour utiliser la machine comme relais de nuisance (ZOMBI) ou de puissance additionnelle.
- Conséquences: risque pour l'individu de détenir des contenus illicites (photos, musique). Problème d'image. Machine encombrée, perte de puissance.



- **L'exploitation des failles logiciels:**
- Cibles : les logiciels les plus utilisés, les logiciels utilitaires standards
- Technique: Exploiter au maximum les failles de sécurité des logiciels courants entre la période de découverte de la faille et la mise à jour corrective.

Les enjeux de la sécurité informatique

Pour la fédération

- Préserver son fonctionnement en réduisant au maximum les indisponibilités de son système d'information.
- Éviter la divulgation ou la perte de données.
- Authentifier les utilisateurs et rester maître du système en suivant les comportements.
- Mettre en œuvre les moyens techniques de sécurisation des données et des matériels.
- Conserver sa e-réputation

Pour les clubs et les comités

- Participer à la sécurisation des données proposées en adoptant un comportement responsable et en respectant les procédures.
- Prévenir la divulgation des clés d'accès aux données FFN.
- Mettre en œuvre les moyens techniques de sécurisation de leur matériel et de leurs logiciels.

Les risques de contamination

Rappel des principales nuisances potentielles!

- **Les risques liés a consultation Internet et/ou aux téléchargements**
  - Les virus
  - Les cookies
  - Le détournement de contenu (vulnérabilité des enfants)

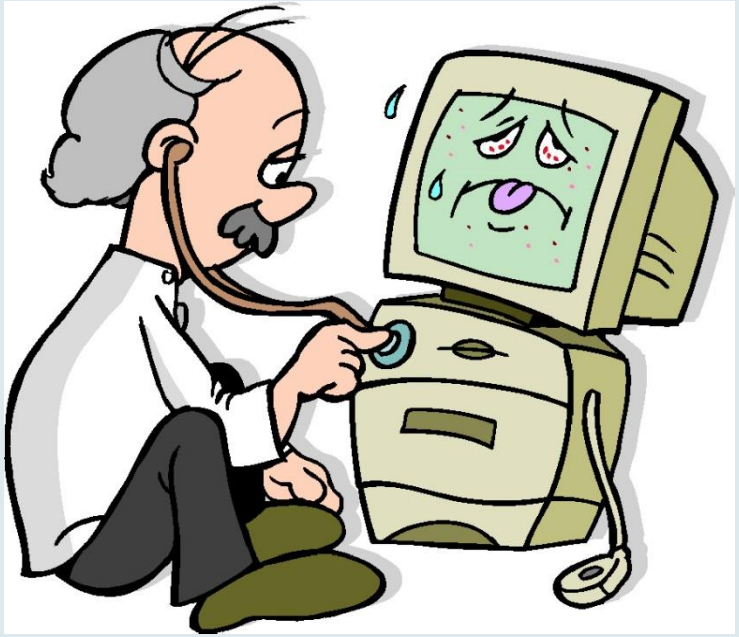
- **Les risques liés à l'utilisation de la messagerie**
  - Les virus
  - Le spamming
  - Le phishing
  - Les hoax
  - Le mail bombing

- **Les risques liés aux blogs et réseaux sociaux**
  - La fuite d'informations personnelles et la perte de confidentialité
  - L'usurpation d'identité

Les nuisances potentielles (Malware)

Les virus : les .....ware

Malware, Spyware, Cryptoware, Adware, Ransomware, Crapware, Scareware



Humour

Les belges ont ajouté:

Un mouchware : logiciel antivirus

Un entoware : logiciel de compression de données

Un tireware : logiciel de classement

Un mirware : logiciel de copie

Un abreuware: logiciel réseau

Un depotware : poubelle Windows

Et bien d'autres.....

http://slideplayer.fr/slide/1709450/

Les nuisances potentielles (Malware)

Les virus

- **Définition:** Tout programme d'ordinateur capable d'infecter un autre programme d'ordinateur en le modifiant de façon à ce qu'il puisse à son tour se reproduire.

- **Fonctionnement:** morceau de programme dans un programme standard. Exécution -> Activation -> Infection

- **De quoi sont capables les virus:**
- Ralentir la messagerie (Sobig)
- Subtiliser des données confidentielles (keylogger : BugDear-D)
- Utiliser votre ordinateur pour attaquer un site web (MyDoom)
- Corrompre des données (virus macro Excel)
- Effacer des données (Sircam)
- Désactiver des matériels et périphériques (Chernobyl -> écrase la bios)
- Faire des farces (Netsky-D -> émet un son pendant 4 heures)
- Afficher un message: (Cone-F -> message politique)
- Mettre dans l'embarras (Polypost -> place vos fichiers et nom sur forum X)

Les nuisances potentielles (Malware)

Les virus (suite)

- **Les différents types de virus:**
- **Les virus mutants:** ils sont réécrits régulièrement par leurs auteurs pour dérouter les antivirus.
- **Les virus polymorphes:** ils sont programmés pour changer leur apparence.
- .**Les macros-virus :** ils s'attaquent aux macros VBA en priorité, trouvent de bonnes cachettes dans les applications de Microsoft Office.
- **Les rétrovirus :** ils s'attaquent aux antivirus et modifient leur signature.
- **Les virus de boot et de démarrage :** S'attaquent au secteur de démarrage du disque dur, en diminution.
- **Les bombes logiques:** s'activent à un moment précis. Elles sont activées par la date système ou un appel système. (date anniversaire, etc...)
- **Les vers:** s'auto-reproduisent; se déplacent à travers le réseau. Les vers actuels se servent de la messagerie pour se déplacer à l'aide de scripts (VB script ou des fichiers exécutables)

