

# Sécurité Internet

# Objectifs

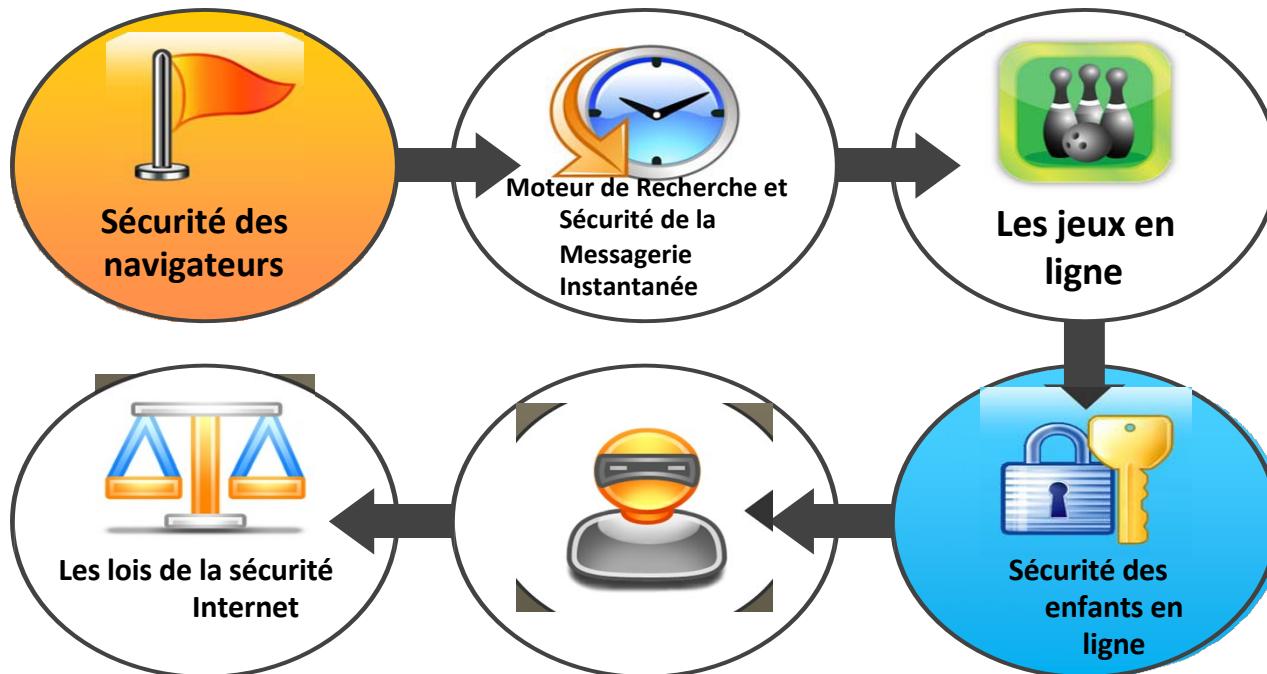
- Sécurité Internet
- Paramètres de Sécurité d'Internet Explorer
- Paramètres de Sécurité Mozilla Firefox
- Paramètres de Sécurité Google Chrome
- Paramètres de Sécurité Apple Safari
- Messagerie Instantanée (IMing)
- Recherche sur le Web
- Jeux en ligne et MMORPG



- Les risques de jeu en ligne
- Pratiques de sécurité spécifiques aux jeux en ligne des enfants
- Rôle d'Internet dans la pornographie infantile
- Protéger les enfants contre les menaces en ligne
- Comment signaler un crime?
- Lois de Sécurité Internet
- Listes de contrôle de sécurité Internet



# PLAN



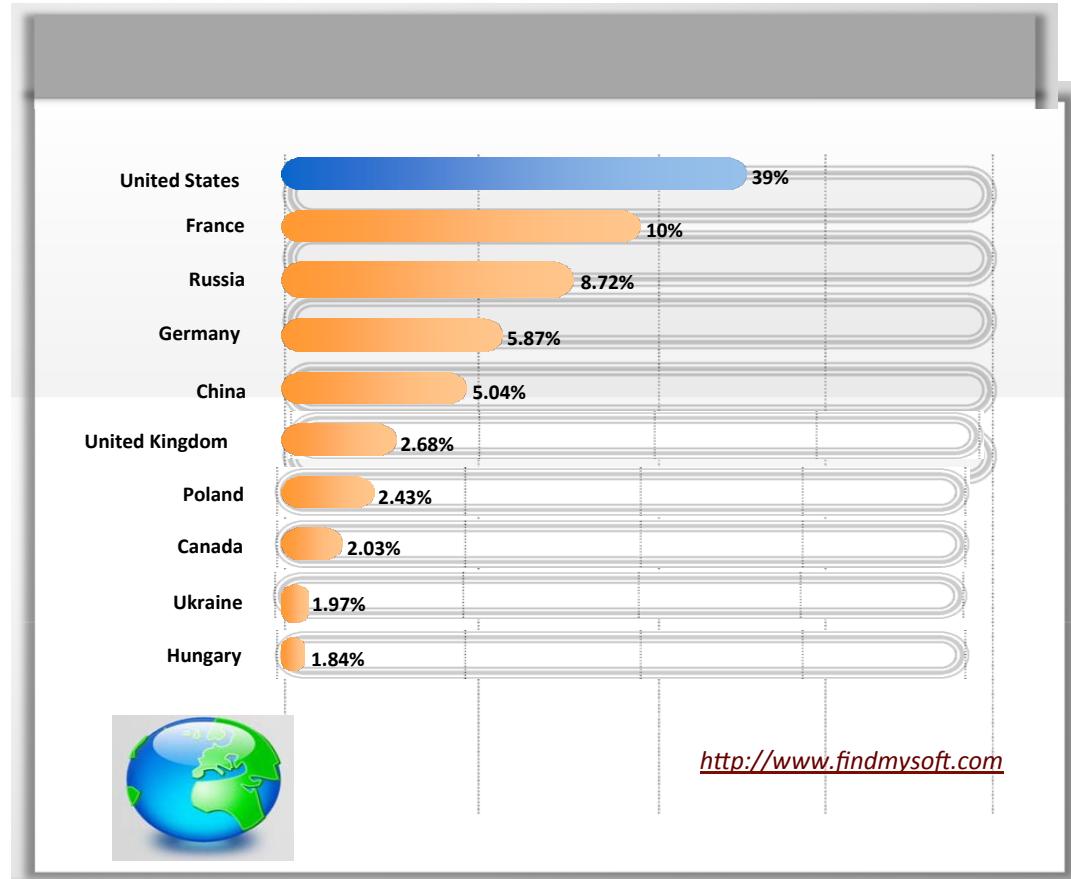
# Sécurité Internet

La sécurité Internet implique:

- La protection les données des utilisateurs contre les accès non autorisés et les dommage quand ils sont connectés à Internet
- Une bonne configuration du navigateur qui permet d'éviter les programmes malveillants, de protéger les informations personnelles, et de prévenir ou de limiter les dégats d'une cyberattaque.

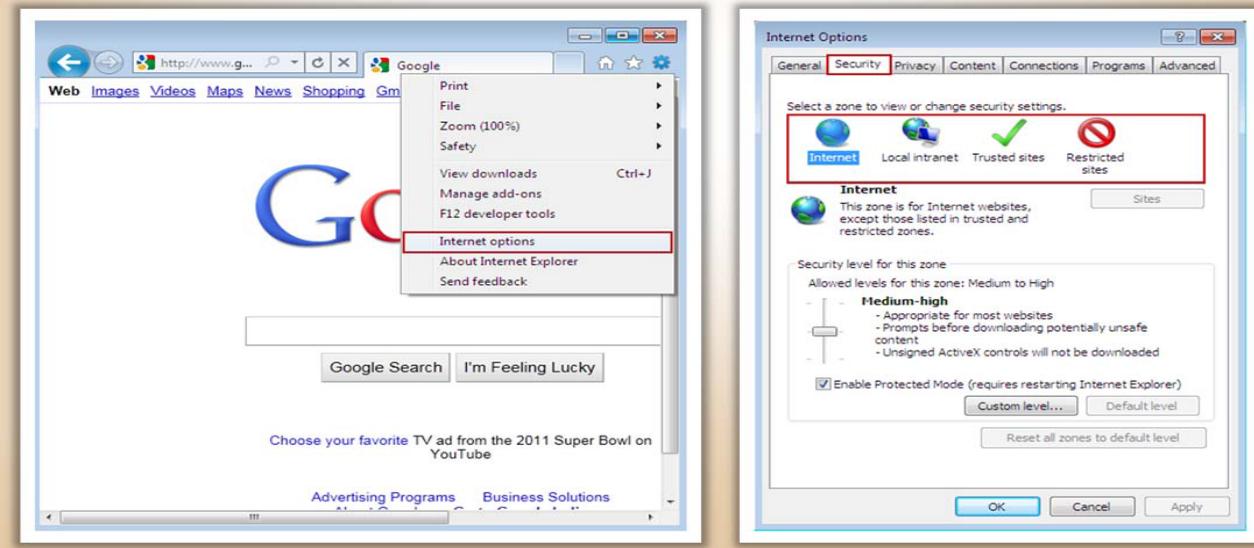
Les sources d'attaque en ligne:

- Emails
- Messagerie instantanée
- Chat rooms
- Partage de fichiers et téléchargement

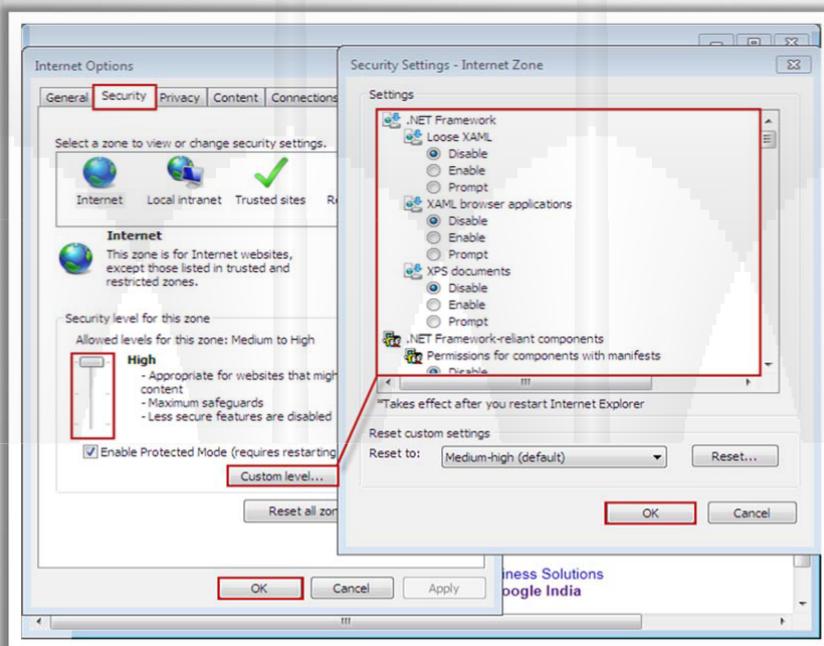


# Paramètres de Sécurité Internet Explorer

- Exécuter Internet Explorer, cliquer **Outils**, et sélectionné **Options Internet**
- Sélectionner l'onglet **Sécurité**, qui affiche les sites web classés en quatre zones :
- 1. Internet 2. Intranet Local 3. Sites de confiance 4. les sites sensibles.



# Paramètres de Sécurité Internet Explorer : Zone Internet



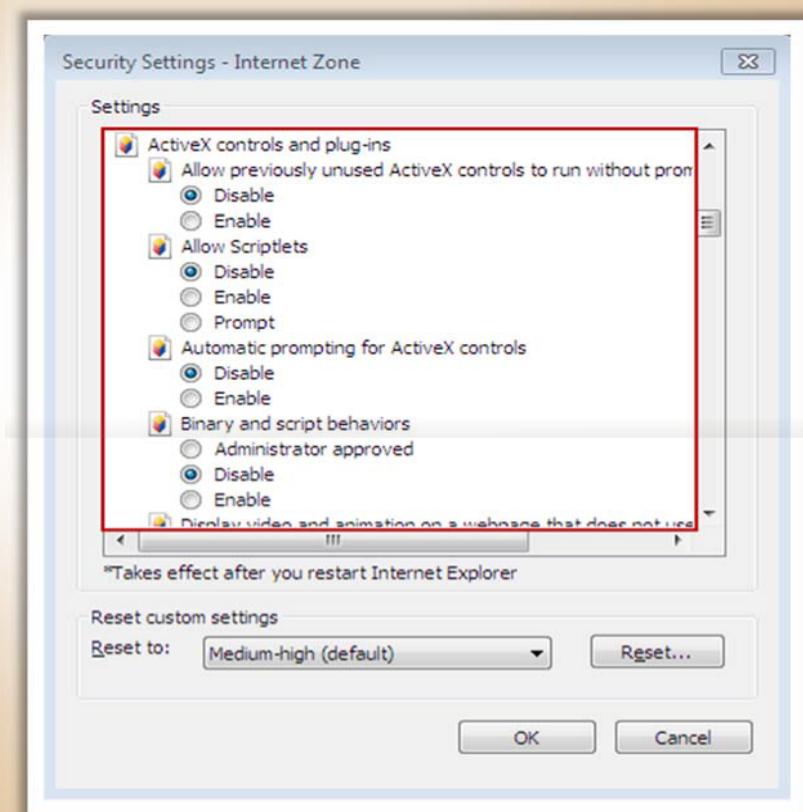
- La Zone Internet est réservée à tous les sites Internet exceptés ceux qui sont listés dans la **Zone de confiance ou de restriction Internet**

Cliquer sur **Personnaliser le niveau** pour définir les paramètres de sécurité de la zone Internet

