LE GOUVERNEMENT
du Grand-Duché de Luxembourg

mySecureIT

Programme de sensibilisation des jeunes à la sécurité informatique

www.mysecureit.lu
www.cases.lu

CASES LUXEMBOURG

CLUSSIL

mySchool!

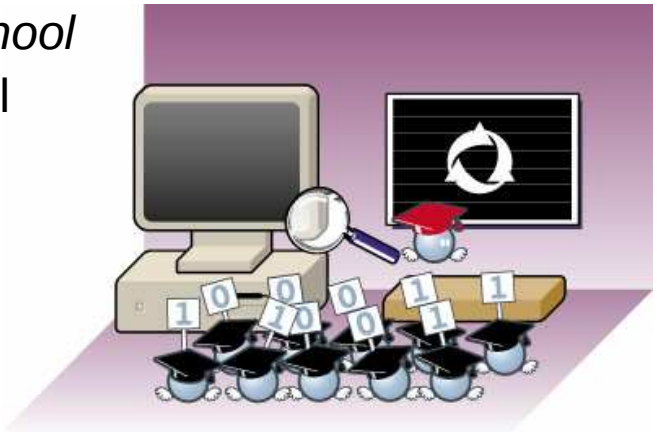
script Service de coordination de la recherche et de l'innovation pédagogiques et technologiques

- mySecureIT, c'est quoi ?

- De qui ?
  - Ministère de l'Éducation Nationale
  - MinEco (CASES)
  - *mySchool*
  - Clussil
- Pourquoi ?

  Quels sont les dangers et comment peut-on se protéger ?
- Pour qui ?

  Tous les élèves de septièmes qui :
  - utilisent les ordinateurs pour jouer et s'intéressent aux nouveautés,
  - veulent plus d'accès à internet,
  - se préparent à utiliser le PC pour apprendre et pour travailler.



Pourquoi une sensibilisation est-elle nécessaire ?

- Informatique incontournable.
- PC avec DSL en permanence sur Internet .
- Propagation rapide de « malware » (virus, vers etc.).
- Un PC non protégé sur Internet devient immédiatement exploitable.
- Se sécuriser présuppose la connaissance des dangers existants.
- Média utilisé pour harcèlement (cyberbullying)

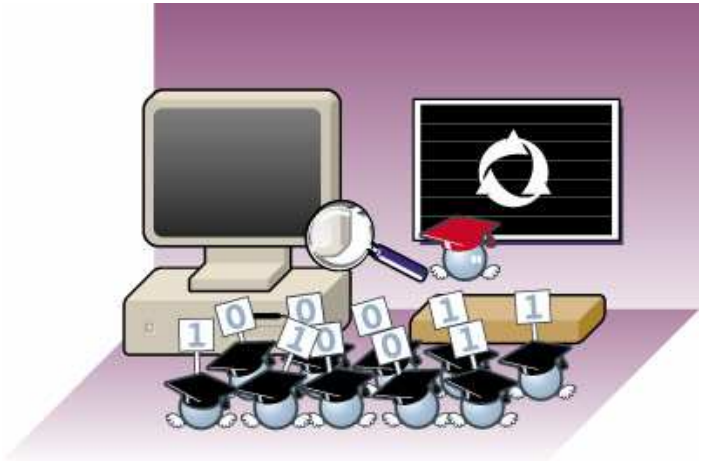
Un homme prévenu en vaut deux.

Sensibilisation à la Sécurité Informatique

- *mySecureIT*, c'est quoi ?

Menu du Jour:

1. La sécurité de l'information, c'est quoi ?
2. Quelles sont les menaces pour mon PC ?
3. Comment me protéger ?
4. Pourquoi ne pas devenir cracker ou Bully ?
5. Qu'est-ce qu'il faut retenir ?



Questions?

LE GOUVERNEMENT
du Grand-Duché de Luxembourg

1) La sécurité de l'information c'est quoi ?

- **Information:**

  Photos, e-mail, texte du Chat, notes, mots de passe, données bancaires, jeux.

- **Sécurité :**

  La qualité d'être protégé contre des abus.

  Abus: Divulgation, altération, pertes, accès illicite, disponibilité…)

- **Risque :**

  Possibilité qu'une menace exploite une vulnérabilité et crée un impact.

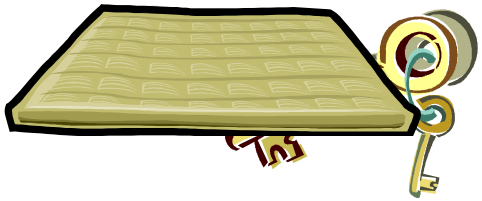
- **Risque résiduel :**

  Risque qui subsiste après application des précautions et contre-mesures servant à réduire le risque.

Sensibilisation à la Sécurité Informatique

1) La sécurité de l'information c'est quoi?

- Exemple d'un risque: Le cambrioleur



Vulnérabilité:
Clés sous le tapis.

Menace:
Cambrioleur essaie d'entrer.

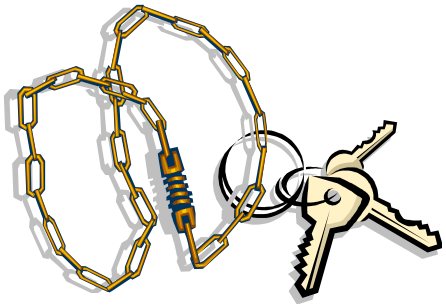
Impact: Cambrioleur casse l'armoire, vole de l'argent, crée des ennuis.

Risque = Vulnérabilité • Menace • Impact

Sensibilisation à la Sécurité Informatique

1) La sécurité de l'information c'est quoi?

- Exemple d'un risque résiduel : Le pickpocket



Réduction de risque :
Prendre les clés avec soi.

Risque résiduel : Un pickpocket vole les clés.

→ La sécurité à 100% n'existe pas.

2) Quelles sont les menaces pour mon PC ?

1. Menaces «aveugles»
   - vers et virus
   - spam
   - phishing
   - autres: dialer, spyware

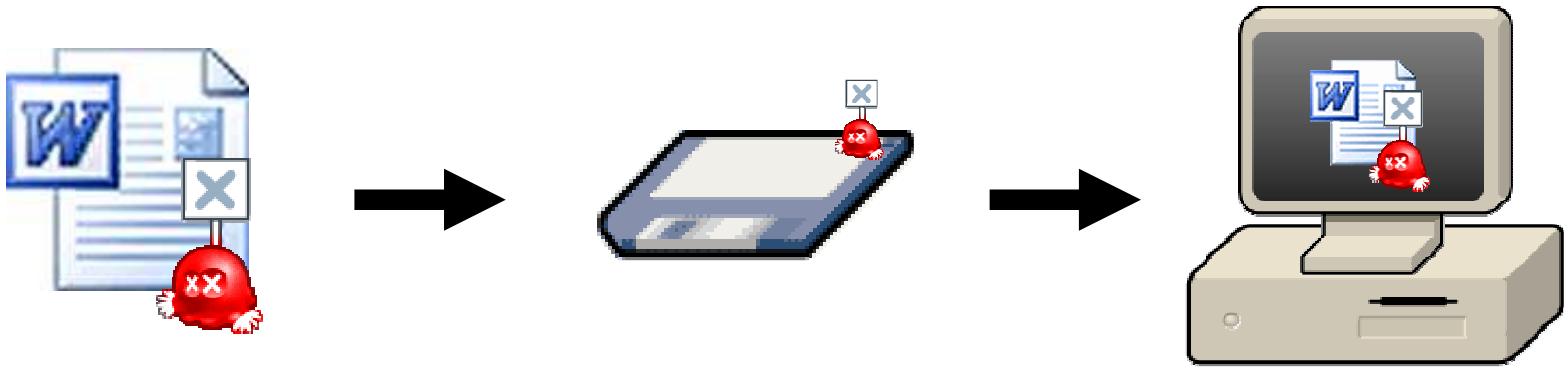
2. Menaces ciblées
   - attaques ciblées en ligne.
   - divulgation par chat.

2.1. Menaces «aveugles»

- Virus

Virus

Un **virus** est un logiciel qui **s'attache** à tout type de document électronique, et dont le but est d'infecter ceux-ci et de se propager sur d'autres documents et d'autres ordinateurs.
Un virus a besoin d'une intervention humaine pour se propager.

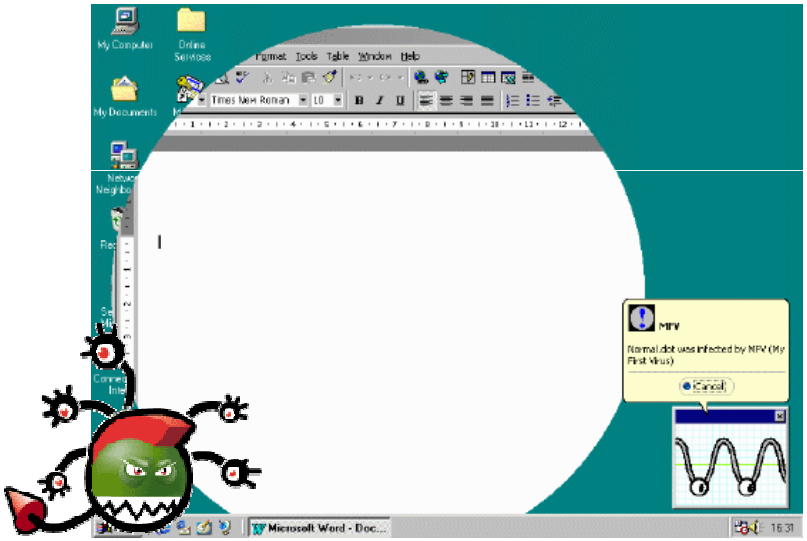


Sensibilisation à la Sécurité Informatique

2) Quelles sont les menaces pour mon PC ?