Les nuisances potentielles (Malware)

Les Chevaux de Troie

- **Définition:** un programme caché dans un autre qui exécute des commandes, généralement pour donner accès à la machine sur laquelle il est installé en ouvrant un port de communication. (backdoor)
- **But:** Voler des mots de passe, copier des données sensibles ou exécuter tout autre action nuisible.
-

Les nuisances potentielles (Malware)

Spyware (logiciel espion)

Définition: Logiciel analysant le comportement d'un utilisateur, pas forcément illégal

But: Renvoie des infos à son expéditeur:

-traçabilité des URL des sites visités;
-traque les mots clés saisis dans les moteurs de recherche
-analyse des achats réalisés sur internet
-essai de captation des données personnelles et bancaires

– Principales catégories de Spywares

- Le Keylogger: Spyware espionnant la frappe au clavier (interception mot de passe, code bancaire, etc…)

- L' Adware: logiciel espion souvent cachés dans des publicités ou les services des réseaux sociaux, observe le comportement de l'utilisateur (site visités, intérêts, etc..) et envoie les informations soit pour alimenter des bases de données commerciales, soit pour afficher en retour des publicités ciblées. Génère des revenus publicitaire à son éditeur.

Les nuisances potentielles (Malware)

Ransomware (Très présent en France depuis Mars 2016)

Un ransomware (rançon)
- C' est un logiciel qui va crypter vos fichiers et vous demander de l'argent (une rançon) pour que vous puissiez les décrypter.
Ce type de malware est particulièrement nocif car lorsqu'il s'attaque à un ordinateur, il crypte l'ensemble des documents qui lui sont accessibles en local, comme sur le réseau.

Peu d'entreprises acceptent de payer la rançon réclamée en 'Bitcoins', préférant repartir d'une sauvegarde des documents.

Bitcoin est une technologie P2P fonctionnant sans autorité centrale. Bitcoin est *libre et ouvert*. Force est de constater que la clé attachée à l'achat de bitcoins fonctionne et déchiffre effectivement les données cryptée.

Les nuisances potentielles (Malware)

Rootkit (les virus qui rendent fou les anti-virus)

Rootkit :Programme parasite se logeant dans le noyau du système, se rend invisible au système d'exploitation et peut rendre invisible d'autres nuisibles (spyware , backdoor). Très difficile à démasquer et à éradiquer car il utilise la même technique que les antivirus.

Technique du rootkit: Installer au niveau du noyau du système, avant le démarrage de l'antivirus un ensemble de 4 modules regroupant un process, un drivers, une librairie et un programme exécutable. Chacun des éléments pouvant à lui seul régénérer et relancer les trois autres. Seule, l'éradication complète des 4 modules supprime le rootkit.

Afin de diffuser une infection sur une plus grande échelle, la tendance est de constituer un réseau de PC infectés par des **rootkits** qui servira de plate-forme de diffusion à grande échelle. Ces regroupements sont appelés **'BOTNET'**

Les **rootkits** sont difficilement détectables aux antivirus, ils constituent une menace de plus en plus importante face aux techniques actuelles d'éradication.

Les nuisances potentielles (cookies)

Les cookies

- **Définition:** Un **cookie** est un petit fichier texte au format alphanumérique déposé sur le disque dur de l'internaute par le serveur du site visité ou par un serveur tiers (régie publicitaire, service de web analytique, etc.) On considère généralement qu'un **cookie** permet de reconnaitre un visiteur lorsqu'il revient sur un site web.
- Conçus pour faciliter la navigation sur le site visité, ils peuvent néanmoins être potentiellement nuisibles.
  Exemple: Datr de Facebook qui piste tous les internautes non inscrit sur Facebook.

Il est nécessaire de les purger régulièrement

Les nuisances potentielles

La vulnérabilité des enfants sur internet

Autres nuisances

- Vos enfants sont une cible sur Internet. Ils peuvent être victimes de détournements de contenu en recherchant sur le net et de racolage d'informations à caractère privé en particuliers sur les réseaux sociaux..

- Un conseil: Même avec le meilleur des logiciels de contrôle parental, ne laisser pas vos enfants en bas âge, vos petits enfants, seuls face à Internet, à la messagerie ou aux réseaux sociaux. Ils tomberont indéniablement sur des images obscènes, des incitations commerciales ou autres non sollicitées.

ATTENTION: De très nombreux sites très connus pour les enfants (dessins animés, BD, coloriages etc..) sont ciblés pour être détournés de leur vocation d'origine. Expl: Mickey, les Simpsons, etc...

Les chiffres de la messagerie en 2016

Nombre d'utilisateurs: Monde=**2,672** milliards (prévisions: **3** milliards en 2020)

Nombre de comptes e-mail: Monde **4,4** milliards, France: **68** millions en mars 2015

En France les internautes ont en moyenne 2,1 adresses e-mail

Nombre d'email envoyés chaque jour (hors spam):

Monde: **215 milliards** France: **1,4 milliards**

Un internaute français reçoit en moyenne 39 e-mails par jour

Les principales messagerie:

Gmail: **1 milliard** d'utilisateur (janvier 2016)

Outlook.com, Hotmail: **400 millions** (avril 2015)

Yahoo : **225 millions** d'utilisateurs (oct 2015)

Moyens de consultation des mails (mars 2015)

Le mobile: **48%**

Le Webmail: **30%**

Le logiciel de messagerie **22%**

(sources: Étude SNDC-EMA B2C 2015)