- Activer ou désactiver les options requises
- Déplacez le curseur pour modifier le niveau de sécurité
- Définissez le niveau de sécurité à **haut** pour assurer une plus grande sécurité
- Le maintien du niveau de sécurité plus élevé peut dégrader les performances du navigateur
- Cliquez sur **OK** pour appliquer les paramètres

# Paramètres sécurité d'Internet Explorer: les contrôles ActiveX

- Les contrôles ActiveX sont de petits programmes qui fonctionnent sur Internet via le navigateur
- Ils comprennent des applications personnalisées qui sont nécessaires pour recueillir des données, voir les fichiers sélectionnés et exécuter des animations lorsque les utilisateurs visitent des sites web
- les Programmes malveillants sont téléchargés sur le système de l'utilisateur grâce à des contrôles ActiveX quand il visite les sites Web malveillants
- **Désactiver** les **contrôles ActiveX et les options plug-in** dans la fenêtre **Paramètres de sécurité**
- Activer la demande de confirmation pour l'option **des contrôles ActiveX** afin que le navigateur demande quand il y a une exigence de **contrôles ActiveX et les plug-ins** de pouvoir les activer
- Cliquer **OK** pour appliquer les paramètres

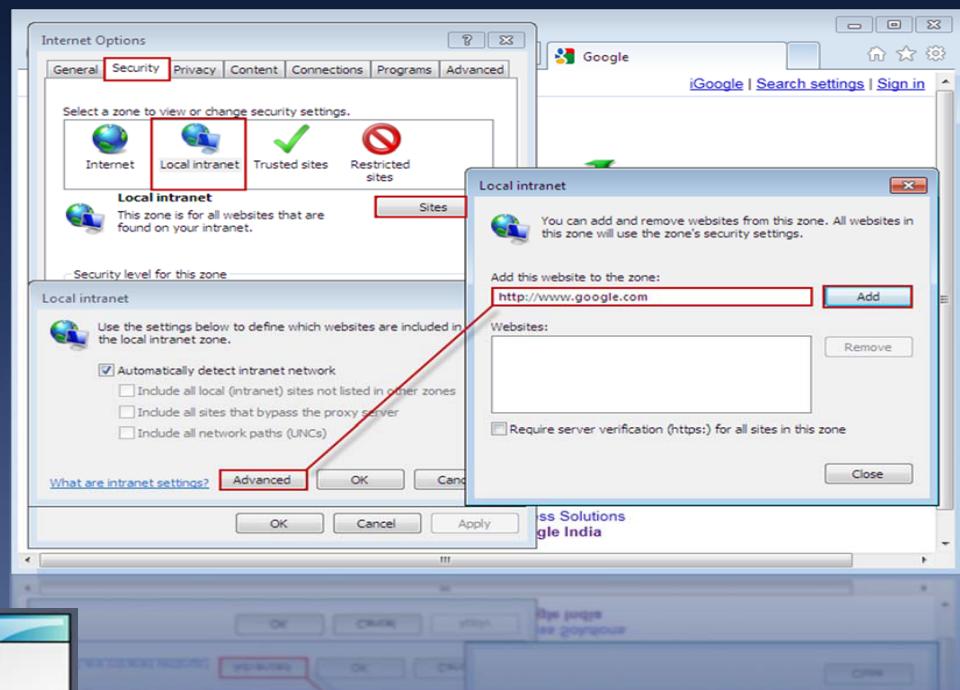


# Paramètres sécurité d'Internet

## Explorer: Zone Intranet Local

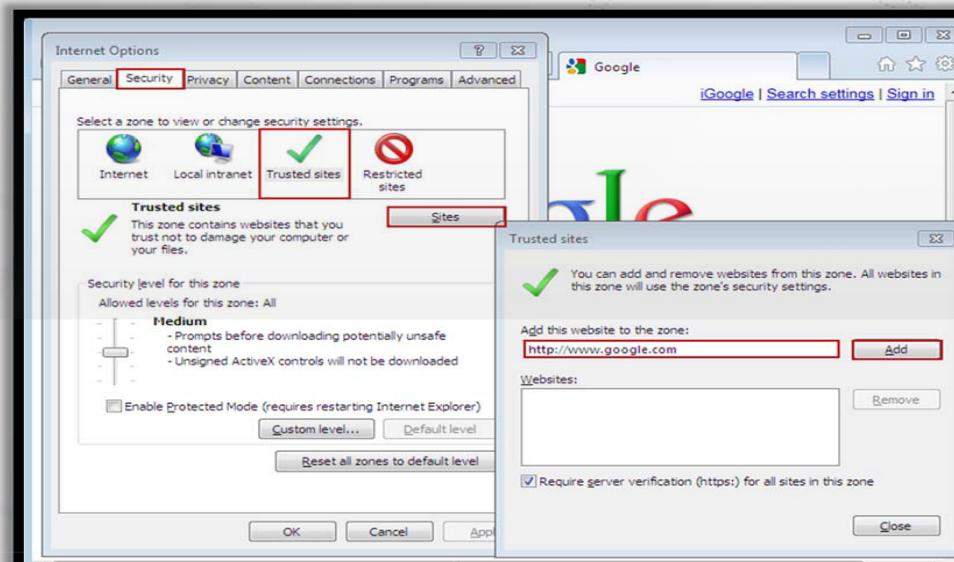
- Zone **Intranet local** couvre les sites intranet
- Étapes à suivre pour ajouter des sites Web à la zone Intranet local
- Sélectionner **Sécurité** → **Intranet Local**

- Cliquer **Sites**
- Cliquer le bouton **Avancé**
- Entrer l' URL dans **Ajouter ce site Web à la zone**
- Cliquer **Ajouter**
- Cliquer **OK** pour appliquer les paramètres



# Paramètres sécurité d'Internet Explorer:

## Zone Sites de confiance



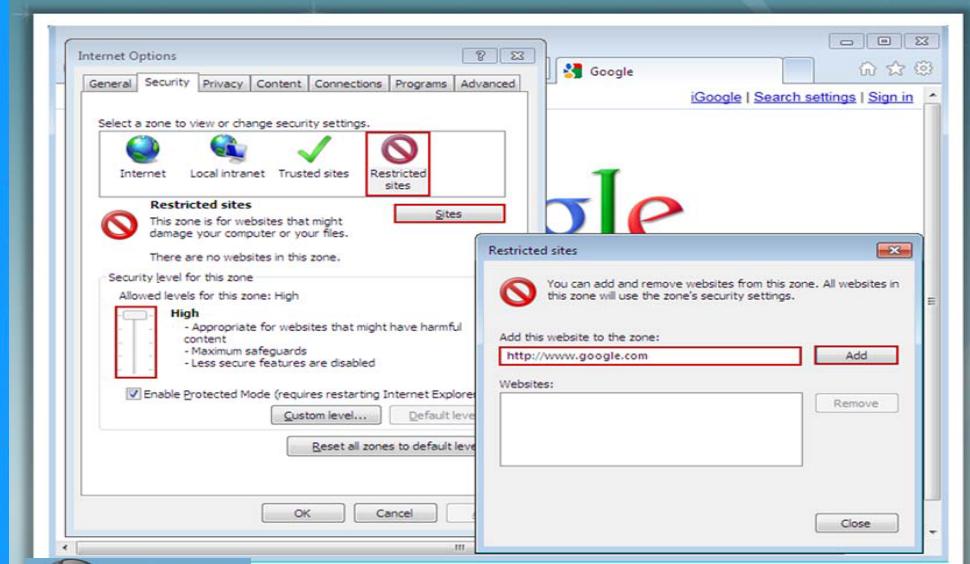
La zone **Sites de confiance** contient les sites que les utilisateurs croient ne pas pouvoir endommager leurs ordinateurs ou de données

- Sélectionner **Sécurité** → **Sites de confiance**
- Cliquer le bouton **Sites**
- Entrer Entrer l' URL dans **Ajouter ce site Web à la zone**
- Cliquer **Ajouter**
- Cliquer **OK** pour appliquer les paramètres

# Paramètres de sécurité d'Internet Explorer: Zone sites sensibles

La zone **Sites sensibles** restreint l'accès aux sites Web qui pourraient causer des dommages à un ordinateur  
Pour ajouter des sites Web à la zone **Sites sensibles** :

- Sélectionnez l'onglet **Sécurité** et Cliquez sur **Sites sensibles**  
Cliquez sur le bouton **Sites**
- Entrez l'URL du site dans la zone Ajouter ce site web à la zone : pour restreindre l'accès
- Cliquez sur **Ajouter**, puis cliquez sur **OK** pour **appliquer** les paramètres



# Comprendre les cookies

- Un cookie est **une information qui est fournie par un serveur Web au navigateur Web**, puis renvoyée inchangée par le navigateur chaque fois qu'il accède à ce serveur ;
- Lorsque le site est **revisité**, le navigateur renvoie l'information à ce dernier pour l'aider à reconnaître l'utilisateur ;
- Cette activité est transparente pour l'utilisateur et est généralement destinée à **améliorer** l'expérience de navigation Web (par exemple, dans une boutique en ligne)



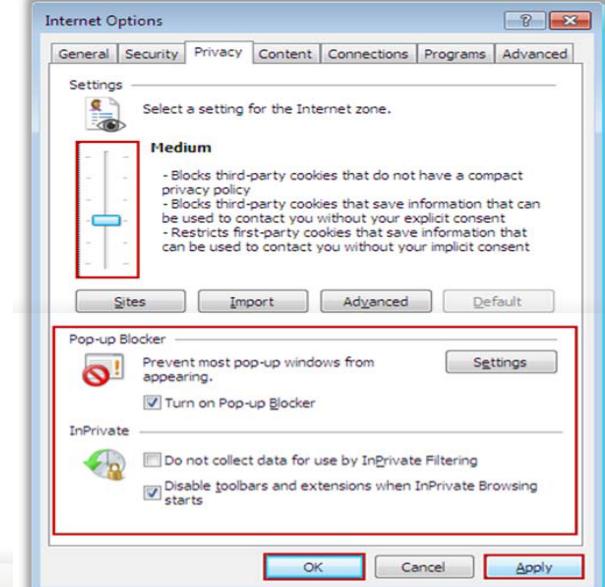
# Internet Explorer Paramètres de confidentialité

L'utilisateur peut limiter l'information qui est stockée dans un cookie

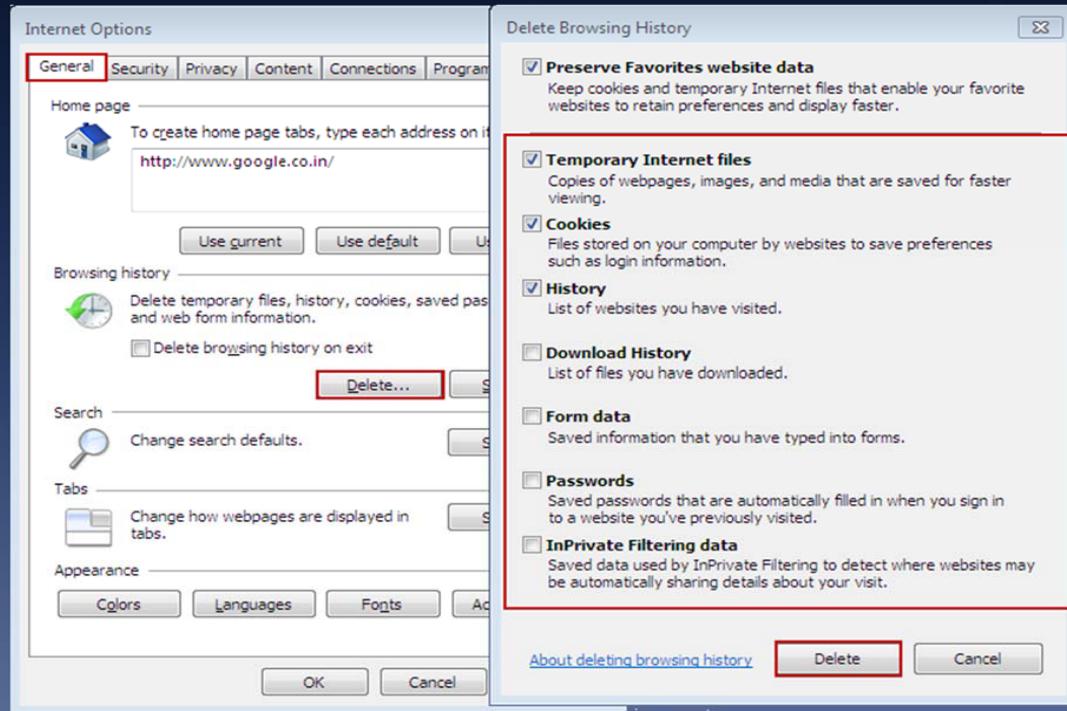
Un cookie n'est qu'un fichier texte et ne peut pas porter de virus

Pour configurer les paramètres des cookies:

- Choisir **options Internet, Sélectionner** l'onglet **Confidentialité** et définir bas, moyen et bas
- Bloquer tout ou accepter tous les cookies en fonction de l'exigence  
Vérifiez la **Activez le bloqueur de fenêtres publicitaires** pour bloquer les pop-ups qui apparaissent tout en visitant certains sites Web



# Supprimer l'historique de Navigation



1. Choisissez **Options Internet** dans le menu **Outils** dans le navigateur
2. Aller à la section **l'historique de navigation**
3. Cocher les options souhaitées dans la boîte de dialogue **Supprimer l'historique de navigation**
4. Cliquez sur Supprimer pour supprimer **l'historique de navigation**



# Ne laissez pas le navigateur mémoriser un mot de passe

Internet Explorer Autocomplete Password prompt  
Invite Mot de passe Autocomplete Internet Explorer