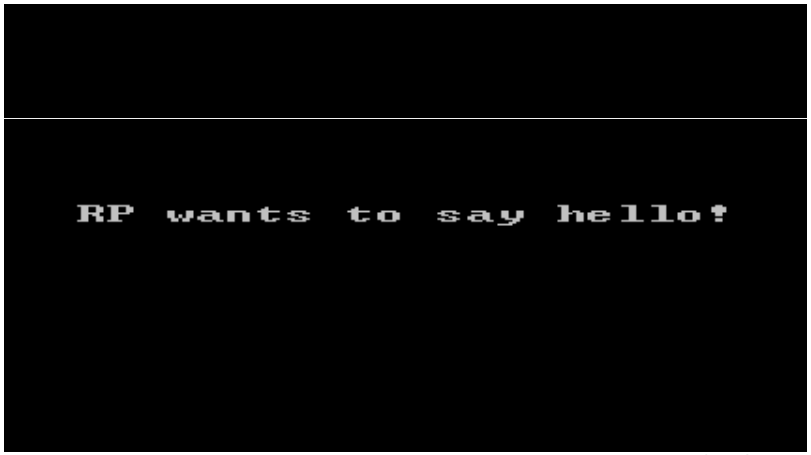
- Exemples concrets de Virus:

Macro Virus: Gullible

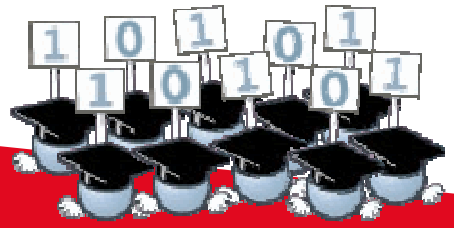


© F-Secure

Boot Sector: Rhubarb



© F-Secure

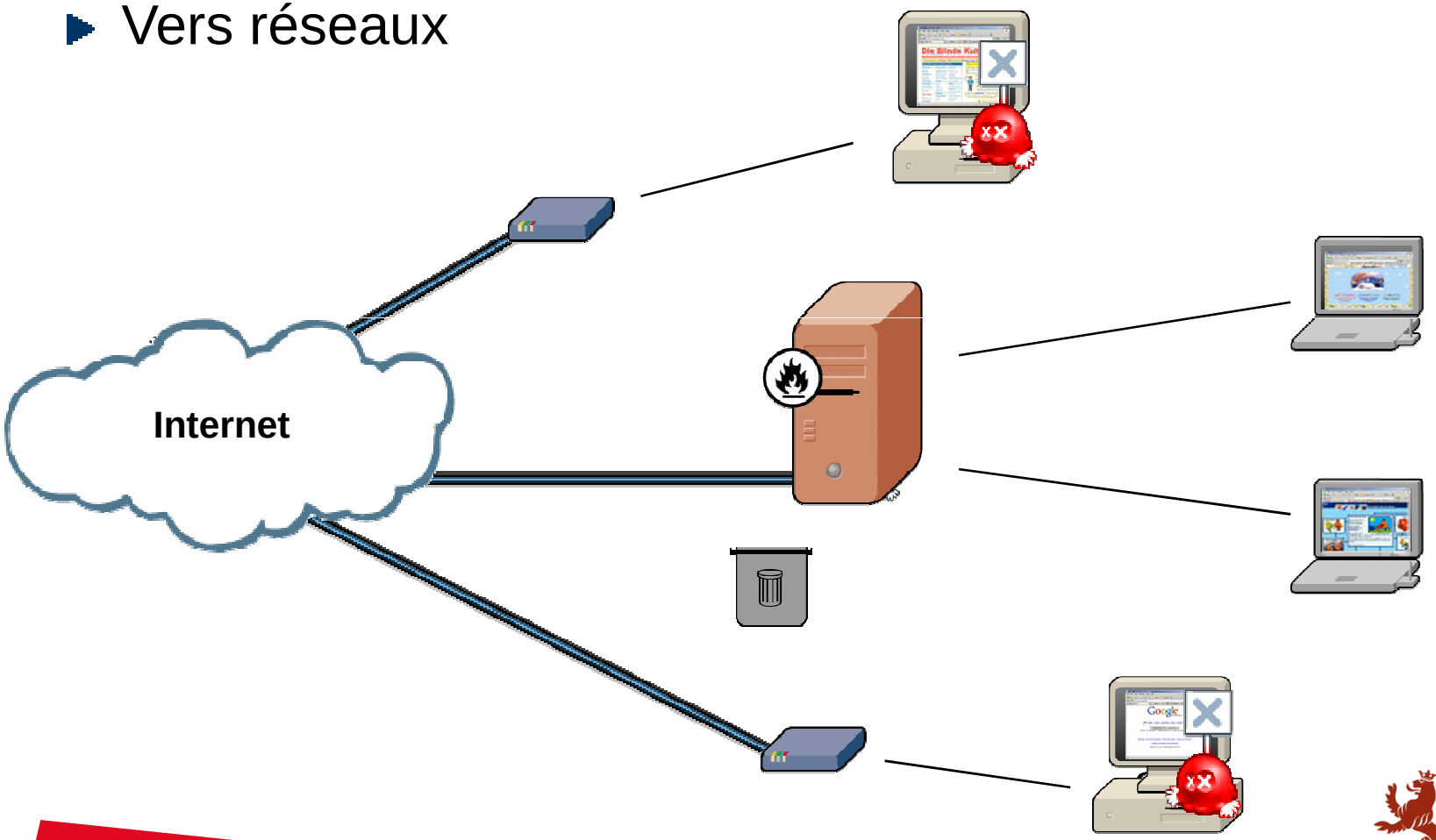


LE GOUVERNEMENT
du Grand-Duché de Luxembourg

Sensibilisation à la Sécurité Informatique

2) Quelles sont les menaces pour mon PC ?

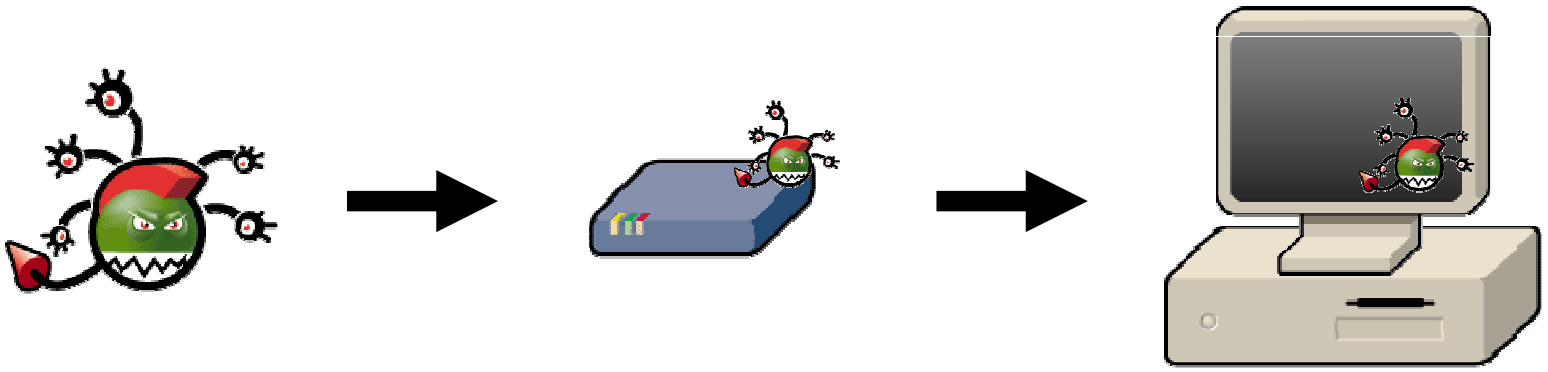
- Vers réseaux



LE GOUVERNEMENT
du Grand-Duché de Luxembourg

Vers

Un **ver** se reproduit en s'envoyant à travers un réseau (e-mail, Bluetooth, chat..)
Le ver n'a pas besoin de l'interaction humaine pour pouvoir se proliférer.

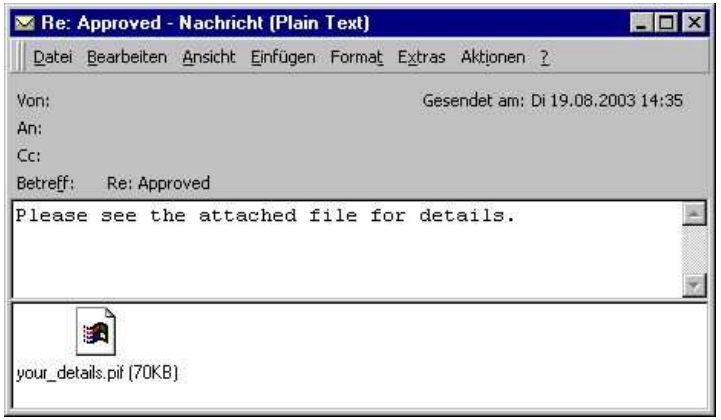


Sensibilisation à la Sécurité Informatique

2) Quelles sont les menaces pour mon PC ?