Les risques liés à l'usage de la messagerie

Les risques liés à l'usage de la messagerie (suite)

- Le phishing (hameçonnage)
- C'est une technique utilisée par des escrocs pour obtenir des informations personnelles.
- Le phishing n'est pas une méthode basée sur une faille informatique, mais sur la naïveté des internautes.
- Les escrocs se font souvent passer pour un organisme de confiance 'spoofing' (organisme bancaire, Paypal, eBay, Amazon ...),en recopiant l'aspect du site origine, dans le but d'obtenir des données confidentielles

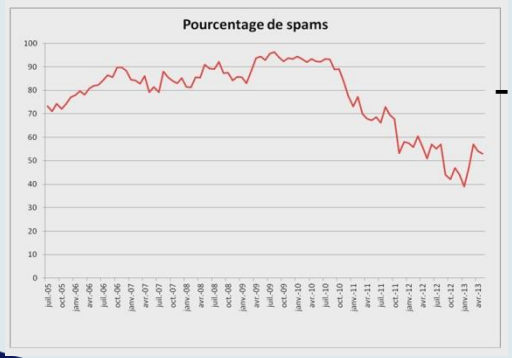
Exemple: Suivez ce lien pour réinitialiser vos données bancaire:
https://laposte.fr/loggin

Les risques liés à l'usage de la messagerie

- Le spamming (pourriel)

- C'est l'envoi massif et automatique, parfois répété, de courriers électroniques non sollicités, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a récupéré les adresses électroniques de façon irrégulière.

- Le spamming provoque un engorgement des communications et une réelle surcharge d'infos à «éliminer», néanmoins, en moyenne un destinataire sur 4,5 millions achèterait un produit suite à la réception d'un spam, poussant les spammeurs à poursuivre leurs campagnes.
- Attention: Certains ' malwares' peuvent transformer votre machine en distributeur de spams, vous serez alors 'blacklisté'



- En baisse depuis 4 ans, grâce aux filtres mis en place par les FAI et les logiciels anti-spam. (2011=90%, 2015=50%) au détriment des 'malwares'

Les risques liés à l'usage de la messagerie

- Le blacklistage (liste noire)

C'est ajouter un nom de personne, de programme, de domaine , d'adresse de courriel, ou une adresse IP sur une blacklist, c'est-à-dire une liste de malveillance.
Conséquence: Blocage de votre messagerie électronique par votre FAI.

Les raisons d'un blacklistage mail

- Votre ordinateur (ou plusieurs) de votre parc informatique ont été infectés par un virus qui émet des SPAM (courriers indésirables) en masse.
- Un spammeur a réussi à usurper votre identité pour émettre des courriers indésirables. Cette technique s'appelle **l'email spoofing**.

- Dans certains cas, il se peut qu'un client de votre fournisseur de messagerie ou votre fournisseur d'emailing ait été placé sur liste noire et que vous en subissiez les séquelles.

Les risques liés à l'usage de la messagerie

- Le mail Bombing (bombardement de messagerie)

- Le 'Mail Bombing' consiste à envoyer un nombre impressionnant d'emails à un destinataire ou des destinataires définis.

- L'objectif du 'Mail Bombing' est de saturer le serveur mail du destinataire et de saturer sa bande passante afin de le neutraliser temporairement en rendant impossible l'utilisation de son système de messagerie et son accès Internet. Le regroupement de plusieurs milliers de machines infectées ('PC zombie') au sein d'un même 'botnet' amplifie la technique du mail bombing.

- Malheureusement cette pratique augmente grâce à la mise à disposition sur Internet de logiciels gratuits qui permettent à n'importe quel internaute de faire de mauvaises blagues.

-Il n'y a malheureusement très peu de possibilités pour échapper à une attaque de ce type si elle vous est destinée, par contre l'expéditeur à de gros risques 'blacklistage'..

Autres risques liés à l'usage de la messagerie

– Les Hoaxes (canulars ou rumeurs):

- Un 'Hoax', caractérise un message dont le but est de manipuler les internautes en les poussant à répandre une rumeur (chaîne), une fausse alerte ou en les poussant à modifier et à endommager la configuration de leur machine.

- Le seul but de ces messages est de provoquer un effet 'boule de neige' par la diffusion pyramidale d'une fausse information et de saturer les circuits de communications.

Conseils: Ne détruisez pas de fichiers sans vous renseigner (INTERNET) et ne transférez pas les messages de chaînes reçues (même si le contenu touche votre sensibilité, les auteurs n'hésitent pas à utiliser des arguments convaincants pour arriver à leurs fins)

Crédibilité d'un HOAX: http://www.hoaxkiller.fr/hoax/2005/virus_invitation.htm

Des exemples

Exemples de piratage dans le sport

JO 2016: Après le piratage de l'Agence Mondiale Antidopage, les Fancy Bears (Hackers russes) révèlent une cinquième liste d'athlètes qu'ils accusent de dopage.

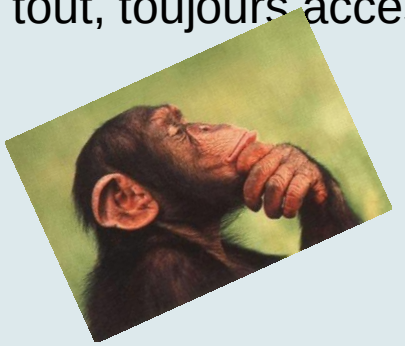
En 2015, Baseball: une équipe espionne une autre, 1er cas de cyber-attaque dans le sport.

Juin 2015, le portail Associations Sportives, qui répertorie plus de 240,000 clubs et associations françaises est infiltré.