Invite de mémorisation de Mot de Passe de Firefox

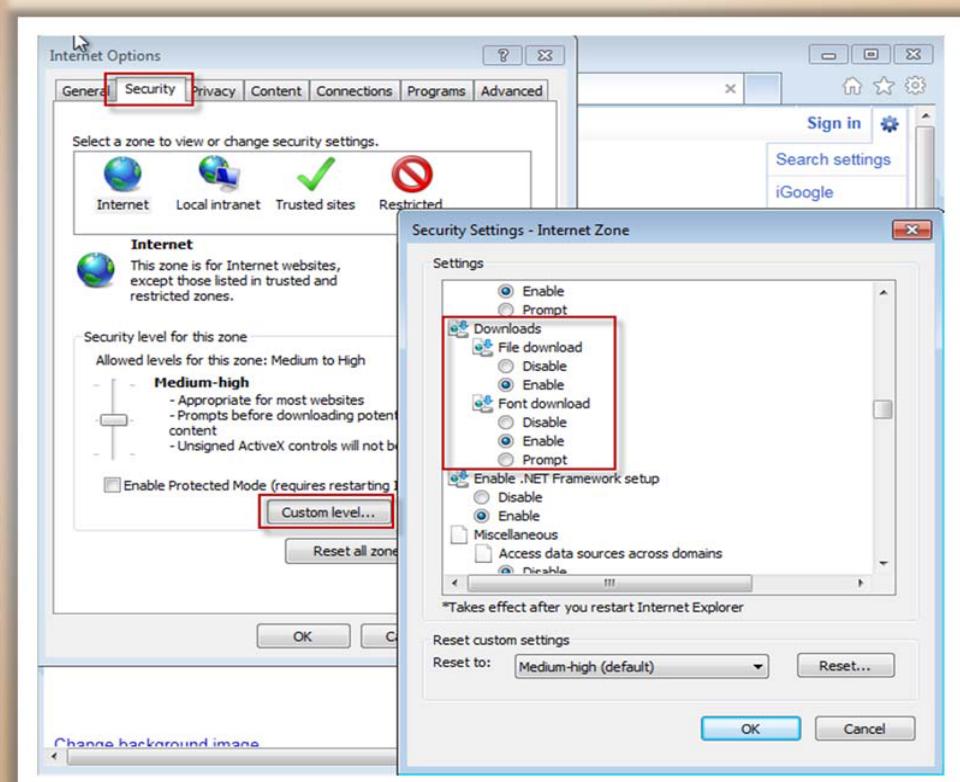
# Sécuriser le Téléchargement de Fichiers

Pour configurer les paramètres de téléchargement d'Internet Explorer, accédez à **Outils** → **Options Internet** → allez à l'onglet **Sécurité**

Cliquez sur le bouton **Personnaliser le niveau** dans la fenêtre Paramètres de sécurité

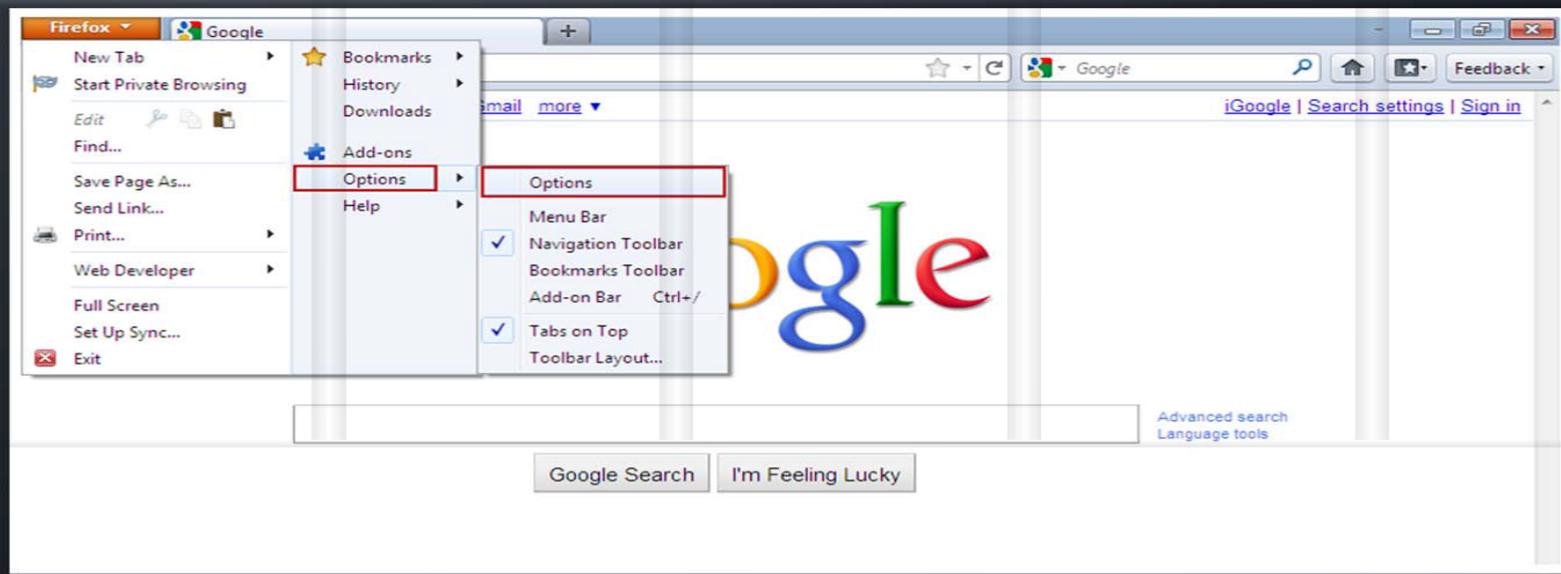
Dans le menu **Téléchargements** Activer la demande de confirmation pour les téléchargements automatiques de fichiers

Cliquez sur **OK** pour enregistrer les paramètres

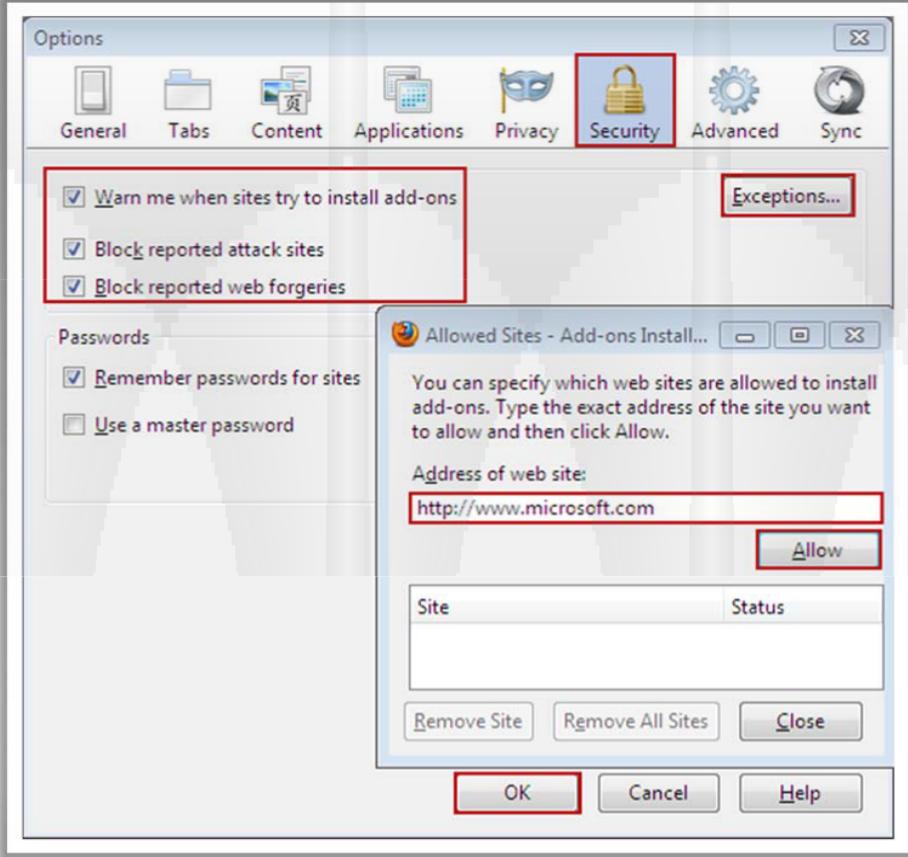


# Mozilla Firefox: Paramètres de sécurité

- Lancez le navigateur **Mozilla Firefox**
- Cliquez sur le menu **Outils** et sélectionnez **Options**



# Mozilla Firefox: Paramètres de sécurité



- Sélectionner **Sécurité** dans la fenêtre **Options**
- Cochez l'option **Prévenir lorsque les sites essaient d'installer des modules complémentaires** afin pour que le navigateur nous demande avant d'installer ces modules
- Cliquez sur le bouton **Exceptions** et entrez l'URL dans la zone **Adresse du site Web** et cliquez sur **Autoriser** pour spécifier les sites Web qui sont autorisés à installer des modules
- Cochez l'option **Bloquer les sites signalés comme étant des sites d'attaque afin** d'éviter de visiter les sites Web malveillants
- Cochez l'option **Bloquer les sites signalés comme étant des contrefaçons** pour éviter que les sites visités tentent de voler des informations personnelles
- N'oubliez pas de décocher **enregistrer les mots de passe** pour empêcher le navigateur de se souvenir des mots de passe pour les pages de connexion visités

# Mozilla Firefox: Paramètres de confidentialité

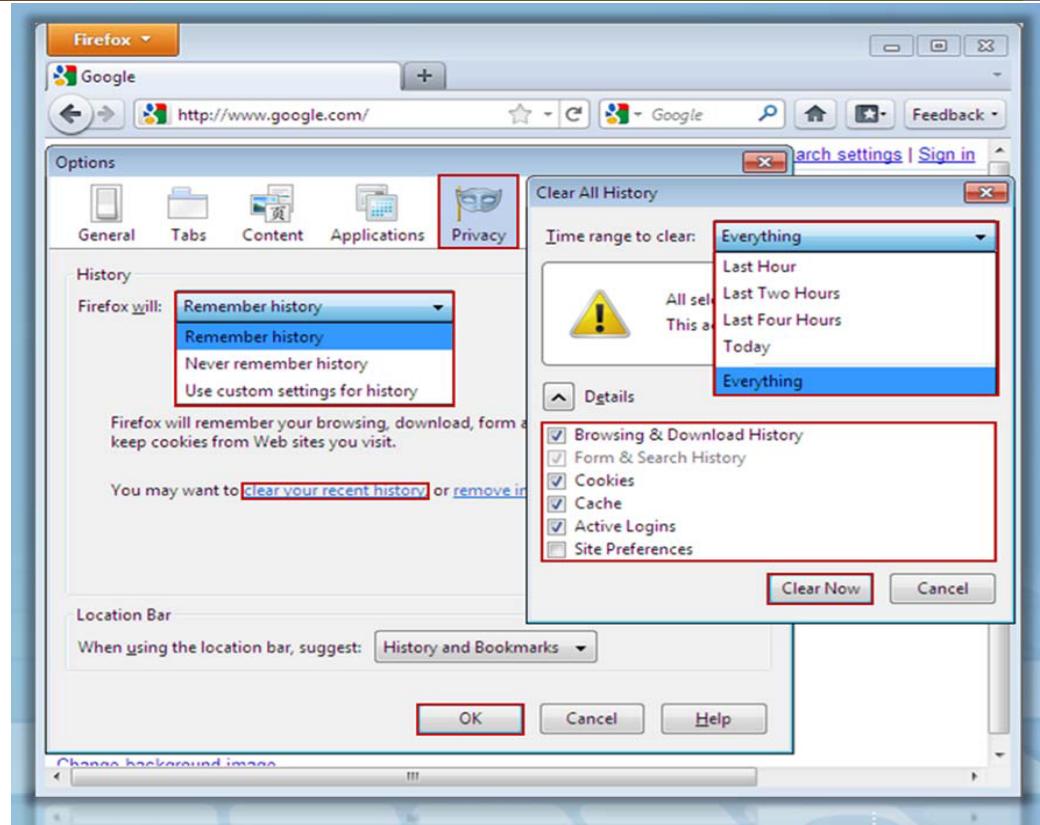
Selectionnez **vie privée** dans la fenêtre Options

L'utilisateur peut choisir si Firefox doit se souvenir de l'historique de navigation

Cliquez Cliquez **effacer votre historique récent**

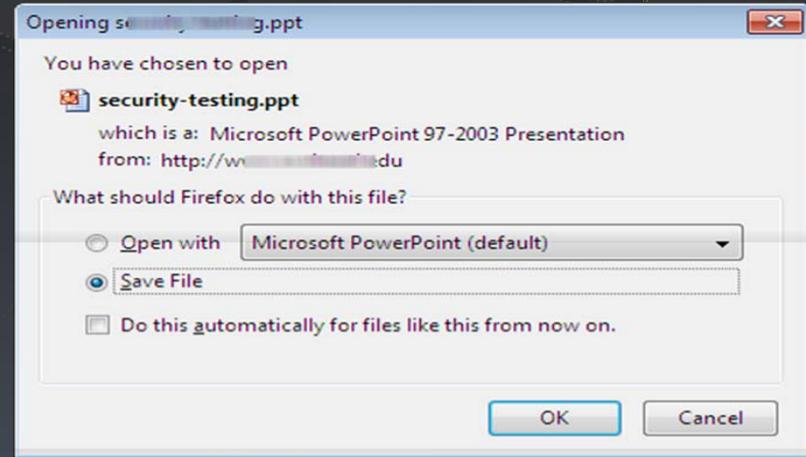
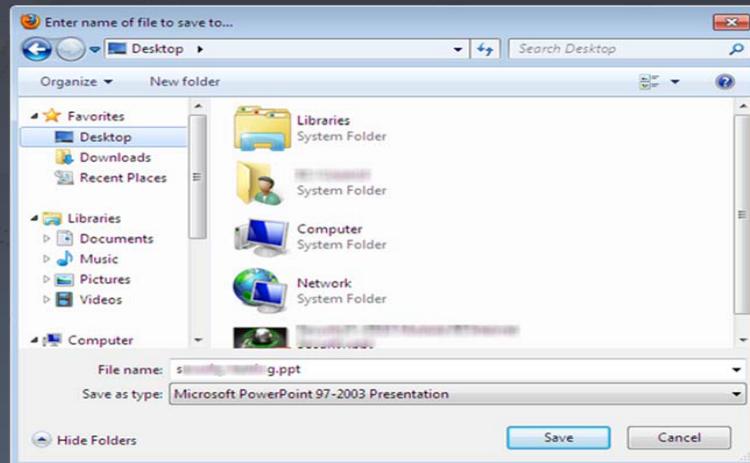
Sélectionnez **l'intervalle de temps** pour supprimer l'historique