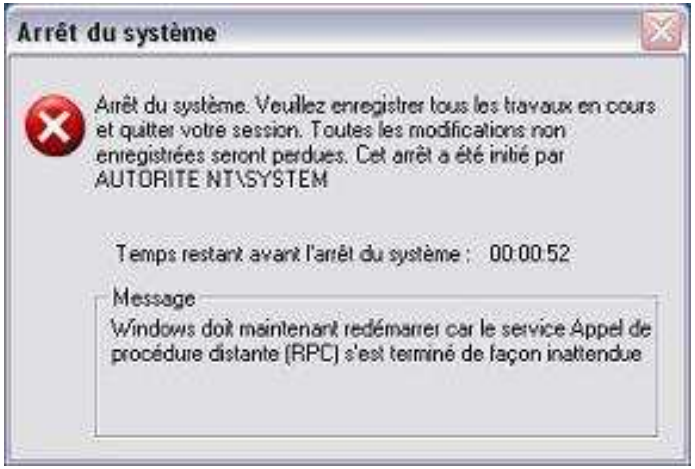
- Exemples concrets de vers:

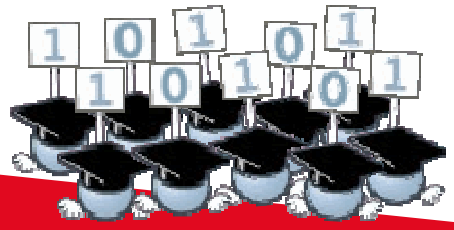
Email: Sobig.F



© BSI

Réseau RPC: MSBlaster

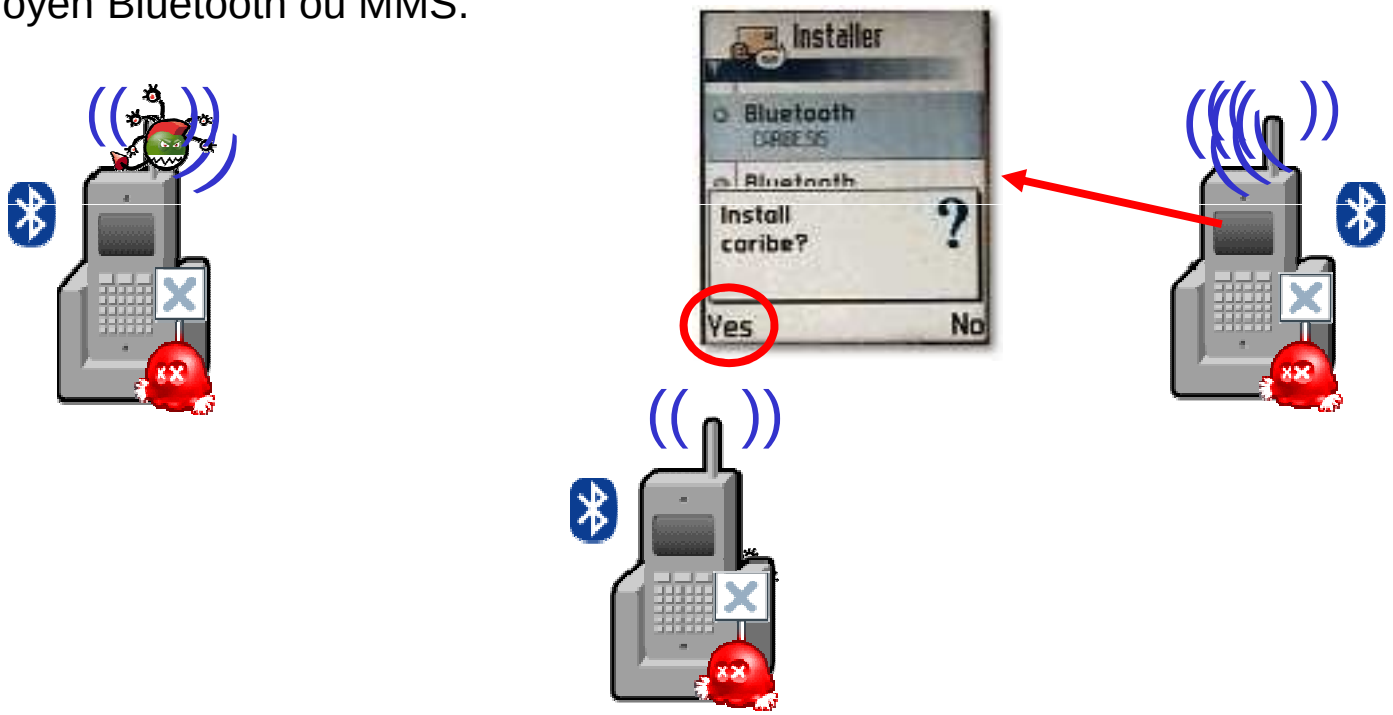




LE GOUVERNEMENT
du Grand-Duché de Luxembourg

Vers GSM

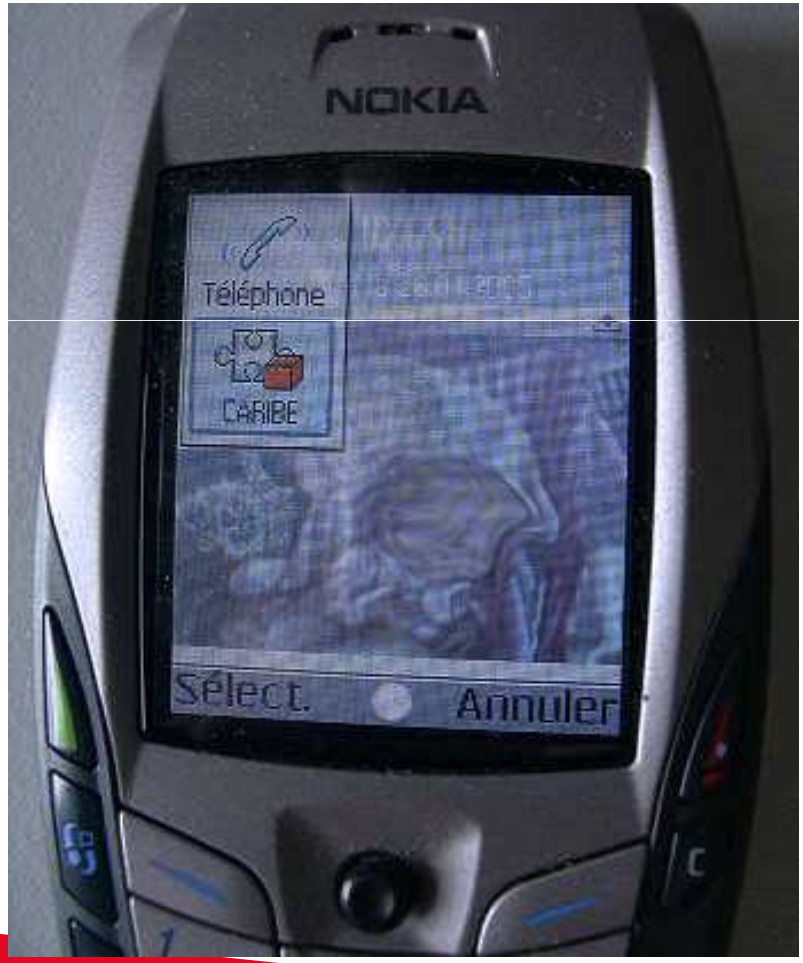
- Un **ver** GSM se reproduit en s'envoyant à un autre téléphone mobile par moyen Bluetooth ou MMS.



Sensibilisation à la Sécurité Informatique

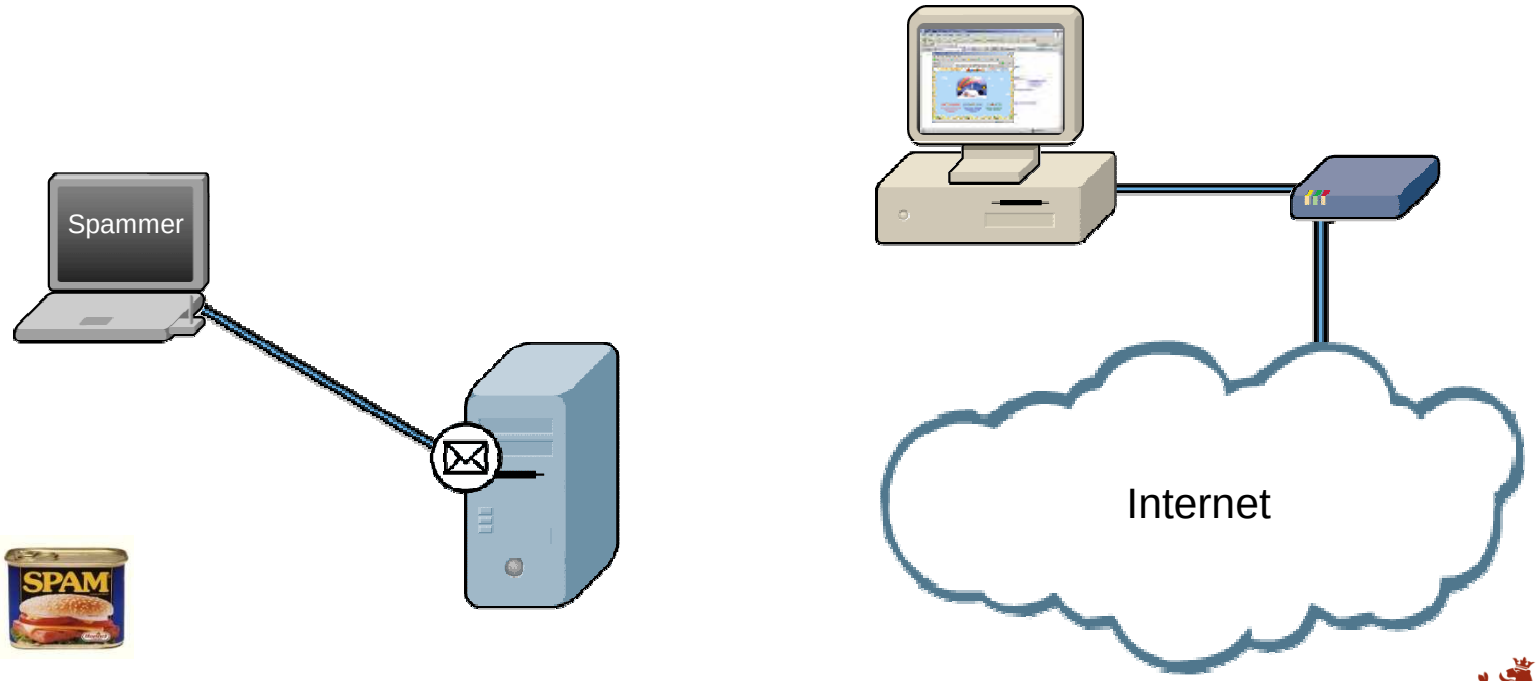
2) Quelles sont les menaces pour mon PC ?

Première infection connue d'un ver Bluetooth au Luxembourg - 26/04/05



LE GOUVERNEMENT
du Grand-Duché de Luxembourg

- SPAM
  - Le spam est du courrier électronique non sollicité envoyé a un très grand nombre de personnes sans leur accord préalable.