UJSF
union des journalistes de sport en france

Mardi dernier, le site de l'Union des journalistes sportifs piraté par des djihadistes.

-**DES PHOTOS QUI ONT LA VIE LONGUE :** Selon une étude, menée par des chercheurs de l'Université de Cambridge, des photos effacées par des utilisateurs sur des réseaux sociaux en ligne sont malgré tout, toujours accessibles.



Les premiers émois d'un jeune hacker

Note: De nombreuses astuces et autres logiciels de hacking sont accessibles librement sur Internet et permettent aux futurs pirates de se faire la main.

yatto 02/02/2013 à 21:46:31

Haha sécurité informatique, cette semaine y'avait UN ordinateur qui pouvait booter sur l'USB, j'ai lancé Ophcrack et j'ai trouvé en 10mn le mot de passe Administrateur du lycée x)

Côté sécurité ils sont plutôt bons au lycée, mais avec une faille, on met en péril tout le réseau !

Alerte récente : 5 septembre 2016

ALERTE : Campagne de Spams déployant le cryptoware Zepto

1 - Risque(s)

Installation d'un logiciel malveillant de type Cryptoware nommé **Zepto**.

Un cryptoware exécute une attaque irréversible en chiffrant (cryptant) toutes les données de l'utilisateur victime, sur tous les supports connectés, y compris les dossiers (répertoires) partagés par/avec le compte utilisateur compromis se trouvant sur les autres machines d'un réseau local

2 - Systèmes affectés

Tous les systèmes d'exploitations Windows peuvent être victimes de ce logiciel malveillant.

3 - Résumé

Depuis le début septembre 2016, il est constaté à l'échelle nationale une vague de pourriels (e-Mails d'attaque) dont le taux de blocage par les passerelles anti-pourriel est relativement faible. Ces pourriels ont pour objectif la diffusion de Ransomware ou du Cryptoware Zepto.

Un cas concret : Ransomware LOCKY (rançongiciel)

Logiciel malveillant, sévit particulièrement en France depuis mars 2016, il en existe 60 variantes à ce jour.
Il cible plus particulièrement les abonnés de Free et les petites structures, lesquelles reçoivent des mails contenant de fausses factures.
Rédigé en français et émis par une adresse qui semble officielle, il invite à l'ouverture d'une pièce jointe pour consulter une facture. […]
L'ouverture du fichier exécute l'installation d'un logiciel malveillant venant infecter la machine et crypter les données.

La cible: Comité Ile de France de natation

La rançon demandée : 5 bitcoins (soit 447$ *5= **2.235 $**

Détails*: intervention de Nicolas*

Je suis infecté ?

Les principaux symptômes d'infection

- Votre ordinateur tourne plus lentement.
- Votre ordinateur se bloque et cesse de répondre.
- Des messages d'erreur inhabituels apparaissent
- Votre antivirus n'est plus actif et/ou vous ne pouvez plus l'exécuter.
- Vos correspondants ont reçus des mails que vous n'avez pas envoyés.
- Vous n'avez plus accès à vos périphériques (USB, imprimante, etc...)
- La lampe indiquant les accès à votre disque dur est constamment allumée alors que vous n' effectuez aucune opération.
- Le démarrage de mon ordinateur est devenu excessivement long.
- Mon ordinateur redémarre spontanément sans y être invité.
- Certaines applications ne fonctionnent plus normalement et/ou disparaissent.
- De nouvelles icônes sont apparues sur le bureau
- La page d'accueil de votre navigateur Internet a été modifiée et il est impossible de la restaurer;

Réaction en cas d'infection

- 1- **Isoler la machine** de tout réseau de communication (réseau local ou Internet)
- 2- Vérifier que votre antivirus est actif et qu'il est à jour. *(Au cas, le mettre à jour avec les fichiers d'une machine non contaminée)*
- 3- Lancer un scan complet de la machine si possible en mode sans échec. *(F8 ou F5 au démarrage)* pour chercher à identifier l'infection.
  - *Si l'antivirus ne fonctionne pas correctement vous pouvez soit essayer en copiant un antivirus sain sur clé USB ou en reconnectant temporairement votre machine et effectuer un antivirus en ligne.*
- 4- Rechercher d'autres possibilités de malware *(malwarebytes –anti-malware)*
- 5- Rechercher les logiciels espions (spyware) -> (*Spybot-Search & destroy)*
- 6- Rechercher les rootkits *(Sophos anti-rootkit)*
  - Si le virus est détecté, chercher le maximum de renseignements sur l'infection sur les forums spécialisés INTERNET pour comprendre 'COMMENT vous avez été infecté' (privilégier les sites officiels des anti-virus).
- 7- Faire le ménage dans votre machine en supprimant les fichiers facultatifs *(Ccleaner)*

- Si vous n'êtes pas sur d'avoir éradiquer l'infection, avant de reconnecter votre machine à INTERNET, faites la vérifier par un spécialiste qui vérifiera si des traces sont encore présentes (process, drivers, etc…) sur votre machine
- Terminer toujours une désinfection par un scan antivirus complet de votre machine en mode 'sans échec'

FIN
de la 2ème partie

FÉDÉRATION FRANÇAISE
NATATION

FÉDÉRATION FRANÇAISE
NATATION

La sécurité informatique

3ème partie

Sommaire

La sécurité informatique (1ère partie) *Vendredi 30 septembre*

1) - **Sauvegarde et restauration** *(Voir Présentation Jacques)*

La sécurité informatique (2ème partie) *Samedi 1er octobre*

2) - **Bilans, tendances et enjeux de la sécurité informatique**

3) - **Les risques de contamination?**

- Rappel des différentes nuisances potentielles

4) - **Des exemples**

5) - **Je suis infecté?**

- Les symptômes d'infection
- Que faire en cas d'infection ?