Vérifiez les options nécessaires pour effacer l'historique et cliquez sur Effacer **maintenant**



# Sécuriser le Téléchargement de Fichiers

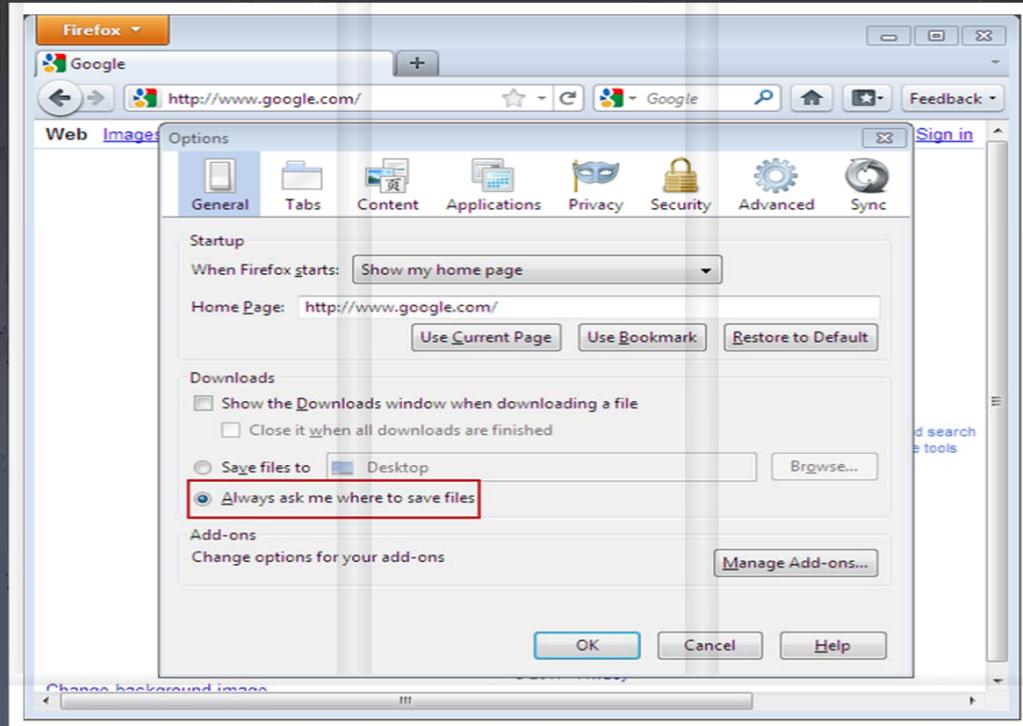
- N'acceptera pas les téléchargements de fichiers de membres inconnus sur Internet
  - Ces téléchargements peuvent contenir des logiciels malveillants qui dégrade les performances de l'ordinateur



- Fichier sont téléchargés par défaut dans Mes Documents → Téléchargements
  - L'utilisateur peut configurer les paramètres du navigateur afin qu'il invite à indiquer l'emplacement pour enregistrer le fichier.



# Sécuriser le Téléchargement de fichiers



- Pour configurer les paramètres de téléchargement de Mozilla Firefox, accédez au **Outils → options** → **Général**
  - Cochez l'option **Toujours demander où enregistrer les fichiers** pour permettre au navigateur de demander avant de télécharger un fichier et de spécifier l'emplacement où il sera téléchargé
  - Le navigateur télécharge directement le fichier à l'emplacement par défaut sans aucune annonce si cette option ne est pas cochée

# Installer les Plugins

1

Le message **d'installation du Plugins manquant** apparaît pendant l'ouverture de certains sites



2

Plug-ins sont nécessaires pour afficher **les fichiers graphiques, ou lire une vidéo** sur une page Web



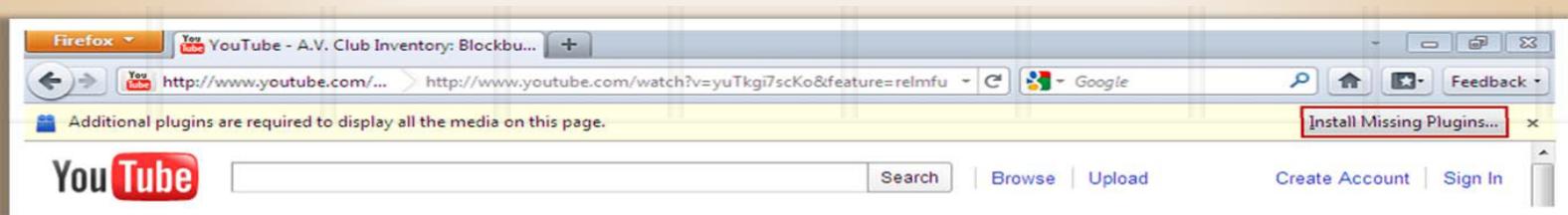
3

Vérifiez si la source de plug-ins manquants est **digne de confiance** ou non



4

Scannez le plug-in téléchargé à l'aide d'un logiciel **antivirus** avant de **l'installer**

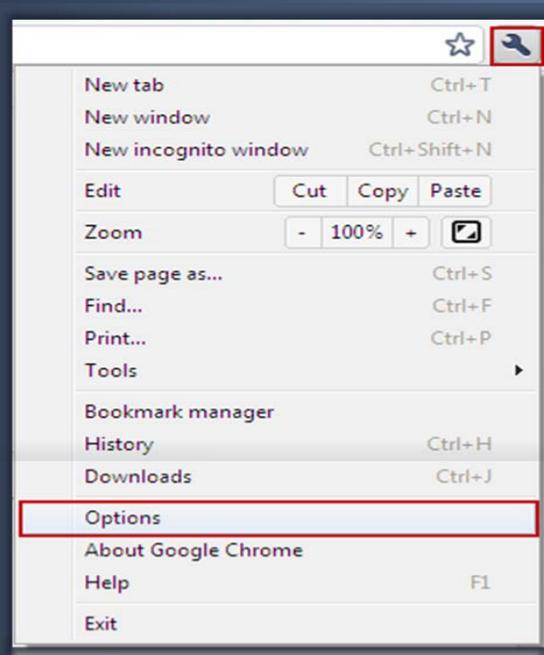


Firefox - YouTube - A.V. Club Inventory: Blockbu...

Additional plugins are required to display all the media on this page.

Install Missing Plugins...

# Google Chrome : Confidentialité et Paramètres de Sécurité



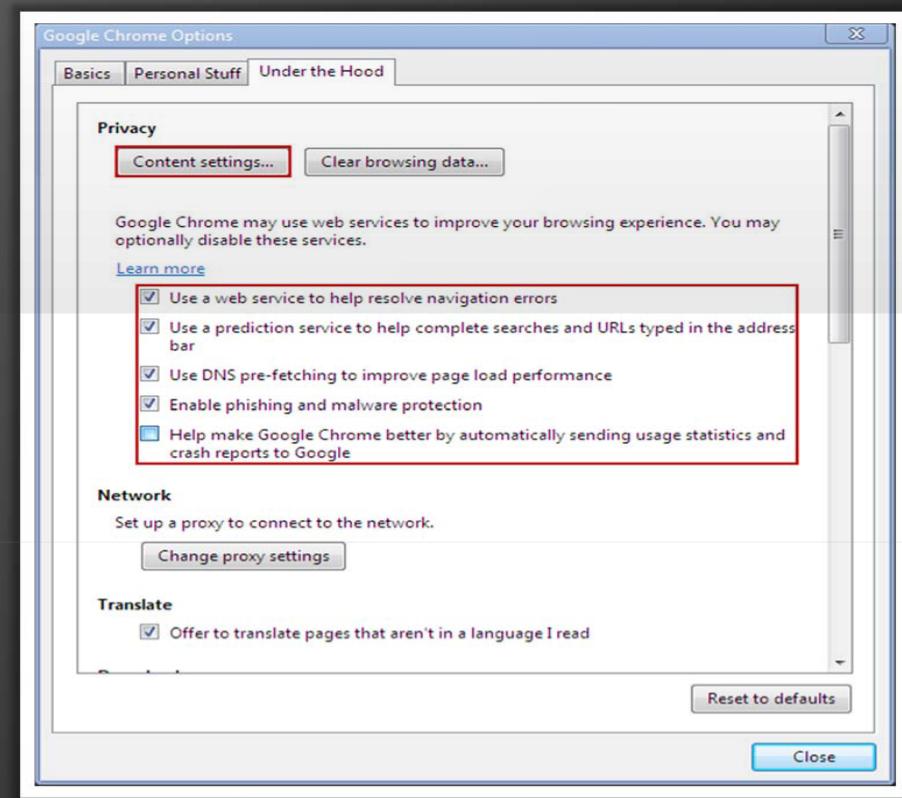
Lancer **Google Chrome**

Cliquer sur l'icône , puis  
Sélectionner **Options**

# Google Chrome: Paramètres de confidentialité



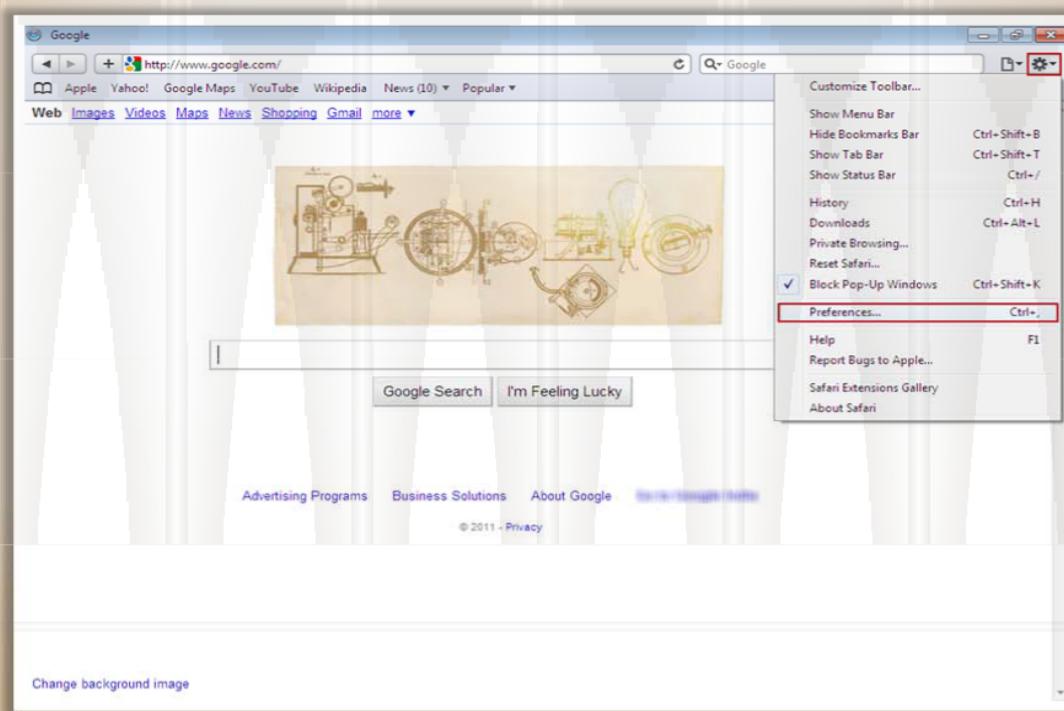
- Cliquez sur l'onglet paramètres avancés dans la fenêtre paramètres de Google Chrome  
**Sous Confidentialité**, vérifiez les services web souhaités
- Cochez l'option **Prédire les actions du réseau pour améliorer les performances de changement des pages**
  - Lorsque l'utilisateur visite une page Web, Google Chrome peut rechercher ou pré-rechercher les adresses IP de tous les liens sur la page WebCheck
- Cochez **Activer la protection contre l'hameçonnage et les logiciels malveillants** pour empêcher le navigateur d'ouvrir des sites Web malveillants