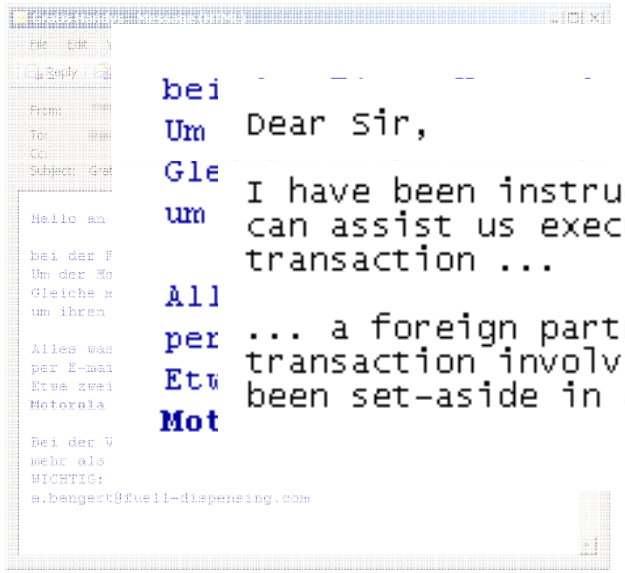
Sensibilisation à la Sécurité Informatique

2) Quelles sont les menaces pour mon PC ?

- SPAM

Gratis Handy (HOAX)

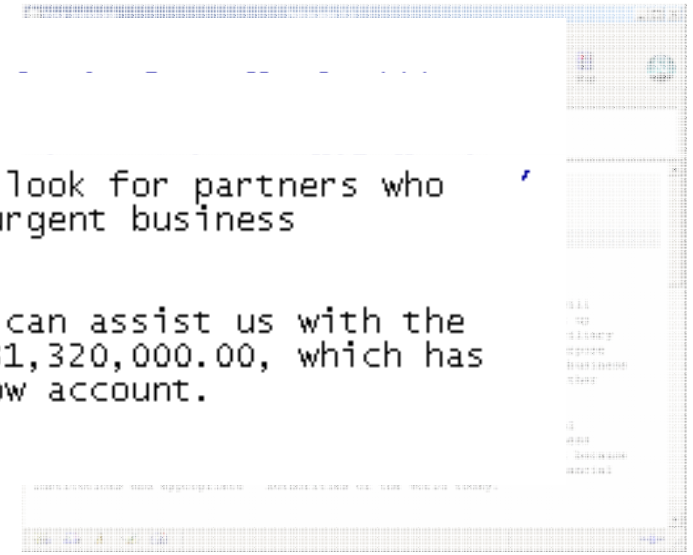
Nigeria 419 (Email/Fax&Fraude)



Dear Sir,

I have been instructed to look for partners who can assist us execute an urgent business transaction ...

... a foreign partner who can assist us with the transaction involving US$31,320,000.00, which has been set-aside in an escrow account.



LE GOUVERNEMENT
du Grand-Duché de Luxembourg

My eBay

Please follow these 2 quick steps to Submit and Verify your information

1 Enter your current credit/debit card information.

Name (from credit card statements)

Address (from credit card statements)

City

State

Zip/postal Code

Country United States

Phone Number

Credit Card Number

(e.g. 1234 5678 1234 0000 for Visa)

Expiration Date 01 / 2005

PIN Number

Important Guidelines

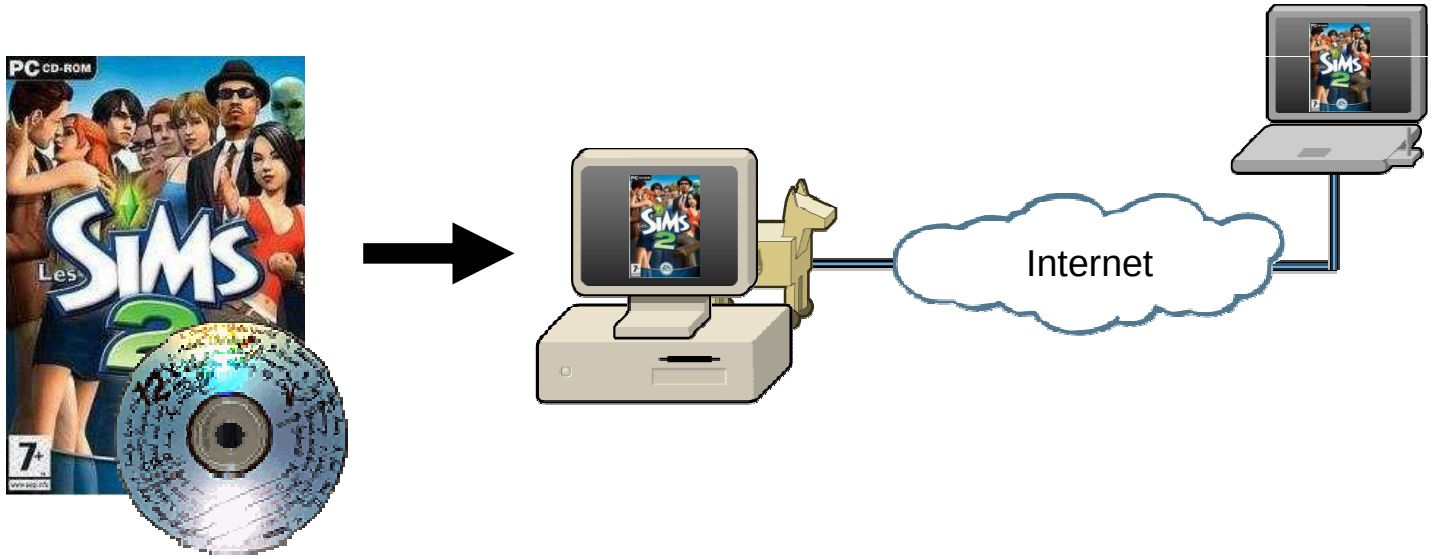
Please type your name and address *as it appears on your credit card statements.*

You must be the credit card holder or an authorised user of the credit card.

LE GOUVERNEMENT
du Grand-Duché de Luxembourg

2.2. Menaces ciblées

- Attaques en ligne ciblées : Cheval de Troie



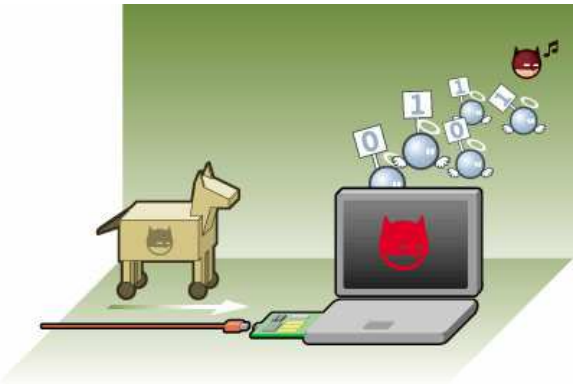
LE GOUVERNEMENT
du Grand-Duché de Luxembourg

Sensibilisation à la Sécurité Informatique

2) Quelles sont les menaces pour mon PC ?

- **Cheval de Troie**

  Programme bénin (jeux, documents…) cachant un autre programme.
  Lorsque le programme est exécuté, le programme caché s'exécute aussi et pourrait ouvrir une « porte cachée ».



Conséquences de cette attaque :

- contrôle du PC de l'extérieur
- perte de données
- divulgation de données privées (chat, e-mails …)
- espionnage: microphone, webcam
- attaques à partir du PC « infecté »

LE GOUVERNEMENT
du Grand-Duché de Luxembourg

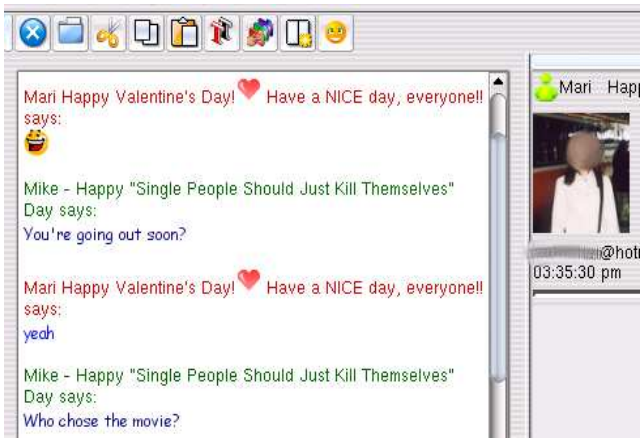
Sensibilisation à la Sécurité Informatique

2) Quelles sont les menaces pour mon PC ?

- Divulgation dans le chat
  - Le chat est un moyen amusant de se retrouver avec des amis et de rencontrer de nouvelles personnes. Le chat se fait par interface Web ou par moyen de logiciels spécifiques.

Profitez du chat en respectant quelques règles :

- Ne divulguez pas votre nom ou adresse.
- Pas de rencontres secrètes « réelles » avec des connaissances du chat.
- N'acceptez pas de fichiers d'étrangers.
- Discuter des discussions désagréables, les agressions, des problème (avec vos parents).



LE GOUVERNEMENT
du Grand-Duché de Luxembourg

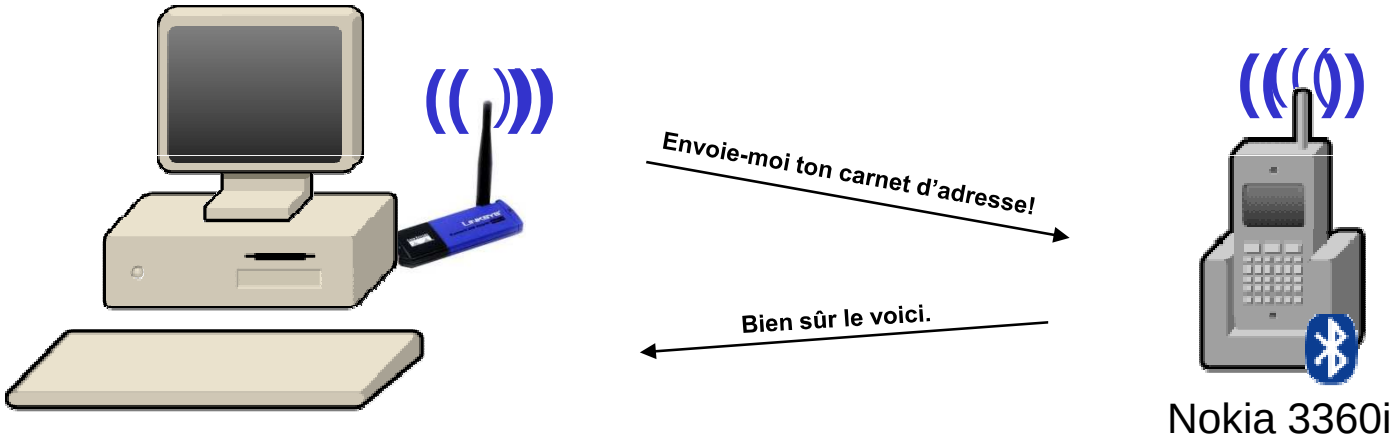
Attaque Bluetooth :

Téléphones vulnérables à cette attaque spécifique :

- Nokia 6310, Nokia 6310i, Nokia 8910, Nokia 8910i
- Sony Ericsson T68, T68i, R520m, T610, Z600, Z1010.