La sécurité informatique (3ème partie) *Dimanche 2 octobre*

6) - **La prévention et les remèdes**

- Ou se place la vulnérabilité?
- Le PC 100% sécurisé existe-t'il?
- Le comportement de l'utilisateur et les reflexes de sécurité
- La fiabilité des mots de passe
- Les logiciels de protection
- Quelques astuces

7) - **Conclusion**

La prévention et les remèdes

Ou se place la vulnérabilité ?

La vulnérabilité est liée principalement à:

- L'utilisation et au comportement des individus

- Le respect des procédures d'accès à l'information
- Précautions dans la consultation internet et les téléchargements
- Comportement lié à l'utilisation de la messagerie
- La sobriété au niveau des blogs et des réseaux sociaux

- La mise en place de protections

- Logiciels spécifiques (antivirus, anti spam, firewall, etc....)
- Mise à jour des configurations
- Disponibilité d'une sauvegarde
- La fiabilité des mots de passe

Ou se place la vulnérabilité ?

Protéger ses données, c'est déjà bien, mais il existe des tas d'autres manières de se faire plumer par internet. En informatique, on dit souvent que le problème se situe entre la chaise et le clavier. De très nombreux arnaqueurs l'ont compris et s'attaquent donc au maillon le plus faible: VOUS!

La prévention

- Le principal remède préventif réside dans

le comportement de l'utilisateur

Tout comme vous fermez la porte de votre domicile, il convient de verrouiller un minimum votre ordinateur afin que ce ne soit pas ' les portes ouvertes' à tous les virus et intrus de passage.

L'arrivée de l'INTERNET à haut débit a multiplié les possibilités d'utilisation de ce merveilleux outil mais malheureusement a démultiplié les risques de contagion et les conséquences d'infection.

Votre comportement, c'est 75% de votre sécurité informatique, les 25% restant sont à la charge de l'ensemble des logiciels de sécurité installés sur votre machine.

La prévention

Comportement RESPONSABLE de l'utilisateur

- **Comportement et réaction face à un incident**
  - Déceler l'incident
  - Supprimer la nuisance et nettoyer la machine
  - Prendre les mesures de sécurité adaptées pour éviter une récidive
- **Utilisation 'sobre' du système de messagerie**
  - Diffusion contrôlée des données et des adresses de messagerie
  - Méfiance absolue et réaction à l'égard de courriers suspects reçus
  - Soyez concis, la messagerie n'est pas un forum de discussion ni une initiation aux beaux arts.
  - ATTENTION aux courriers de type 'Chaine'
- **Comportement responsable dans l'utilisation du réseau INTERNET**
  - Sites accédés,
  - Traces laissées (coordonnées, renseignements professionnels ou privés) sur les sites ou les réseaux sociaux
  - Vérification de la sécurisation des sites en cas de paiement par Internet.

La prévention

A chaque démarrage de sa machine, l'utilisateur devrait avoir des réflexes préventifs et se poser les questions suivantes:

1- Mon logiciel antivirus est-il actif et à jour ?
2- Mon 'Firewall' (pare-feu) est-il actif ?
3- Les derniers correctifs de mon environnement Windows et de mes applications sont ils en place? (Windows & Office update)
4- Depuis quand date ma dernière sauvegarde?

A chaque consultation Internet ou utilisation de sa messagerie, l'utilisateur devrait avoir des réflexes préventifs et se poser les questions suivantes:

1- Si je dois fournir des renseignements personnels ou bancaires:
Est-ce que le site est sécurisé (adresse : https)?
Est-ce que les données fournies sont cryptées ('cadenas')?

CONSEILS: Ne remplissez aucun formulaire non demandé et évitez de répondre aux 'spams' que vous recevez.

La prévention

- **Quelques conseils**

1- N'ayez pas une confiance aveugle dans les outils de protection,

2- Ne téléchargez pas et n'installez pas n'importe quel logiciel sur votre machine, surtout si celui-ci vous promet de nettoyer votre machine.

3- N'exécutez pas le premier programme venu, même si votre antivirus ne signale rien

4- Ne jamais oublier que le mail est la voie d'infection la plus répandu. Ne jamais répondre et éviter de se désinscrire à un message non sollicité (Spam).

5- Ne multipliez pas les outils de protection de même type, un bon logiciel antivirus est plus efficace que trois logiciels antivirus qui vont se contrarier.

6- Préservez vos données personnelles privées, ne les divulguez pas sur des réseaux sociaux , sur des sites non sécurisés ou sur le 'Cloud'.

7- Sauvegardez régulièrement vos données et maintenez à jour votre système.

8- Paramétrez correctement les outils de sécurité de base de votre machine (niveau de sécurité, anti-hameçonnage, firewall, etc..). Fermez les portes!