# Apple Safari: Paramètres de sécurité

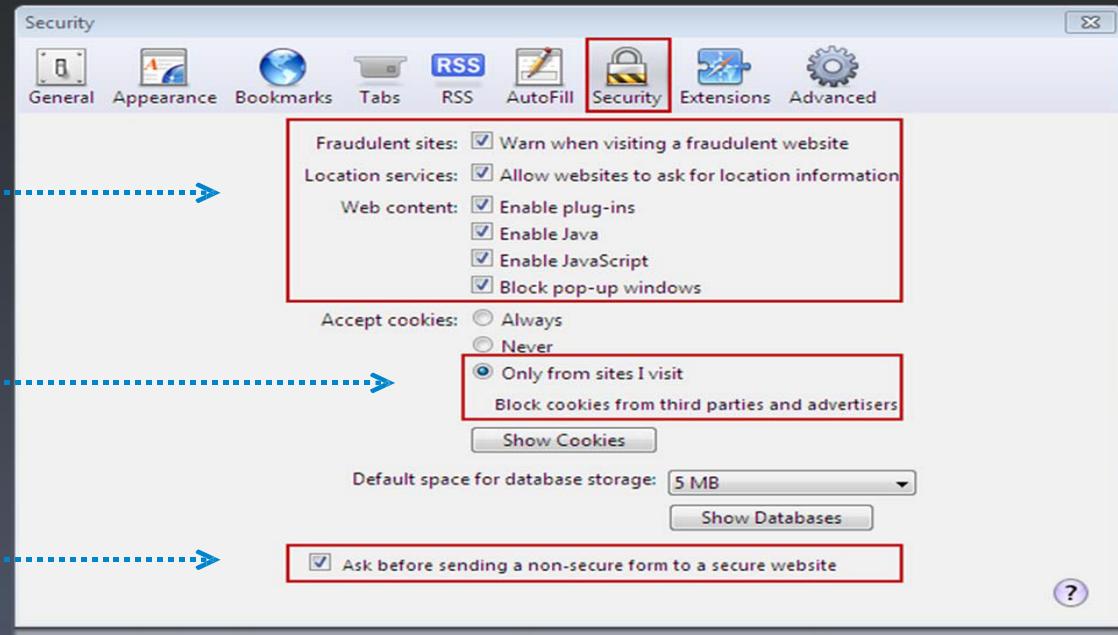
■ Lancer le navigateur **Safari**

Pour changer de paramètres , sélectionner l'icône  : puis sélectionner **Préférences**

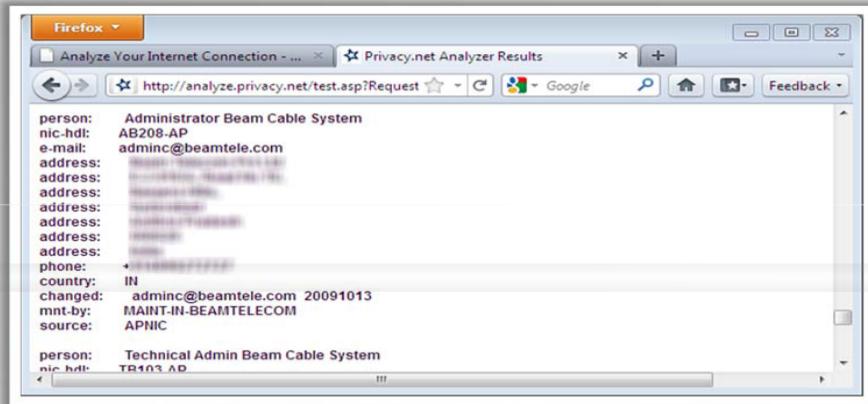


# Apple Safari: Paramètres de sécurité

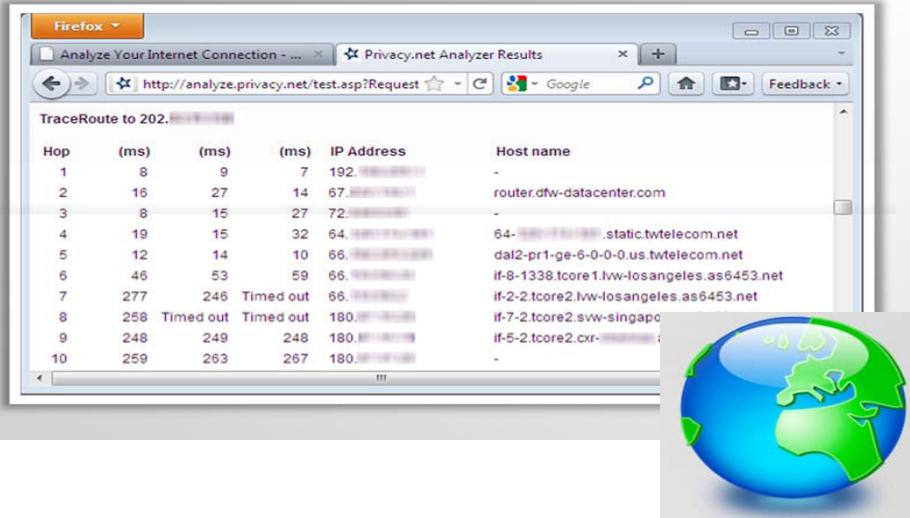
- Sélectionnez l'onglet **Sécurité** dans la fenêtre des préférences
- La section de **contenu Web** permet à l'utilisateur d'activer ou de désactiver diverses formes de scripts et le contenu actif
- Il est recommandé d'accepter uniquement les cookies des sites visités
- Cocher cette option permet au navigateur d'avertir l'utilisateur avant d'ouvrir un site Web qui n'est pas sécurisé



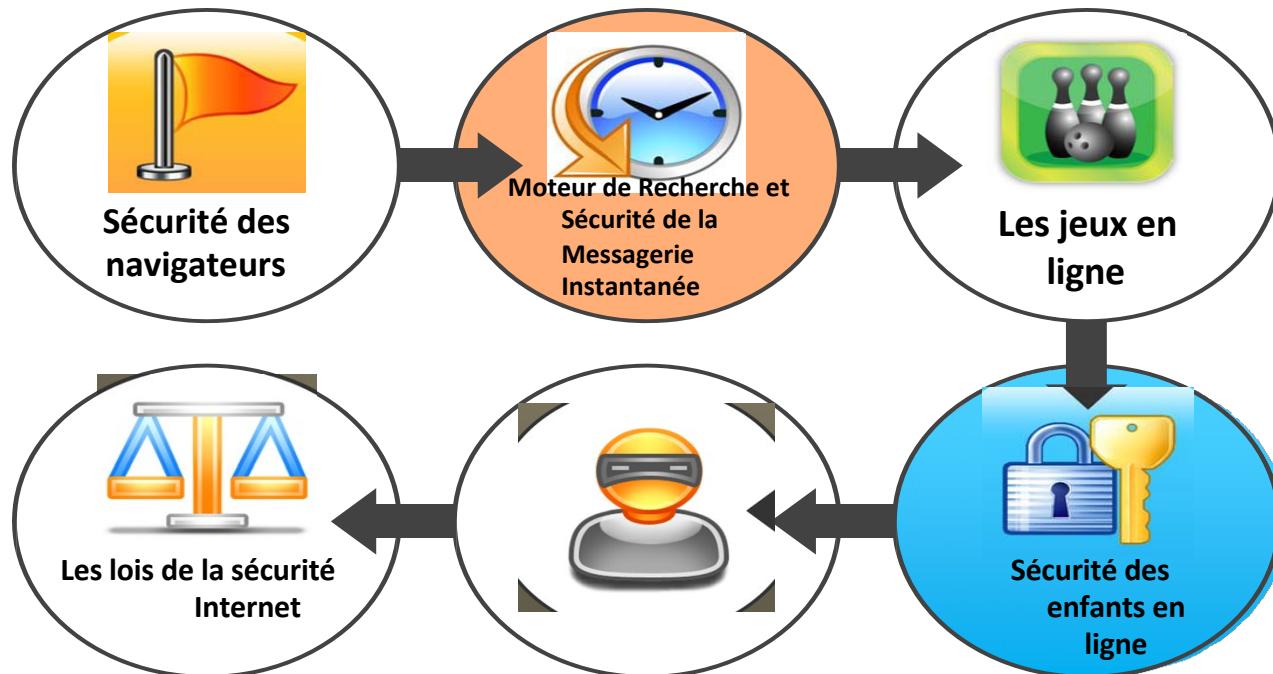
# Tester le navigateur: la vie privée



- Lancez le navigateur Internet et aller sur la page <http://privacy.net/> pour tester la vie privée
- Cliquez sur **Cliquez ici pour passer le test de navigateur** et d'analyser l'intimité de votre connexion Internet

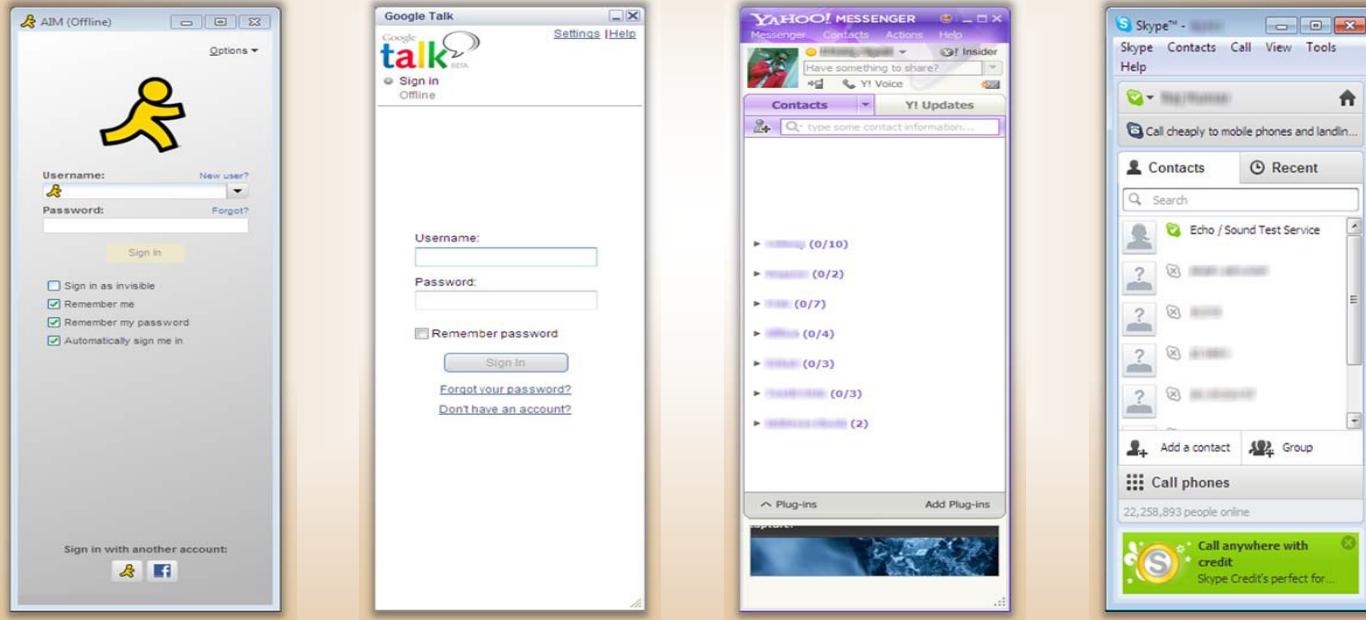


# PLAN



# Messagerie Instantanée (IMing)

- Messagerie instantanée (IMing) **permet à l'utilisateur d'interagir avec d'autres personnes** sur Internet à l'aide d'une application logicielle



# Messagerie Instantanée : Mesures de Sécurité



## IMWorm

- Un ver qui nuit à l'ordinateur et localise tous les contacts dans le carnet d'adresses de messagerie instantanée  
Le IMWorm tente d' envoyer à tous les contacts de messagerie instantanée la liste des contacts de l'utilisateur

## Ingénierie sociale

- L'ingénierie sociale dépend de **l'interaction** humaine qui consiste à tromper les gens par messagerie instantanée et d'obtenir leurs informations personnels

## Spam à travers l' IM( SPIM)

- SPIM est le spam **délivré par la messagerie instantanée** au lieu de le livrer par messagerie électronique.
- Les systèmes de messagerie instantanée comme Yahoo! Messenger, AIM, Windows Live Messenger, et salles de chat dans les sites de réseaux sociaux sont les cibles populaires des spameurs

# Messagerie Instantanée: Mesures de sécurité



N'accepter pas de révéler des informations personnels sur les IMS



Ne acceptez pas de liens reçus de personnes inconnues sur IM



Bloquer les utilisateurs qui envoient des liens web non sollicités



Toujours utiliser des mots de passe forts



Se déconnecter de l'application de messagerie après usage



Ne cochez pas l'option **enregistrer le mot de passe**



Username:

Password:  
 ······

Remember password

Sign In

[Forgot your password?](#)

[Don't have an account?](#)

# Recherche sur le Web

Les moteurs de recherche affichent des centaines de résultats pour une requête de recherche

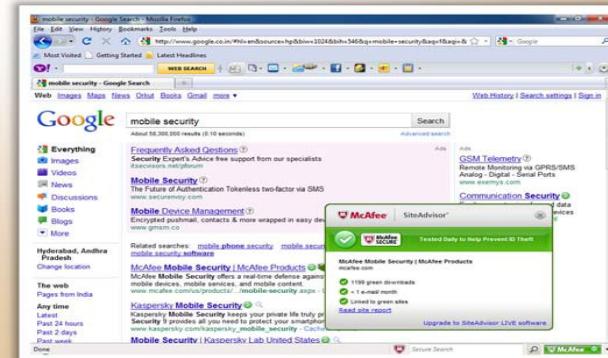
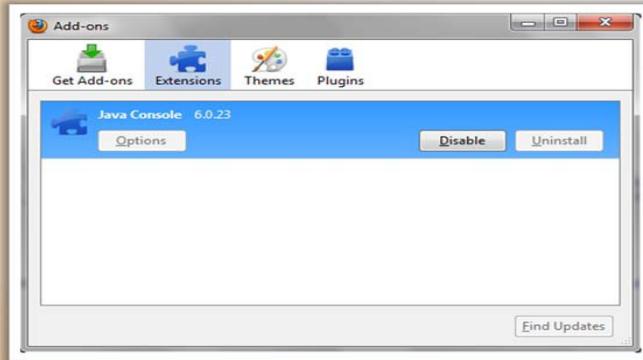


Ce n'est pas tous les résultats de la page Web obtenus par le moteur de recherche sont en sécurité