La démonstration a été faite avec un téléphone **standard** Nokia 6310i.

Attaque Bluetooth :



LE GOUVERNEMENT
du Grand-Duché de Luxembourg

- Questionnaire - Menaces

Grand quiz www.mysecureit.lu

Si vous fermez cette fenêtre, toutes vos réponses seront perdues. **Session démarrée à 23:09:09**

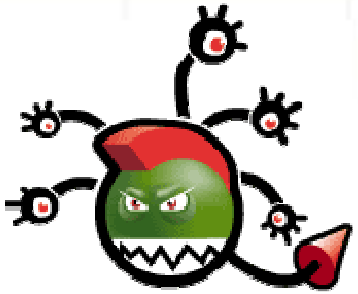
Cochez la constatation correcte! **[8/10]**

- ○ Un ver infecte d'autres fichiers tandis qu'un virus s'envoie soi-même à travers un réseau.
- ○ Un virus peut infecter un être humain alors qu'un ver ne le peut pas.
- ○ Un ver utilise un réseau (avec câble ou sans fil) pour se propager tandis qu'un virus nécessite l'intervention de l'utilisateur d'un PC pour infecter un autre PC.

Les conséquences d'un 'Cheval de Troie' sont: **[9/10]**

- ○ Il fait autre chose que ce que l'on croit à première vue.
- ○ Il ne fait rien de spécial.
- ○ Il affiche des graphiques sur l'écran.

Continuer



3) Comment me protéger?

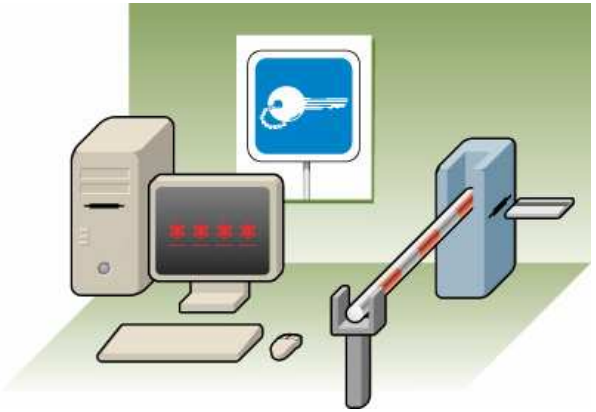
- **Contre-mesures techniques**

  A) Limitez vos droits

  B) Auto-Update

  C) Anti-virus

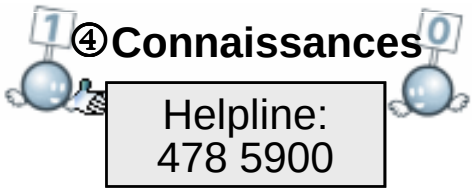
  D) Personal firewall



- **Contre-mesures humaines**

  Attention aux messages d'avertissement

Contre-mesures humaines:

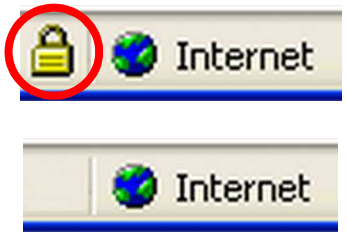


LE GOUVERNEMENT
du Grand-Duché de Luxembourg

Sensibilisation à la Sécurité Informatique

3) Comment me protéger ?

- Messages d'avertissement
  - N'envoie pas de données sensibles à travers des connections non sécurisées.



  - Lis les messages d'avertissement consciemment, en cas de doutes contactez vos parents ou la **Helpline** au **478 5900**.
  - Exemple : Les mots de passe sauvegardés de cette façon ne sont pas sécurisés.

LE GOUVERNEMENT
du Grand-Duché de Luxembourg

Contre-mesures techniques :

A) Limitez vos droits !

- GSM: Ne laissez pas Bluetooth allumé en permanence.
- PC: Coupez Internet si vous ne surfez pas.
- PC: Créez un utilisateur SURF avec des droits limités.

Si vous êtes alors attaqué, le pirate ne peut causer que des damages limités.

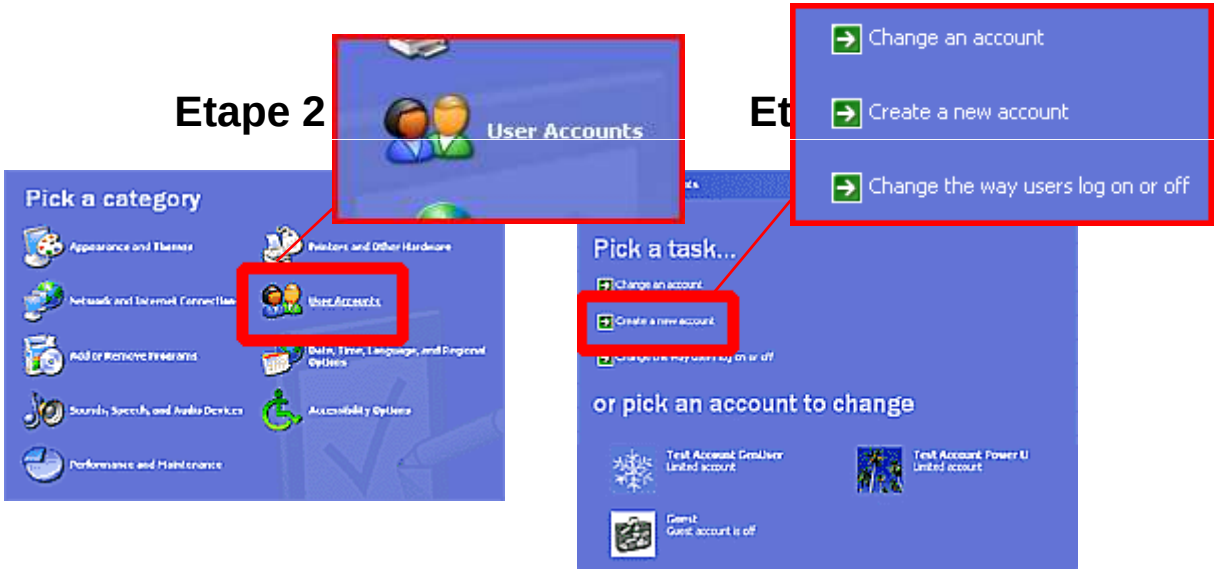
LE GOUVERNEMENT
du Grand-Duché de Luxembourg

Création d'un nouvel utilisateur avec des droits limités

- **1.** Control Panel **2.** User Account **3.**Create a User Account

Etape 1

Etape 2

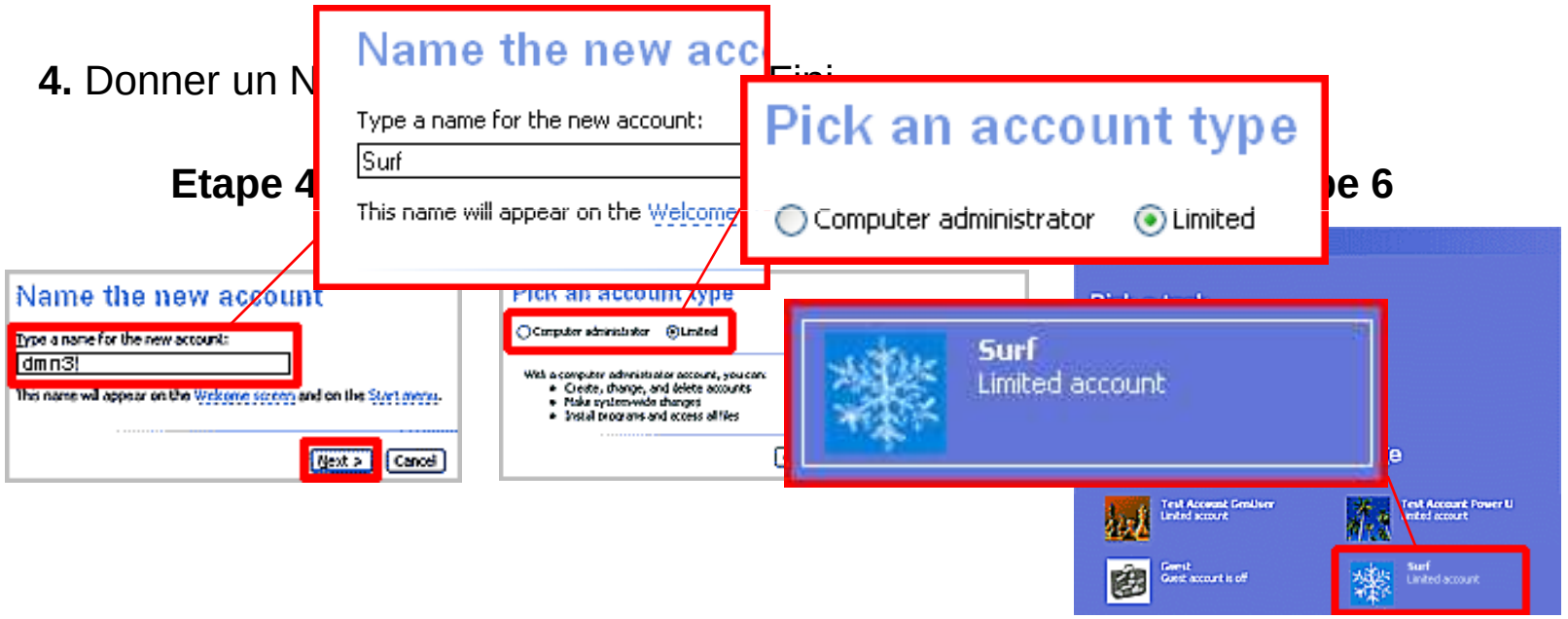


LE GOUVERNEMENT
du Grand-Duché de Luxembourg

Création d'un nouvel utilisateur avec des droits limités (suite)