9- Fermer vos session,

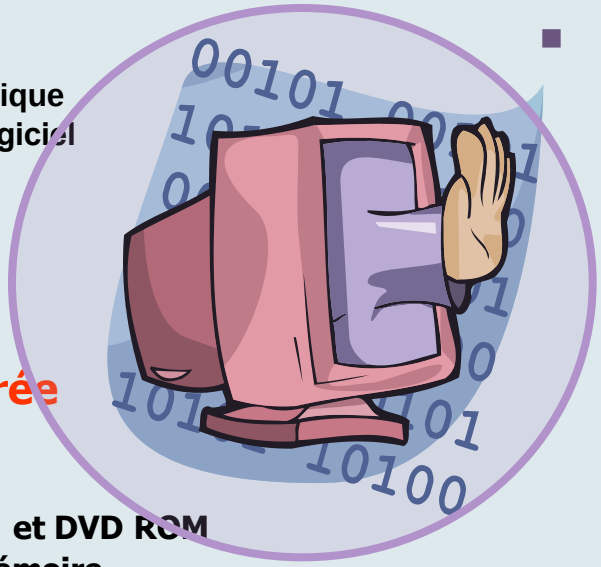
10- Eviter d'installer les compléments fournis lors de l'installation d'un logiciel (barre d'outils, accélérateur, module de recherche, etc… (case à cocher)

La prévention

Description du PC parfait - 100% sécurisé

Supprimer les menaces externes

- **Pas de connexion extérieure**
  - **Pas d'INTERNET**
    - Pas de Messagerie
    - Pas de consultation Web
    - Pas de mise à jour automatique
    - Pas d'enregistrement de logiciel en ligne
    - Pas de services en lignes
  - Pas de modem
  - Pas de connexion réseau
- **Pas de périphériques d'entrée**
  - **Pas de lecteurs**
    - Pas de disque externes
    - Pas de lecteur de CD ROM et DVD ROM
    - Pas de lecteur de carte mémoire
  - **Pas de transfert direct de données**
    - Pas de clé USB
    - Pas de branchement de PDA, Tel portable
    - Pas de branchement appareil photo, caméscope, etc..



Supprimer les menaces locales

- **PC installé dans un lieu sécurisé**
- **Un seul utilisateur**
  - Accès par login
  - Mot de passe indéchiffrable
- **Des sauvegardes permanentes**
  - Duplication des données (Raid 1)
- **Une protection électrique indiscutable**
  - onduleur, circuit protégé
  - alimentation redondante

La prévention

Description du PC parfaitement sécurisé

Aujourd'hui pouvez-vous travailler dans cette configuration sur votre PC ?

NON !

Supprimer les menaces locales

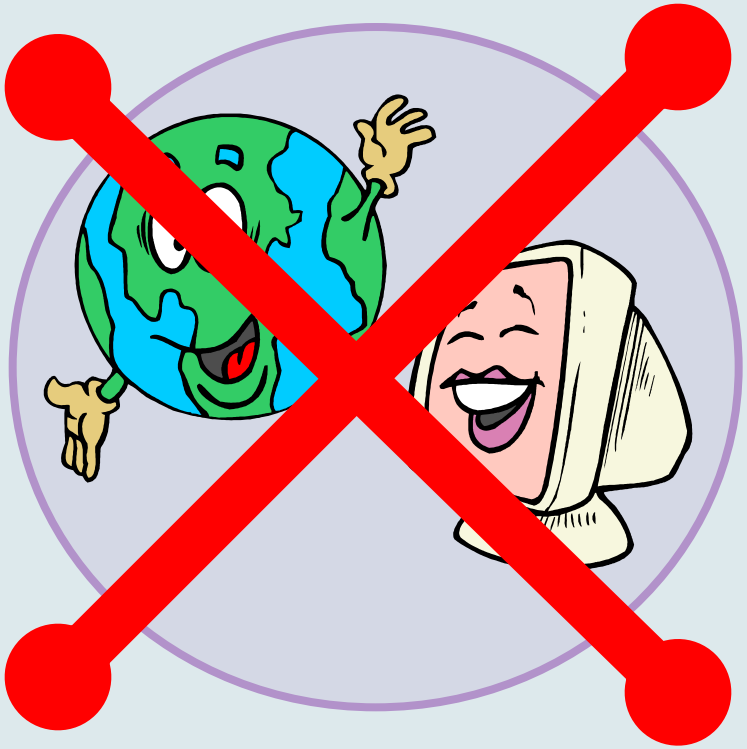
- **PC installé dans un lieu sécurisé**
- **Un seul utilisateur**
  - **Accès par login**
  - **Mot de passe indéchiffrable**
- **Des sauvegardes permanentes**
  - **Dupli tion d**
  - **ns (Ra**
  - **d**
- **r élec ue**
  - **u**
  - **cuit pr égé**
  - **redo nte**

Supprimer les menaces externes

- **Pa e**
  - **RNET**
    - **Pas de Messagerie**
    - **Pas de cons eb**
    - **Pas de or**
    - **de giciel e**
    - **ces en lignes**
  - **Pa e modem**
  - **Pas de connexion éme**
- **Pas**
  - **de disque externes**
    - **Pas de lecteur de CD ROM et DVD RO**
    - **Pas de lecteur de carte mémoire**
  - **Pas de transfert direct de données**
    - **Pas de clé USB**
    - **Pas de branchement de PDA, Tel portable**
    - **Pas de branchement appareil photo, caméscope, et**

La prévention

Le PC parfait, efficace, opérationnel, 100% sécurisé n'existe pas!