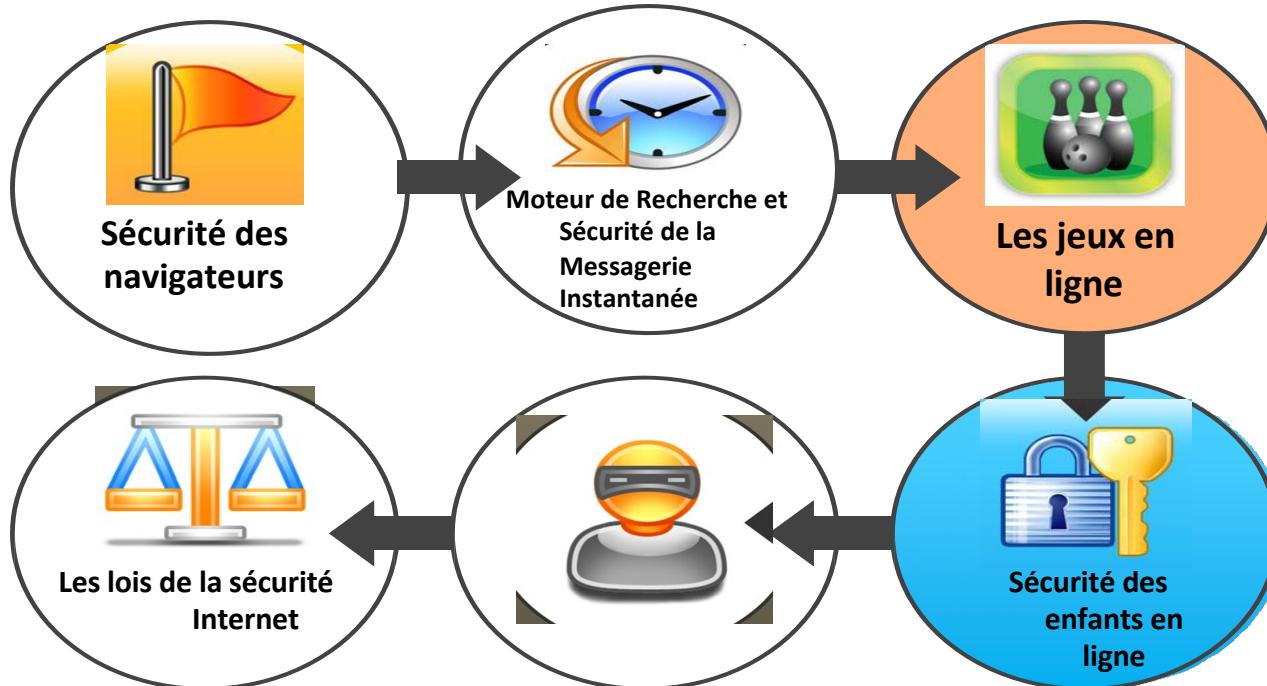
Pour filtrer les résultats de la recherche malveillantes, utilisez une application tel qu'un antivirus ou un add-on pour le navigateur



Pour ajouter un **Add-ons** dans Mozilla Firefox, aller dans **Outils → Modules complémentaires**



# PLAN



# Jeux en ligne et MMORPG

Massively Multiplayer Online Role- Playing Game

Le jeu en ligne est devenu un passe-temps populaire, notamment en raison de l'Internet haut débit et les nouvelles technologies

MMORPG sont très populaires dans le monde entier et les revenus pour ces jeux sont supérieurs d'un milliard de dollars



Jeux de rôle en ligne massivement multijoueurs (MMORPG) est un type de jeu où un grand nombre de joueurs interagissent entre eux dans un monde virtuel



Il est également devenu la cible pour les pirates avec de grosses sommes d'argent impliquées



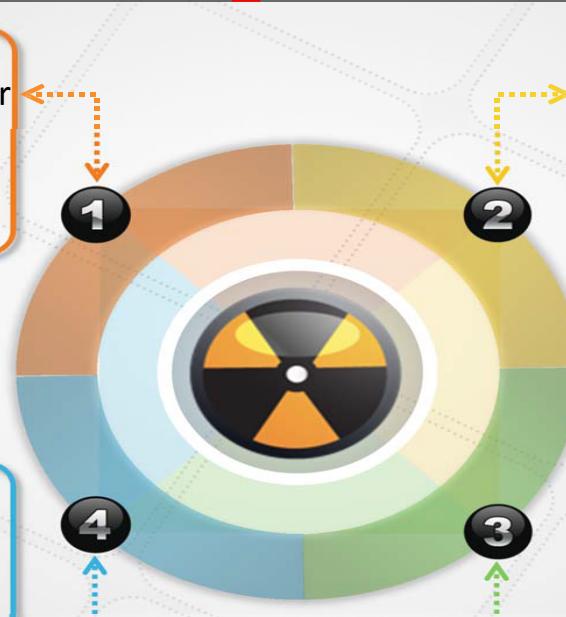
Dans le monde des MMORPG, connu aussi comme les jeux en ligne, les joueurs peuvent rencontrer d'autres joueurs, devenir amis, s' engager dans une bataille, lutter contre le mal et le jeu

# Les Risques des jeux en ligne

Interactions avec les **fraudeurs potentiels** qui peuvent tromper le joueur à révéler des **informations personnelles / financières**



**Logiciels malveillants** tels que les virus, les chevaux de Troie (Trojans), les vers informatiques et les logiciels espions

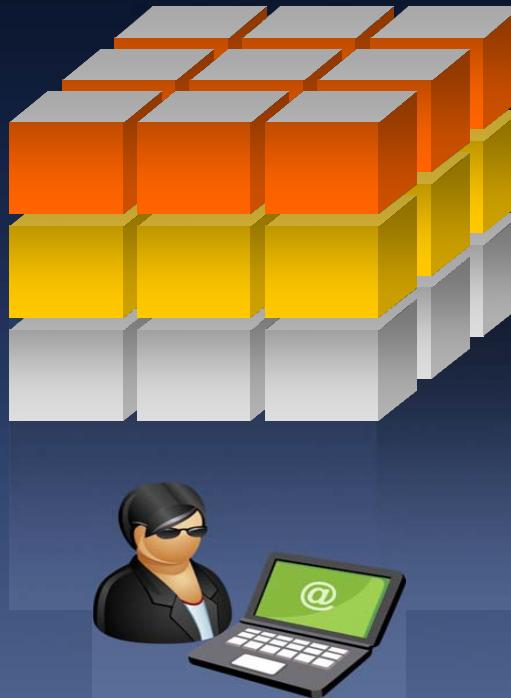


Intrusion pouvant exploiter des **failles de sécurité**



**Prédateurs en ligne et dans la vie réelle**

# Serveurs de jeux compromis ou non sécurisés



- Si le logiciel sur le serveur de jeu est **compromis**, les ordinateurs qui sont connectés au serveur peuvent également être compromis
- N'importe quel jeu avec une **connexion réseau** comporte un risque
- L'attaquant peut même utiliser les vulnérabilités à **planter le serveur de jeu**
- The vulnerabilities in **the** game server can be used by the attackers to:
- Les vulnérabilités du serveur de jeux peuvent être utilisées par les assaillants pour:
  - **Voler des mots de passe de jeu**
  - **Voler des informations à partir des ordinateurs de jeux**
  - **Contrôler les ordinateurs des jeux à distance**
  - **Lancer des attaques sur d'autres ordinateurs**
  - **Installer des programmes tels que les chevaux de Troie, des logiciels espions,**

# Risques Sociaux

Les attaquants peuvent utiliser l'interaction sociale dans l'environnement de jeu en ligne pour **attaquer les ordinateurs non protégés** ou exploiter les vulnérabilités de sécurité



# Ingénierie Sociale

Les attaquants peuvent tromper les joueurs à installer des logiciels malveillants sur leurs ordinateurs par ingénierie sociale



Ils offrent un bonus ou de l'aide dans le jeu en échange des mots de passe des autres joueurs ou d'autres informations dans les forums de jeu

Les joueurs qui sont à la recherche de moyens pour se rendre le jeu plus facile tombent dans ces genres de pièges

Les attaquants envoient les emails d'hameçonnage supposés venir des administrateurs de serveurs de jeu, qui invitera le joueur à s'authentifier à son compte via un site web dans le message

**Note:** Les Maîtres de jeu (GMS) dans un jeu ne demanderont jamais à un joueur son nom d'utilisateur et ou mot de passe

# Message d'un joueur à propos d'un mot de passe volé par un programme malveillant

In-Game Customer Support  
Forum Nav : In-Game Customer Support

New Topic Quick Search Advanced Search Search Login Help Forum Index

Topic Account hacked - psw.wow trojan |

0. Account hacked - psw.wow trojan | Quote Reply

Båt

I got infected with this virus 3 days ago (since that's when my account got "stolen"). I tried to mail blizzard several times but the webform thing seems broken, also asked a friend to ticket a GM ingame but all he got was one of those mails saying something about "this is bееing looked into, don't report the issue again yada yada".

Now i'm facing some other problems:

- Don't have my secret question answer (wouldn't have been here if I did)
- Don't have my CD-Key (can't find the box anywhere)
- No friggin telephone (so I can't phone the support)

So...what on gods green earth am I supposed to do now? It would be great if someone at blizzard would like to take this on and keep in touch with me via mail (yea...fat chance). Anyway, I'll have to prove that it's actually \_my\_ account in some way, which I can if you just contact me. <http://www.racelist.com>

Virus has been taken care of and it's gone, and I'm posting from my brothers account atm.

Blue text plz.

# Systèmes de Protection, Cyber Prostitution et agression virtuelle

## Systèmes de protection

- Le crime organisé a émergé dans la communauté de jeu sud-coréen
- Les organisations criminelles forcent les joueurs dans les **projets de protection**, où les joueurs doivent payer de **l'argent (virtuel ou réel)** pour éviter que des personnages de jeux ne soient tués et des mots de passe ne soient volés

## Cyber Prostitution

- Les jeux en ligne sont utilisés pour la cyber prostitution où les clients / joueurs paient de l'argent pour du cybersex
- **En ligne**, un jeune de 17 ans a développé un jeu en ligne massivement multijoueur (MMO), un cyber "bordel", où les joueurs payent Sim-argent (Simoleans) pour du **cybersex par minute**
- Les **comptes** des joueurs ont **finalement été annulés**

## Agression virtuelle

- L'agression virtuelle a été inventée lorsque certains joueurs de **Lineage II** ont utilisé des robots pour vaincre les autres joueurs et prendre leurs articles; ces éléments ont ensuite été mis en vente aux enchères en ligne



# Comment les utilisateurs malveillants gagnent de l'argent

Les objets volés tels que les mots de passe ou des objets virtuels **sont mis en vente** sur les sites, comme eBay ou sur des forums et sont vendus à d'autres joueurs pour de **l'argent réel ou virtuel**

Le cybercriminel peut demander au joueur d'obtenir une **rançon** en échange de ces informations

**70 Rogue and pally epix!**

Seller of this item? [Sign in](#) for your status



Starting bid: **US \$800.00** [Place Bid >](#)

Make No Payments Until 2008 [Apply](#)

End time: **Aug-27-07 15:40:06 PDT** (6 days 8 hours)

Shipping costs: Check item description and payment instructions or contact seller for details

Ships to: United States

Item location: Florence, AL, United States

History: [0 bids](#)

View larger picture

1 of 2

You can also:

[Watch This Item](#)

Get alerts via [Text message](#), [IM](#) or [Cell phone](#) [Email to a friend](#)

Listing and payment details: [Show](#)

**eBay**

<http://www.securelist.com>

# Pratiques de Sécurité Spécifiques aux jeux

# Reconnaître les Risques en Mode Administrateur



Certains jeux nécessitent le **mode administrateur** pour être exécutés

Si c'est le cas, s'assurer que le jeu a été téléchargé à partir d'un site de confiance ou du **vendeur fournisseur**

1



Téléchargements gratuits de jeux peuvent contenir des **logiciels malveillants**, y compris les plugins pour lancer le jeu

- Ce logiciel peut être utilisé pour obtenir le **privilège administrateur de l'ordinateur**

2



Au lieu d'utiliser le compte d'administrateur, le joueur est conseillé de naviguer sur Internet ou jouer à des jeux en utilisant un **compte d'utilisateur**, qui peut refuser à l'attaquant l'accès aux droits d'administrateur

3

# Reconnaitre les Risques dus à ActiveX et JavaScript

Certains des joueurs de jeux sur le Web exigent ActiveX ou l'activation de JavaScript

L'activation de ces fonctions conduit à des vulnérabilités

Ces fonctions ne doivent être activées que pour des jeux téléchargés à partir de sites de confiance



# Jouer, seulement sur le site de jeu



Jouer au jeu seulement à partir du site du fournisseur et épargner le **Navigateur Internet**



Une fois le jeu terminé,  
**passer sous le compte utilisateur pour naviguer sur Internet**



Cela réduit le risque de visiter un **site Web malveillant** lors du jeu en ligne



# Faites attention à la gestion du pare-feu



Certains jeux multijoueurs peuvent exiger que les **paramètres de pare-feu** soient modifiés pour permettre aux la libre circulation des informations du jeu de passer à travers les ordinateurs de jeu