4. Donner un N… Fin;

Etape 4 … **Etape 6**

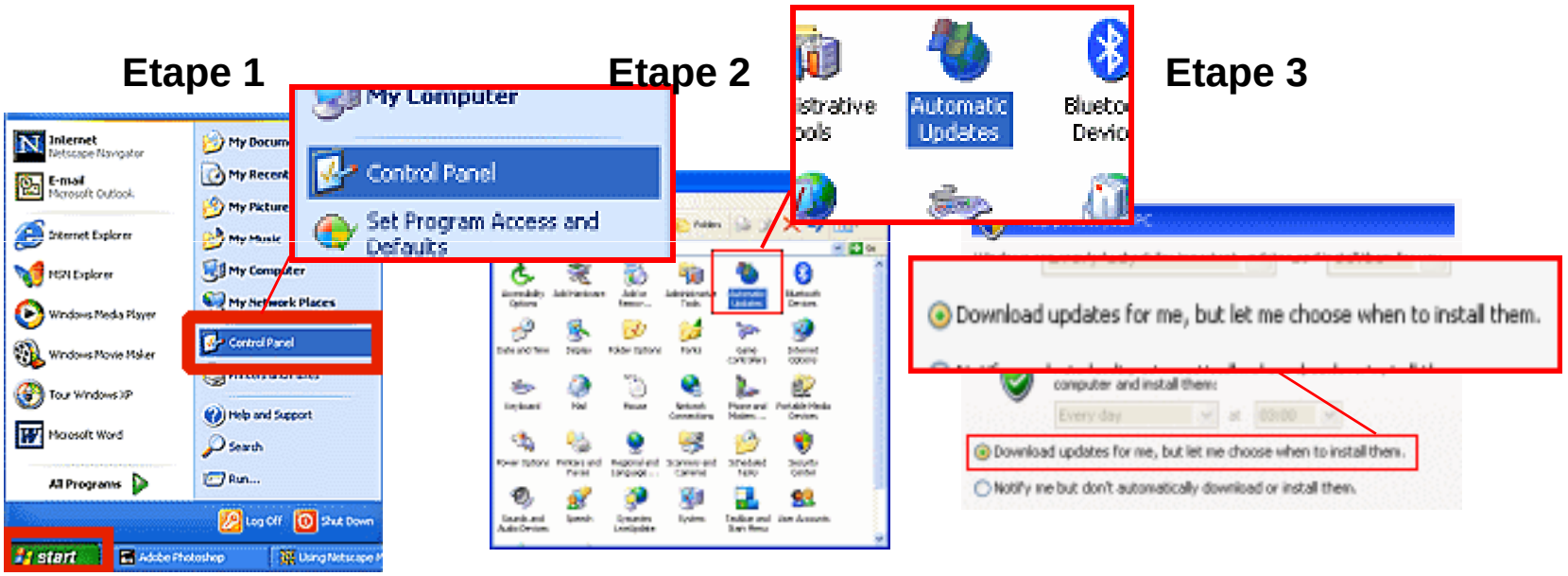


LE GOUVERNEMENT
du Grand-Duché de Luxembourg

Sensibilisation à la Sécurité Informatique

3) Comment me protéger ?

- B) Activez la fonction « Automatic Updates »

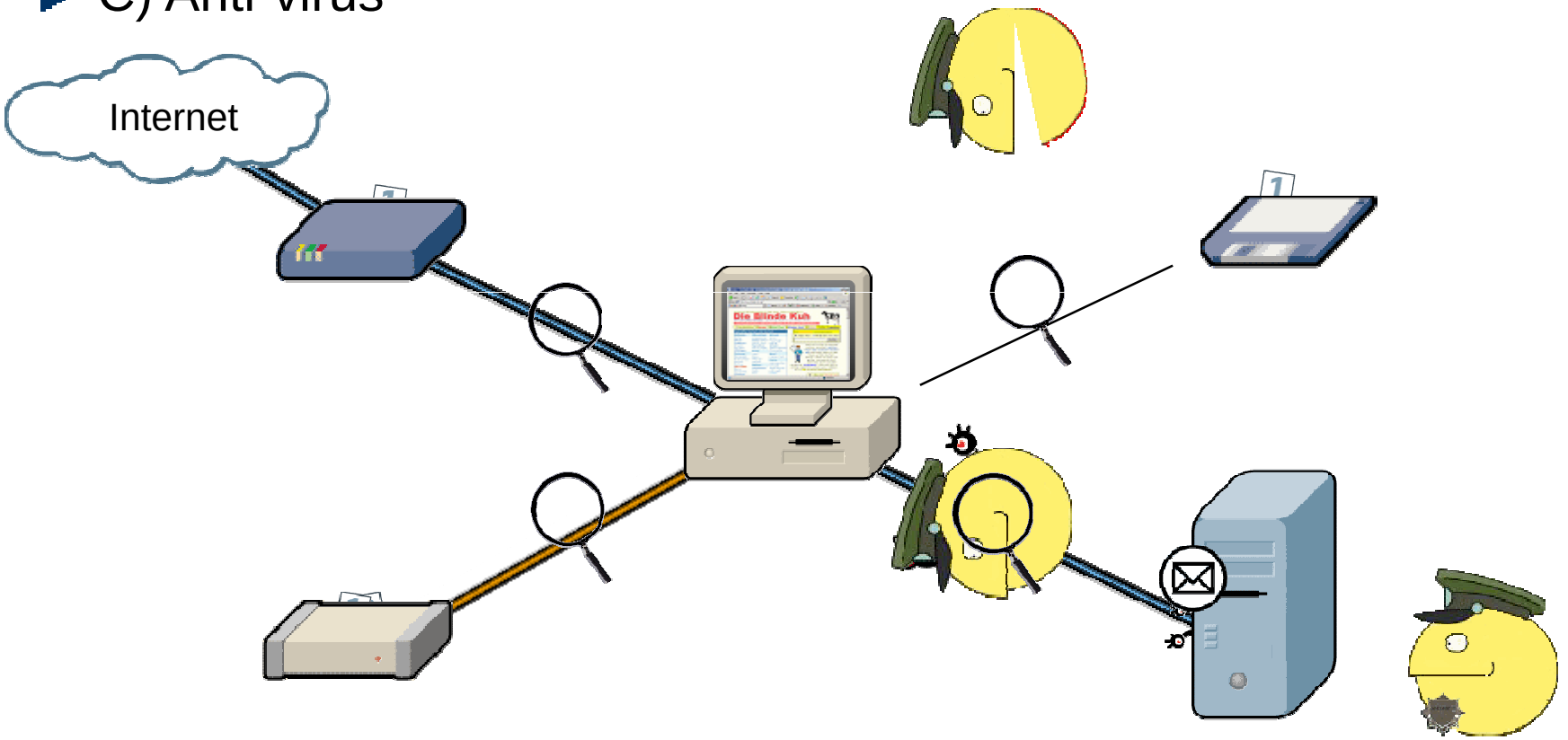


LE GOUVERNEMENT
du Grand-Duché de Luxembourg

Sensibilisation à la Sécurité Informatique

3) Comment me protéger ?

- C) Anti-virus



LE GOUVERNEMENT
du Grand-Duché de Luxembourg

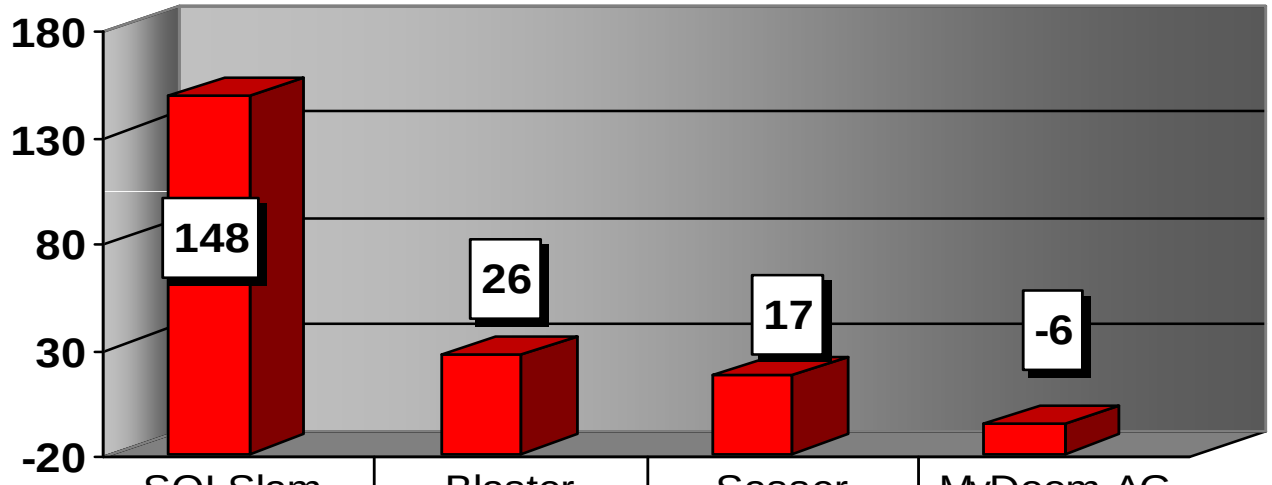
C) Anti-virus

- Un Anti-virus est un logiciel capable de rechercher, d'identifier et de supprimer les virus et autres codes malicieux qu'il connaît. Il recherche des caractéristiques de virus connus dans les fichiers et peut réussir à découvrir de nouveaux virus.