La prévention

Les mots de passe

La prévention

Efficacité et fiabilité du mot de passe

- **Pas trop court** *(expl: 1234, 1111,abcd)*
- Minimum 9 caractères
- Mélange de chiffres, lettres, caractères spéciaux.
- Eventuellement une phrase pour retenir le mot de passe
- Exemple: To be or not to be ? That is the question donne 2Bon2B?TitQ
- **Pas trop simple** *(expl:12345, azerty, password, iloveyou)*
- Pas lié à des informations personnelles (date de naissance, nom d'un animal de compagnie, plaque d'immatriculation, etc..)
- **Pas le même pour tout**
- Exemple: Yves1415lper, Yves1415gtsr, Yves1415orat

- Ne pas le noter ailleurs que dans votre mémoire,
- Ne pas le divulguer,
- Le changer régulièrement

La prévention

Efficacité et fiabilité des mots de passe

Exemples de mot de passe	Temps de crackage avec un ordinateur basique	Temps de crackage avec un ordinateur très performant
bananas	Moins d'une journée	Moins d'une journée
bananalemonade	2 jours	Moins d'une journée
BananaLemonade	3 mois, 14 jours	Moins d'une journée
B4n4n4L3m0n4d3	3 siècles, 4 décennies	1 mois, 26 jours
We Have No Bananas	19151466 siècles	3990 siècles
W3 H4v3 N0 B4n4n45	20210213722742 siècles	4210461192 siècles

(source 01informatique – janvier 2012)

La prévention

Caractéristiques d'un excellent mot de passe :

Minimum de 12 caractères
Au moins 1 chiffre
Au moins 1 caractère en minuscule
Au moins 1 caractère en majuscule
Au moins 1 caractère spécial ($#§/\[]{}...)
Au moins 1 caractère accentué (dans les langues où cela existe)
Aucune chaîne contenue dans votre adresse électronique
Aucun mot figurant dans un dictionnaire, ni ces mêmes mots écrits à l'envers
Aucune date
Aucun code ou numéro tel que numéro de Sécurité Sociale, plaque d'immatriculation de véhicule, etc. ...
Aucun caractère répété (ex. : 55555)
Aucune suite logique de caractères (ex : 123456)

Inconvénient: Il risque d'être dur à mémoriser

Les remèdes

- **Les outils techniques indispensables**
  - **Un bon antivirus avec mise à jour journalière automatique.**
    - assure la protection contre les attaques de virus en provenance d'Internet, de la messagerie ou de supports mémoires externe (clé USB, CD-ROM, etc..)

- **Antivirus local gratuit:**
  - AVG
  - AVIRA
  - AVAST

- **Antivirus en ligne gratuit**
  - Trend House Call 32 ou 64 bits

En 2016, sans anti-virus et pare-feu, votre machine a
4 minutes
pour survivre à Internet

Les meilleurs logiciels antivirus pour Windows

(particuliers)

Juin 2016

Les remèdes

- **Les outils techniques indispensables** (suite)
  - **Un pare-feu (Firewall)**
    - protège des intrusions sur votre PC par des programmes inconnus et non sollicités. Surveille le trafic entre votre PC et l'extérieur (Ports de communication) et ne laisse passer que les programmes autorisés.
    - **Note:** Le pare-feu incorporé dans Windows est généralement suffisant pour la majorité des utilisateurs lorsqu'il est bien paramétré.
    - **Autre pare-feu (firewall) gratuits:**
      - Sophos UTM Home Edition
      - Comodo Personal Firewall
      - Zone Alarm Free

Les remèdes

- **Les outils techniques indispensables** (suite)
  - **Un anti-malware/anti-spyware mis à jour régulièrement**
    - Intercepte les attaques et limite le nombre de logiciels qui espionnent votre comportement en permanence et qui ralentissent votre machine.
    - **Logiciels antimalware/antispyware gratuits:**
      - MBAM Malware Byte Anti-Malware
      - Adw Cleaner
      - Rogue Killer

  - **Éventuellement, un logiciel de contrôle parental**
    - Permet au parents de choisir les sites adaptés à chacun de leurs enfants et d'éliminer tous les autres.
    - **Logiciels de contrôle parental:**
      - XOOLOO PC
      - Web Filter PC

Les remèdes

- **Les outils techniques conseillés** (suite)
  - **Un nettoyeur mis à jour régulièrement**
    - nettoie votre PC, en supprimant les fichiers temporaires, les erreurs, les traces de navigation.
    - Note: Outil à manier avec précautions (un conseil: laisser les paramètres de configuration par défaut).
    - **Nettoyeur gratuits:**
      - Ccleaner
  - **Un anti-rootkit** *(AVG anti-rootkit, Seem, McAfee anti-rootkit, etc…)*
    - Les rootkits utilisent les mêmes techniques que les anti-virus pour se cacher dans le système d'exploitation, la mise au point de ces outils est très délicate mais elle est vitale pour le futur. Une course contre la montre perpétuelle se joue entre les infections et les remèdes
    - **Logiciels anti-rootkit gratuits:**
      - Malware Byte Anti-Rootkit
      - Sophos Anti-Root-Kit
      - Gmer, AVG anti-rootkit
      - Inoculer

Les remèdes

Quelques conseils

- Utilisez deux adresses email
  - Une gardée secrète qui ne vous ne diffuserez que pour les services et communications officielles.
  - Une temporaire que vous pourrez utiliser et diffuser sur Internet sur les sites qui vous demande une inscription.

  Avantage: Tri séparé des messages issus de chaque adresse, limitation de diffusion de l'adresse principale.

- Éliminer régulièrement les traces de navigation sur votre machine
  - Cela empêche les robots collecteurs d'informations de récupérer des données personnelles telles que votre adresse email ou les sites visités. Données exploitées ensuite par les spammeurs..

- Après une absence prolongée
  - Allez consulter votre boite aux lettres de messagerie directement sur le service Webmail mis à disposition par votre FAI. Cela vous permettra d'éliminer directement sur le serveur de votre FAI, tous les messages non sollicités reçus en votre absence et limitera le transfert aux messages sollicités, vous concernant directement.

Les remèdes

Comment savoir si votre email est blacklisté ?