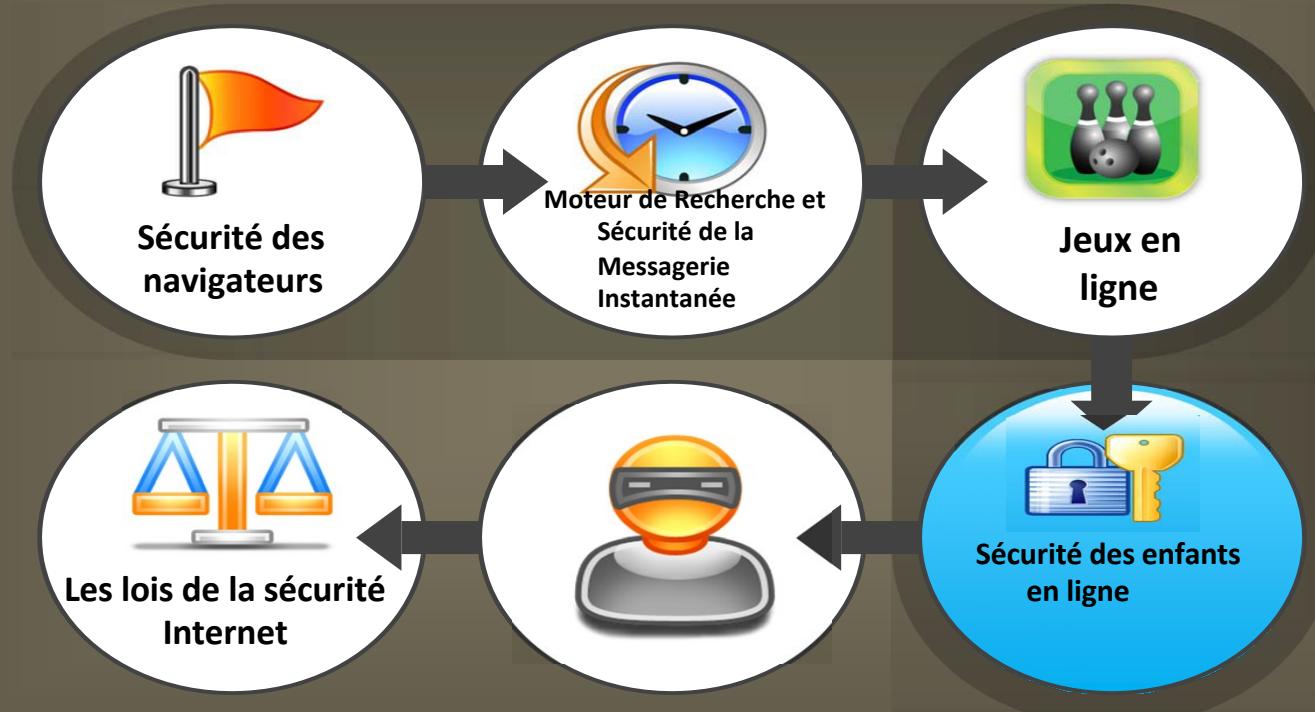


Chaque fois que les paramètres permissifs sont modifiés sur le pare-feu, le risque de sécurité informatique **augmentent sur les ordinateurs concernés**



Dans les pare-feu, le joueur peut insérer les adresses IP des autres joueurs comme de **confiance pour éviter toute interaction avec l'attaquant**

# PLAN



# Risques encourus en ligne

**Les risques encourus lorsqu'un enfant travaille en ligne comprennent:**

- Les sites furtifs et des URLs trompeuses
- Le harcèlement sexuel en ligne

**La cyber intimidation**

- La pornographie infantile
- Grooming (sollicitation en ligne d'un mineur de moins de 15 ans par un majeur à des fins sexuelles)



# Recherches non correctes

- 1** Les parents peuvent prendre toutes les précautions pour protéger l'enfant en ligne de tout ce qui peut être négatif lorsque l'enfant est inconsciemment conduit à visiter les sites nuisibles
- 2** Les moteurs de recherche utilisent des termes connus sous le nom de «méta variables» pour indexer un site Web
- 3** Quand un utilisateur effectue une recherche, les moteurs de recherche affichent les résultats en utilisant les variables méta

Exemple: un site de sport peut être indexé par les termes méta "soccer", "football", «scores», etc.
- 4** Les promoteurs de sites porno ajoutent des termes de recherche populaires à leur liste de variables méta, pour rediriger le trafic Web vers leurs sites
- 5** Les sites pornographiques peuvent utiliser les mots «sport», «école», «films», etc., pour attirer les enfants vers leurs sites Web
- 6** A moins qu'un logiciel de filtrage soit utilisé, les moteurs de recherche ne peuvent pas distinguer entre les demandes de recherche d'un adulte et d'un enfant



# Sites furtifs et des URL trompeuses

Les Sites pornographiques prospèrent avec l'accroissement du trafic Web



Les Sites pornographiques utilisent erreurs typographiques communes pour attirer les visiteurs sur leurs sites Web



Les enfants peuvent se retrouver sur un site Web pornographique en tapant simplement

"[www.whitehouse.com](http://www.whitehouse.com)" au lieu de "[www.whitehouse.gov](http://www.whitehouse.gov)"



Les Promoteurs de sites pornographiques achètent des noms de domaine comme le ".com" et ".gov" ou le ".org", en étant conscients que les internautes se retrouveraient sur leurs sites Web s' il y a une erreur typographique



# Pornographie infantile, Grooming , et la Cyberintimidation

## Pornographie infantile

Selon la loi fédérale (18 U.S.C. §2256), la pornographie juvénile est définie comme toute représentation visuelle, y compris toute photographie, cinéma, vidéo, image, ou une image générée par ordinateur, que ce soit réalisé ou produit par des moyens électroniques, mécaniques ou autres, un comportement sexuellement explicite , où la production de la représentation visuelle implique l'utilisation d'un mineur se livrant à un comportement sexuellement explicite ".  
<http://www.missingkids.com>

## Grooming

- Le « Grooming » est un acte de **consolateur** qui établit une connexion émotionnelle avec les enfants
- Le Pédopiégeage est utilisé pour circonvenir les enfants à des fins sexuelles et à la maltraitance des
- Les délinquants ciblent les enfants par le biais de l'affection, la gentillesse et de sympathie, et leur offrent des cadeaux et / ou de l'argent.....

## Cyber intimidation

- La cyberintimidation se produit quand un enfant ou un adolescent, est **menacé, harcelé et / ou embarrassé** en utilisant Internet ou les téléphones mobiles ou d'autres supports de communication.

- Signes de cyberintimidation:

- **Bouleversé après l'utilisation de l'ordinateur**
- **Refuse de sortir de la maison ou d'aller à l'école**
- **Dessine loin de leurs amis et de la famille**



# Rôle d'Internet dans la pornographie infantile



L'Internet offre un accès facile à d'énormes quantités de **matériel pornographique**  
Il assure **l'anonymat** et **l'intimité**



Divers services Web tels que e-mails, newsgroups, et salles de chat **facilitent le partage** de matériel pornographique



Il fournit un moyen **rentable** pour le transfert de matériel pornographique



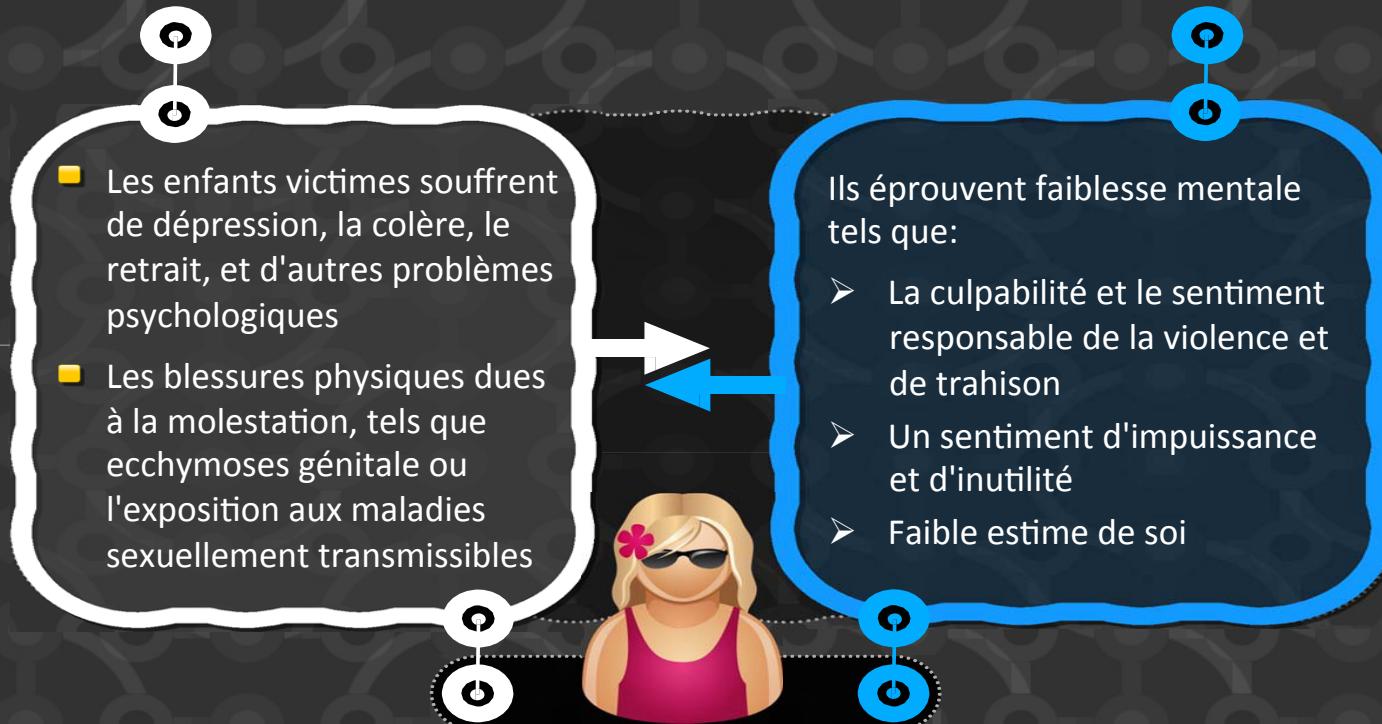
Il permet aux personnes disposant d'une connexion Internet d'accéder à du matériel pornographique à tout moment et de ne importe où



Il prend en charge le transfert de matériels pornographiques dans divers formats qui peuvent être stockés sur différents **périphériques de stockage numériques**



# Effets de la pornographie sur les enfants



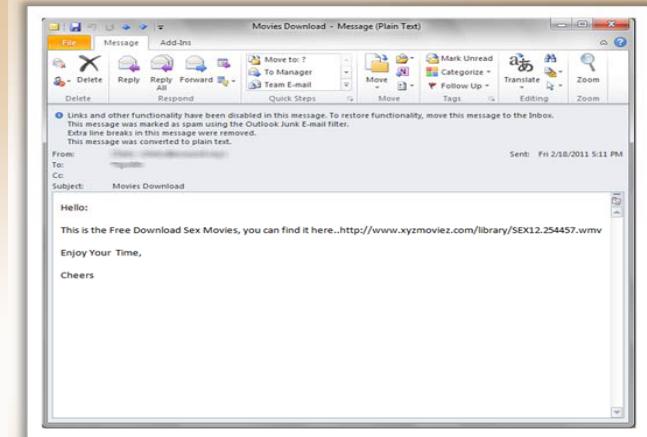
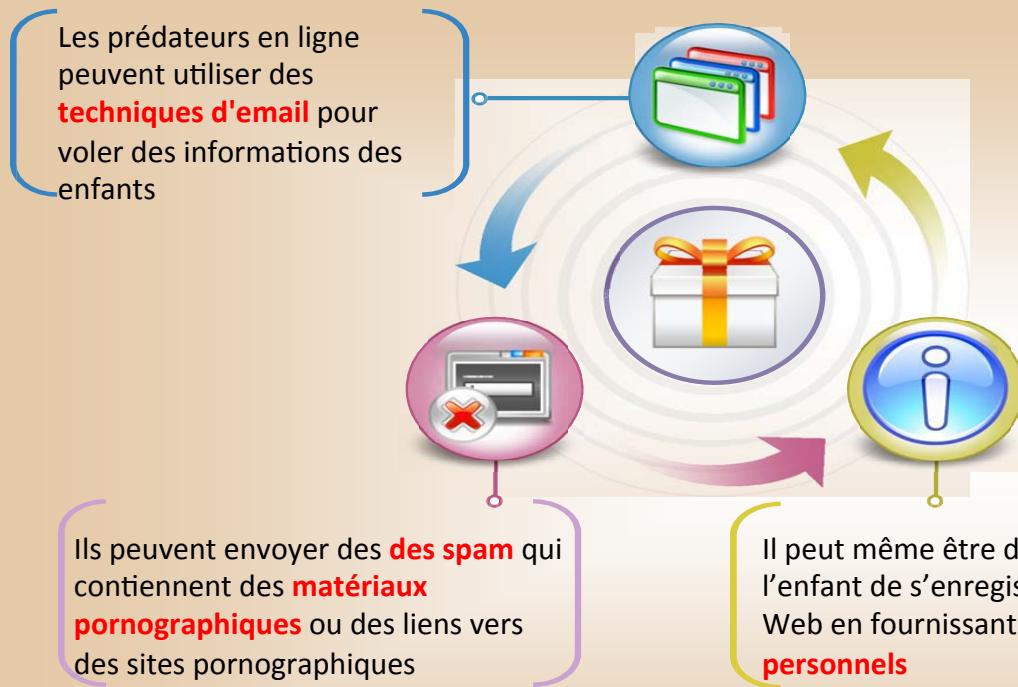
# Risks Involved in Social Networking Websites



# Risques liés aux sites de réseaux sociaux

- Les gens sur les sites de réseaux sociaux peuvent consulter les profils, photos et vidéos d'autres personnes sur ce site 
- L'enfant peut fournir trop d'informations sur un site Web de réseautage social 
- Les prédateurs en ligne peuvent obtenir des informations telles que les Identifiants e-mail, numéros de téléphone, adresses de résidence, les loisirs, les intérêts et plus de leur profil 
- Les prédateurs en ligne peuvent utiliser ces informations pour la cyber intimidation, le vol d'identité, ou la cyber exploitation 

# Les e-mails non sollicités



# Chat Rooms

Les prédateurs en ligne peuvent utiliser des techniques d'ingénierie sociale pour obtenir des renseignements personnels des enfants dans un chat room