Points importants :

- Installez un Anti-virus.
- Mettez-le à jour **régulièrement**.
- Recherche de virus complète une fois par mois.
- Faites des **back-up réguliers**.

- C) Anti-virus – Pourquoi le mettre à jour régulièrement



	SQLSlam.	Blaster	Sasser	MyDoom.AG
Jours	148	26	17	-6
Découvert	24.01.2003	12.08.2003	30.04.2004	08.11.2004

Sensibilisation à la Sécurité Informatique

3) Comment me protéger ?

- C) Anti-virus – Pourquoi le mettre à jour régulièrement

Fri 23.1.2004:	Bagle.A	Wed 10.3.2004:	Netsky.L
Tue 27.1.2004:	Mydoom.A	Thu 11.3.2004:	Netsky.M
Mon 16.2.2004:	Netsky.A	Tue 11.3.2004:	Bagle.M
Mon 16.2.2004:	Mydoom.E	Thu 13.3.2004:	Bagle.N
Tue 17.2.2004:	Bagle.B	Thu 13.3.2004:	Bagle.O
Wed 18.2.2004:	Netsky.B	Sat 15.3.2004:	Bagle.P
Tue 24.2.2004:	Mydoom.F	Mon 17.3.2004:	Netsky.O
Wed 25.2.2004:	Netsky.C	Tue 18.3.2004:	Bagle.Q
Fri 27.2.2004:	Bagle.C	Thu 18.3.2004:	Bagle.R
Sat 28.2.2004:	Bagle.D	Thu 18.3.2004:	Bagle.S
Sat 28.2.2004:	Bagle.E	Thu 18.3.2004:	Bagle.T
Sun 29.2.2004:	Netsky.D	Sun 21.3.2004:	Netsky.P
Mon 1.3.2004:	Bagle.F	Fri 26.3.2004:	Bagle.U
Mon 1.3.2004:	Bagle.G	Mon 29.3.2004:	Bagle.V
Mon 1.3.2004:	Netsky.E	Mon 29.3.2004:	Netsky.Q
Tue 2.3.2004:	Bagle.H	Wed 31.3.2004:	Netsky.R
Tue 2.3.2004:	Bagle.I	Mon 5.4.2004:	Netsky.S
Tue 2.3.2004:	Netsky.F	Mon 5.4.2004:	Bagle.W
Tue 2.3.2004:	Bagle.J	Tue 6.4.2004:	Netsky.T
Wed 3.3.2004:	Mydoom.G	Thu 8.4.2004:	Netsky.U
Wed 3.3.2004:	Bagle.K	Tue 13.4.2004:	Mydoom.I
Wed 3.3.2004:	Mydoom.H	Thu 15.4.2004:	Netsky.V
Thu 4.3.2004:	Netsky.G	Fri 16.4.2004:	Netsky.W
Fri 5.3.2004:	Netsky.H	Fri 16.4.2004:	Mydoom.J
Sun 7.3.2004:	Netsky.I	Mon 19.4.2004:	Bagle.X
Mon 8.3.2004:	Netsky.J	Tue 20.4.2004:	Netsky.X
Mon 8.3.2004:	Netsky.K	Tue 20.4.2004:	Netsky.Y
Tue 9.3.2004:	Bagle.L	Wed 21.4.2004:	Netsky.Z

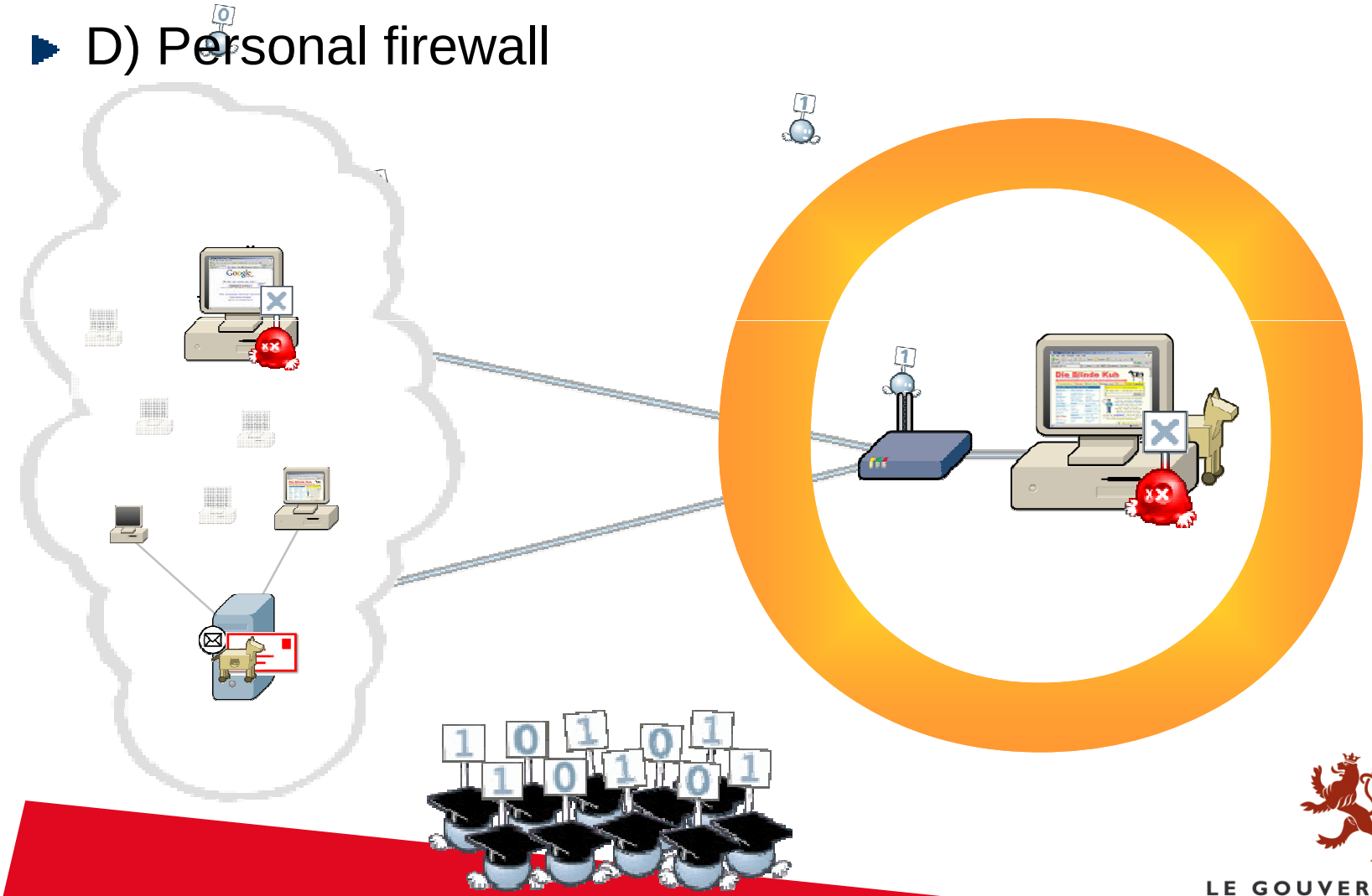
© F-Secure

LE GOUVERNEMENT
du Grand-Duché de Luxembourg

Sensibilisation à la Sécurité Informatique

3) Comment me protéger ?