Il existe plusieurs outils pour vérifier si votre messagerie a été bloquée, en voici quelques exemples :

http://mxtoolbox.com/blacklists.aspx

http://www.audemail.com/

https://www.ultratools.com/tools/spamDBLookup

Ces outils vous permettent d'identifier d'où vient le blocage et quel serveur vous a blacklisté.

Pour arriver à ce résultat, ces sites vont chercher leurs informations auprès de plus de 100 organismes qui listent les blacklistages. Les plus réputés d'entre eux sont CBL, Baracuda et SORBS.

Les remèdes – les cookies

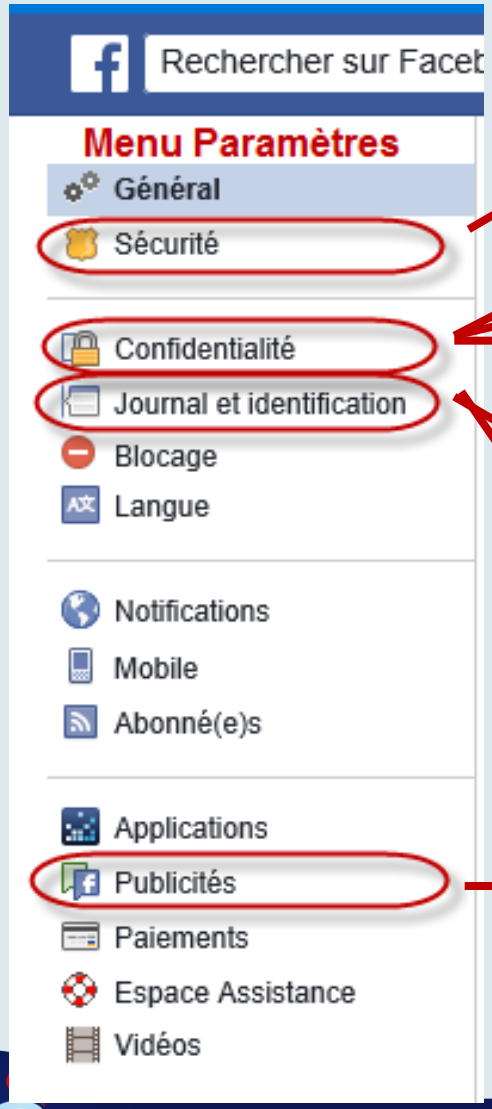
- **Comment se débarrasser des cookies stockés sur son poste.**

- **Sur Firefox**
- Options > Vie privée > Supprimer les cookies spécifiques.

- **Sur Internet Explorer**
- Options internet > Général > Paramètres > Afficher les fichiers.
  C:\Users\xxxx\AppData\local\Microsoft\NetCache\

- **Sur Chrome**
- Paramètres>paramètres avancés\Confidentialité>Paramètres de contenu>Cookies et données du site.

Les remèdes : les bons paramétrages *(Facebook)*



Prenez le temps de bien paramétrer vos accès aux réseaux sociaux

Alertes de connexion

Qui peut voir mon contenu ?

Qui peut me contacter ?

Qui peut me trouver avec une recherche ?

Qui peut ajouter des contenus sur mon journal ?

Qui peut voir les contenus de mon journal ?

Qui peut voir vos actions sociales associées aux publicités ?

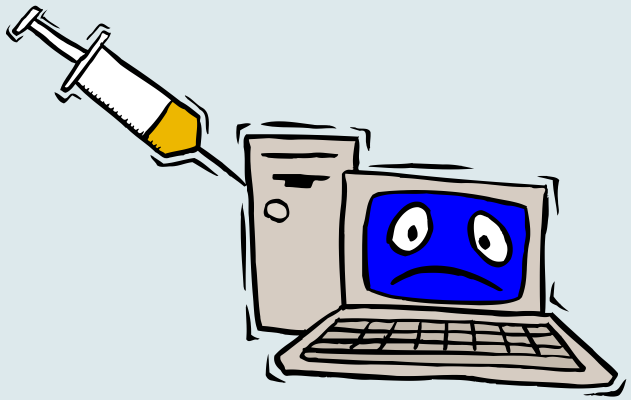
Les remèdes

- **Quelques bonnes adresses et les bons tuyaux**
  - Informations, conseils, actualités sur les virus :
    - https://www.symantec.com/fr/fr/security_response/landing/azlisting.jsp?azid=W
    - https://securelist.fr
    - http://www.zdnet.fr/actualites/10-techniques-pour-detecter-un-virus-informatique-39708433.htm
    - http://www.lemondeinformatique.fr/virus-et-anti-virus-33.html
    - http://nephi.unice.fr/Antivirus/sophos-a-to-z-computer-and-data-security-threats.pdf
  - Sites spécialisés 'Sécurité' et procédures d'éradication

    http://www.assiste.com

    http://www.secuser.com

    http://securite.developpez.com/cours/




Conclusion

Conclusion

La sécurité est l'affaire de tous.
Toute négligence individuelle ou comportement irresponsable, peut entraîner de graves conséquences sur le fonctionnement des machines et des pertes de données

Soyez VIGILANTS
et ne soyez pas crédules!

Les sollicitations bienveillantes d'Internet, le fait que l'on s'intéresse à vous, que l'on vous flatte, que l'on vous propose des affaires mirobolantes ou que l'on vous demande votre avis…..

Tout ceci est rarement gratuit... ne vous laissez pas piéger!

FIN

FÉDÉRATION FRANÇAISE
NATATION

www.ffnatation.fr - T. 01 41 83 87 70 - F. 01 41 83 87 69 - 14 rue Scandicci - 93508 PANTIN Cedex