- D) Personal firewall

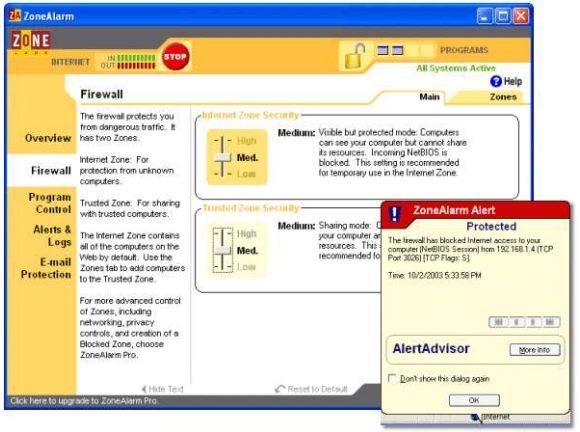


LE GOUVERNEMENT
du Grand-Duché de Luxembourg

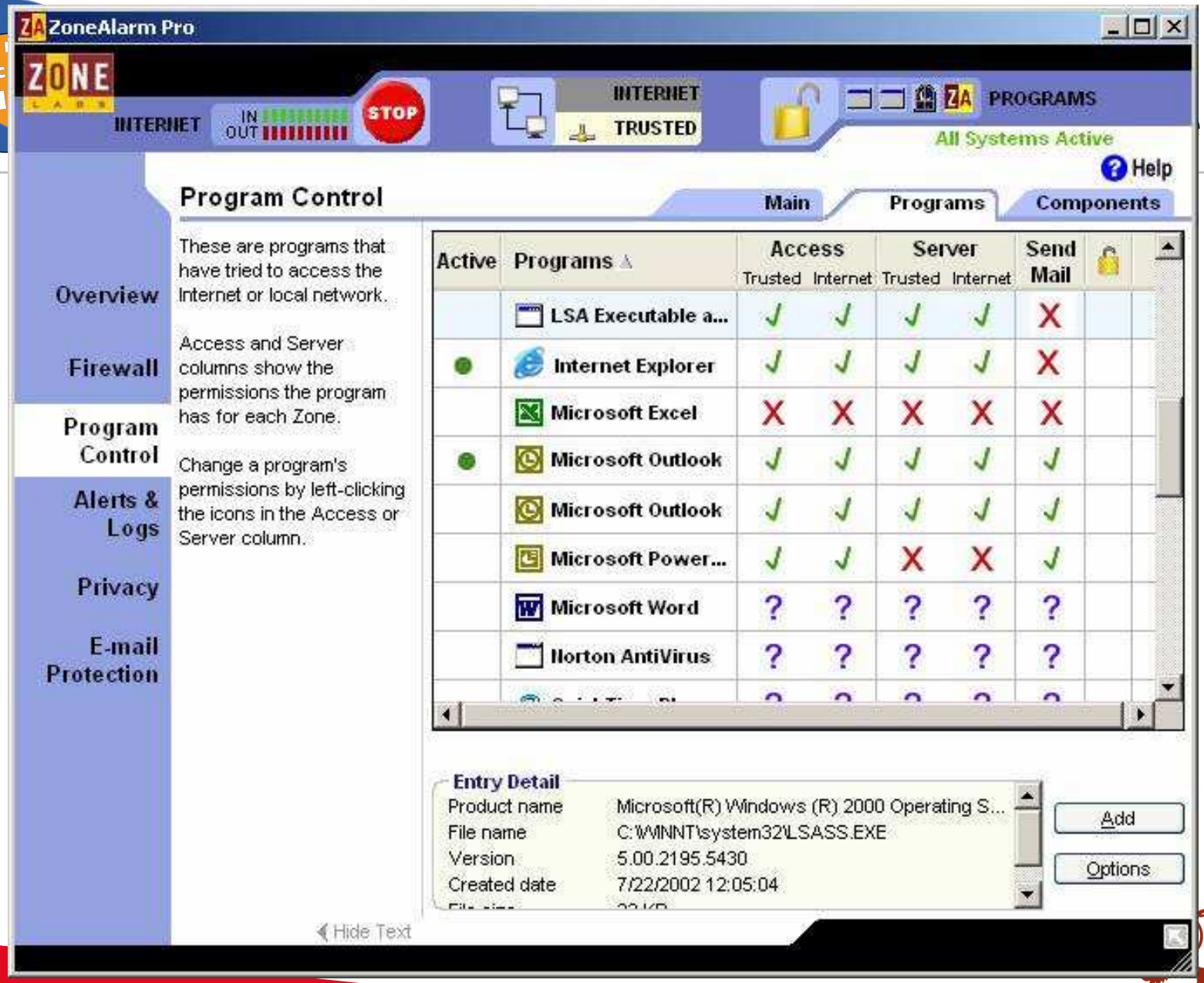
D) Personal firewall: Installation et configuration ?

- Un Personal firewall est un logiciel qui forme une barrière impénétrable autours de l'ordinateur :
  1. Système proactif/réactif avec fonctions additionnelles.
  2. Permets de contrôler les accès Internet de programmes spécifiques.
  3. Fonctions additionnelles : Filtre de processus, Anti-Spam etc.

- Existent comme Freeware :
  - Zone Alarm
  - Sygate Peronal Firewall
  - Kerio Personal firewall



- Comment faire :
  http://www.cases.public.lu/
  Publications → Fiches thématiques → Firewall


ZoneAlarm Pro
ZONE LABS
INTERNET
IN
OUT
STOP
INTERNET
TRUSTED
PROGRAMS
All Systems Active
Help
Program Control
Main
Programs
Components
Overview
Firewall
Program Control
Alerts & Logs
Privacy
E-mail Protection
These are programs that have tried to access the Internet or local network.
Access and Server columns show the permissions the program has for each Zone.
Change a program's permissions by left-clicking the icons in the Access or Server column.
Active
Programs
Access
Trusted
Internet
Server
Trusted
Internet
Send Mail
LSA Executable a...
Internet Explorer
Microsoft Excel
Microsoft Outlook
Microsoft Outlook
Microsoft Power...
Microsoft Word
Norton AntiVirus
Entry Detail
Product name
Microsoft(R) Windows (R) 2000 Operating S...
File name
C:\WINNT\system32\LSASS.EXE
Version
5.00.2195.5430
Created date
7/22/2002 12:05:04
Add
Options
Hide Text

- Questionnaire - Protections

Grand quiz www.mysecureit.lu

Si vous fermez cette fenêtre, toutes vos réponses seront perdues. **Session démarrée à 23:14:31**

Quelle est la raison principale pour laquelle il faut mettre à jour un anti-virus? [4/10]

- L'anti-virus a des problèmes à détecter les virus qu'il ne connaît pas.
- L'anti-virus a une date de validité au-delà de laquelle il ne fonctionne plus.
- Les mises à jour permettent de profiter de versions plus rapides de l'anti-virus.

Pourquoi faut-il toujours utiliser un firewall avec un anti-virus? [11/11]

- Le firewall ne fonctionne pas sans anti-virus et vice-versa.
- L'anti-virus a besoin du firewall pour accéder à un certain type de fichiers.
- L'anti-virus détecte des virus et des vers alors que le firewall ne peut pas scanner un disque dur pour les trouver.

Continuer

Que fait-il ?

- **Hacker (Whitehat)**

  Chercheurs de failles, publient les failles trouvées, tests intrusifs. Leur but: Améliorer la sécurité.

- **Cracker (Blackhat)**

  Ils s'introduisent de manière illégale dans des systèmes divers. Leur but : Argent, nuire, chaos.

- **Script Kiddie**

  Pas de compétences informatiques particulières, utilisent des programmes de tiers pour compromettre un système quelconque; ils sont souvent très jeunes.

- **Bully**

  Agresse des personnes (souvent faibles) sur Internet (Cyberbulying)

Sensibilisation à la Sécurité Informatique

4) Pourquoi ne pas devenir cracker ou bully ?

- Contexte légal :
  - Au Luxembourg :
    - Article 509.1: Accès frauduleux et suppressions et modifications involontaires. (2 mois-3 ans & < 25.000€)
    - Article 509.2: Entrave et faussement d'un Système. (3 mois & 1250€- 12500€)
    - Article 509.3: Introduction et modification de données.(3 mois & 1250€-12500€)
    - Article 509.6: Toute tentative est punie de la même façon que le crime lui - même!
  - Condamnations Internationales :

[**CA**] Pour déni de service (eBay,Yahoo,CNN): Agé de **16 ans**, condamné à 1 an de prison.

[**US**] Création de vers et déni de service : Agé de **14 ans**, condamné à 3 ans de prison.

[**US**] Créateur du vers W32.Blaster: Agé de **19 ans**, 1+1/2 an de prison).

[**ES**] Créateur d'un cheval de Troie : Agé de **26 ans** condamné à 2 ans de prison plus dommages et intérêts.

Les victimes du Cyberbullying

- Pertent confiance en soi
- Souvent seuls dans leur douleur, se sentent rejeté de leur entourage
- Se voient ridiculisés devant tout le monde
- Peuvent aussi devenir Bully ou peuvent songer au suicid

Donc:

- Ne devenez pas coupable de la douleur d'autrui !
- Ne souffrez pas seuls (Demander de l'aide à vos parents, vos amis, votre école, ou la Helpline Jugend- a Kannertelephon (Tel.12345) !
- Aidez les victimes impuissants de s'aider !

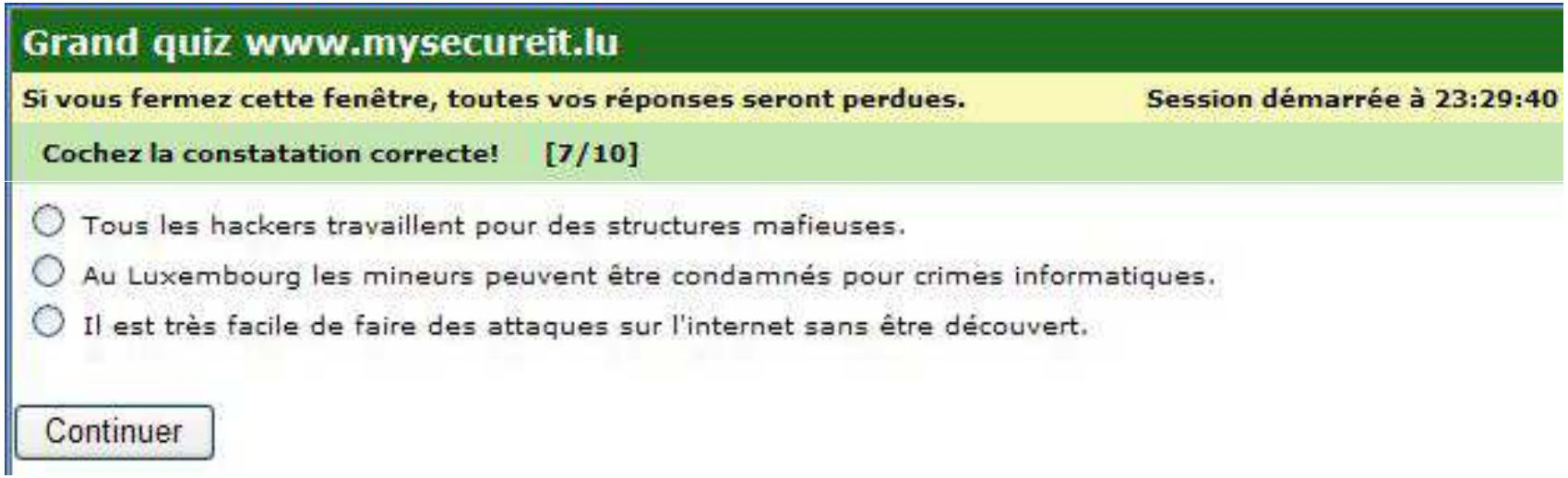
Battre les faibles n'est pas héroïque,

agresser de façon cachée n'est pas courageux !

Sensibilisation à la Sécurité Informatique

4) Pourquoi ne pas devenir cracker ou bully ?

- Questionnaire



LE GOUVERNEMENT
du Grand-Duché de Luxembourg

5) Qu'est-ce qu'il faut retenir ?

1) La sécurité concerne **tous** les utilisateurs.
2) Connaissez les **menaces** : virus, vers, cheval de Troie, phishing, ...
3) Soyez **vigilants** et utilisez des **contre-mesures**.
   - **anti-virus** et mise à jour régulièrement.
   - **firewall** et configuration correcte.
   - **backups** réguliers.
   - activation de la fontion « **Automatic update** » de Windows.
   - **Limiter vos droits**.

↳ **Utilisez Internet avec une méfiance saine.**

LE GOUVERNEMENT
du Grand-Duché de Luxembourg

mySecureIT

Retrouvez plus d'informations sur :
http://www.cases.lu , http://www.mySchool.lu
ou bien au numéro 478 5900