Les prédateurs en ligne peuvent utiliser les salles de chat de nouer des contacts avec les enfants puis les conduire dans la prostitution cyber

Ils peuvent aussi utiliser des chat rooms pour envoyer des liens vers des sites avec des contenus inappropriés, comme la pornographie

Ils peuvent également envoyer des liens malveillants à des enfants, ce qui peut entraîner l'infection de l'ordinateur par logiciels malveillants

# Déceler si les enfants courrent des risques en ligne

Les parents peuvent trouver si leurs enfants sont confrontés à des menaces en ligne à partir des symptômes suivants:



L'enfant passe plus de temps assis devant l'ordinateur



Du matériel pornographique est présent sur l'ordinateur de l'enfant



L'enfant reçoit des appels téléphoniques et / ou des dons de personnes inconnues



L'enfant éteint rapidement le moniteur ou l'écran change lorsque le parent entre dans leur chambre

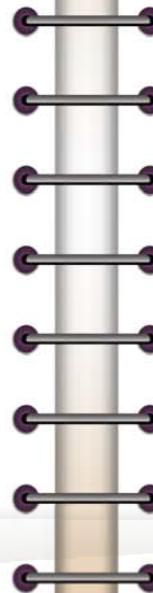


L'enfant se sent déprimé et ne montre aucun intérêt à parler en famille ou entre amis



# Protéger les enfants contre les menaces en ligne

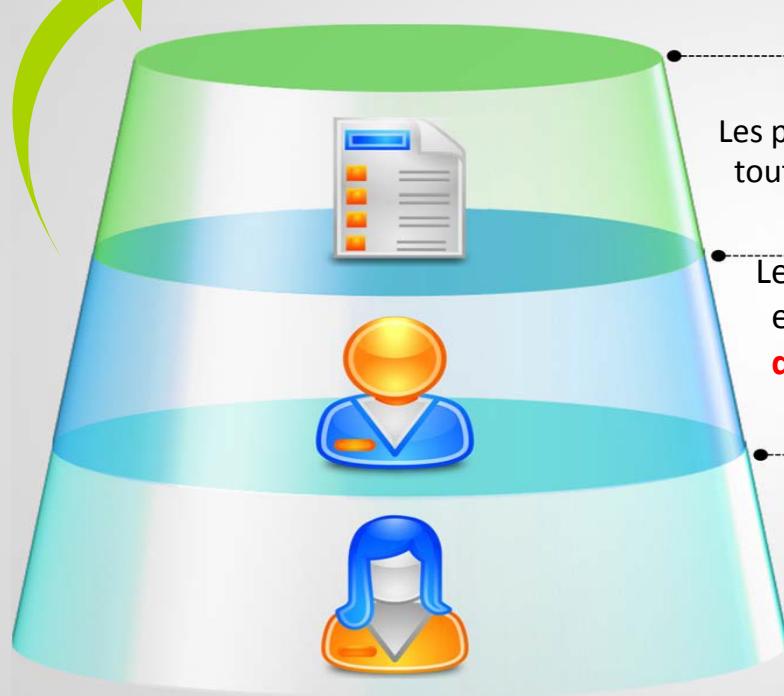
- ➊ Assurez-vous que l'enfant est informé sur les dangers que représentent les **délinquants du sexe-sur ordinateur**
- ➋ **Surveillez** ce que l'enfant fait sur l'ordinateur
- ➌ Utilisez les identifiants des appelants sur les téléphones pour savoir qui appelle l'enfant, et **bloquer les numéros suspects**
- ➍ Surveiller l'accès à tous les types de communications électroniques en direct tels que les **chat rooms, la messagerie instantanée, Internet Relay Chat**, etc. de l'enfant
- ➎ Restreindre l'accès aux sites **Web malveillants et pornographiques** en utilisant un logiciel de filtrage de contenu Internet
- ➏ Si l'enfant a un profil sur les réseaux sociaux, examiner de près les informations qu'il poste dans son **profil et sur des blogs**, y compris des **photos et des vidéos**



- ➊ Vérifiez vos **relevés de carte de crédit** chaque mois pour les frais inhabituels qui pourraient indiquer des achats non autorisés par un étranger ou votre enfant
- ➋ Avertissez la police si quelqu'un un **rencontré en ligne** par l'enfant **commence à l'appeler**, lui envoyer des cadeaux, ou essaye de l'attirer pour lui soutirer des informations sensibles
- ➌ Assurez-vous que l'enfant ne :
  - Fournir des informations personnelles telles que **nom, adresse, téléphone, nom d'école;**
  - Rencontrer personne en ligne **sans autorisation**
  - Ouvrir des E-mails provenant **d'expéditeurs inconnus**
  - Partager ses **photos / vidéos** avec des inconnus sur Internet



## Encourager les enfants à dénoncer



Les parents doivent encourager leurs enfants à dénoncer tout **comportement inapproprié** auquel ils font face

Les parents doivent encourager les enfants à venir à eux s'ils sont victimes d'intimidation ou **font face à des prédateurs en ligne**

Les enfants peuvent aussi être encouragés à parler à une personne de confiance, comme une tante, un oncle ou frère plus âgé, s'ils sont **mal à l'aise** de parler aux parents

# Comment Dénoncer un Crime



Les crimes sur Internet peuvent être signalés au  
[http://www.ic3.gov/complaint/  
default.aspx](http://www.ic3.gov/complaint/default.aspx) en cliquant sur  
**Rapport criminalité sur Internet**

**INTERNET CRIME COMPLAINT CENTER**  
*... an FBI - NW3C Partnership*

[Home](#)   [File a Complaint](#)   [Press Room](#)   [About IC3](#)   [Contact Us](#)

**► If you think your life is in danger, please contact your local and/or state police immediately!**

**File a Complaint**

Prior to filing a complaint with the Internet Crime Complaint Center (IC3), please read the following information regarding terms and conditions. Should you have additional questions prior to filing your complaint, view [FAQ](#) for more information on inquiries such as:

- What details will I be asked to include in my complaint?
- What happens after I file a complaint?
- How are complaints resolved?
- Should I retain evidence related to my complaint?

The information I've provided on this form is correct to the best of my knowledge. I understand that providing false information could make me subject to fine, imprisonment, or both. ([TITLE 18, U.S. CODE, SECTION 1001](#))

The IC3 is co-sponsored by the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). Complaints filed via this website are processed and may be referred to federal, state, local or international law enforcement or regulatory agencies for possible investigation. I understand any investigation opened on any complaint I file on this website is initiated at the discretion of the law enforcement and/or regulatory agency receiving the complaint information.

Filing a complaint with IC3 in no way serves as notification to my credit card company that I am disputing unauthorized charges placed on my card or that my credit card number may have been compromised. I should

**► FAQs**  
**► Legal**  
**► Disclaimer**  
**► Privacy Notice**

**► Protect Yourself**

[► Internet Crime Prevention Tips](#)  
[► Internet Crime Schemes](#)

[► Public/Private Alliances](#)  
[► Site Map](#)

**Protect Yourself With The Latest IC3 Consumer Alerts!**

[► Mass Market Fraud](#)

<http://www.ic3.gov>

# Logiciel de sécurité pour la protection des enfants contre les menaces en ligne

- Les enfants peuvent être protégés contre les menaces en ligne en installant un logiciel de sécurité approprié sur l'ordinateur de l'enfant
- Les fonctionnalités qu'un parent devrait rechercher dans le logiciel comprennent:



## Blocage Web

Pour aider à prévenir l'enfant de regarder du contenu inapproprié



## Blocage de Programmes

Pour aider à bloquer les jeux, le partage de fichiers peer-peer, etc.



## Blocage de courriels

Pour aider à bloquer les adresses email inconnues et empêcher les enfants de communiquer avec des gens qu'ils ont rencontré en ligne par e-mail



## Délai

Pour aider à contrôler la quantité de temps que l'enfant passe sur l'ordinateur

## Fonctionnalités de Messagerie Instantanée

Pour aider à l'enregistrement et au suivi des conversations de messagerie instantanée de l'enfant, afin de permettre aux parents de déterminer si l'enfant est engagé dans un dialogue inapproprié avec des personnes inconnues

## Rapports d'utilisation

Pour fournir un rapport à jour sur l'utilisation d'Internet de l'enfant et l'historique de la Messagerie Instantanée pour surveiller les interactions en ligne de l'enfant

## Filtrage vidéo

Pour s'assurer que l'enfant ne regarde pas les vidéos inappropriées sur des sites comme YouTube, mais en même temps permettre à l'enfant de voir des vidéos utiles

## Fonctionnalités de plates-formes de réseaux sociaux

Pour aider à l'enregistrement et la surveillance de la teneur des messages l'enfant poste en ligne, et déterminer si l'enfant est victime d'intimidation en ligne

- KidZui est un **navigateur web gratuit, moteur de recherche, et aire de jeux en ligne** pour les enfants
- Il dispose d'un grand nombre de jeux, sites web, des vidéos, des photos et revue par les **parents** et les **enseignants**
- It eliminates the need for parents **when kids are online**



The screenshot shows the main interface of the KidZui website. At the top, there's a navigation bar with links for 'Home', 'Back', 'Next', 'Search Here', 'Go', 'My Favorites', and a 'CLOSE' button. On the right side, there's a 'FRIENDS' section showing 'Molly3 Level 1 Points: 96' and 'kidzui Level 1 Points: 141'. Below the navigation bar, there are three tabs: 'WEB', 'PHOTO', and 'VIDEO'. The 'WEB' tab is selected, displaying a grid of 15 cards. Each card has a small thumbnail image and a title. The titles include 'Lego Batman', 'Kitten', 'Tom Arma's Safari', 'School Bat', 'www.noggin.com', 'Orangutans Kissing', 'Tiger rat', 'Chicken Little', 'Brown Horse', 'www.bobthebuilder.com', 'the muppets', 'Finding Nemo DVD', 'Happy Healthy Songs', 'Miniclip Homepage', and 'Popular Websites'. At the bottom of the page, there are several footer links: 'Edit My Zui', 'History', 'Inbox', 'Backgrounds', 'Help', 'Logout', and the current time '8:52:37 AM'.

[www.kidzui.com](http://www.kidzui.com)

# Actions To Take When the Child Becomes an **Online Victim**



Report the offense to the Internet Service Provider (ISP)

Also report to the offender's ISP

Change the online information of the child and delete the social networking accounts if necessary



Encourage the child not to log into the website where **bullying occurred**

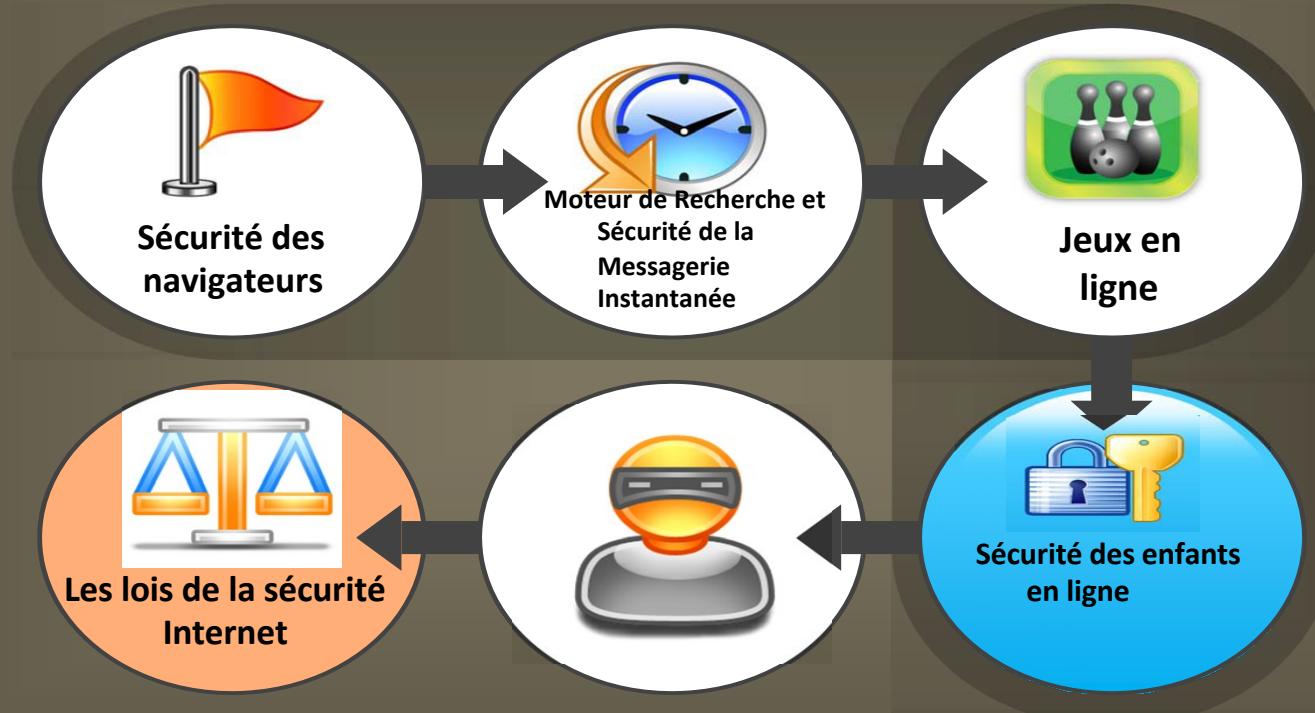
Block the offender's email address and screen name so that they cannot contact the child anymore

# Conduite à tenir lorsque l'enfant devient une victime en ligne

1. **Ignorer** tout contact par le prédateur en ligne ou cyberintimidateur
2. Encourager l'enfant à ne pas se connecter sur le site **où l'intimidation s'est produite**
3. **Bloquer l'adresse e-mail de l'auteur et son pseudonyme** pour qu'ils ne puisse plus communiquer avec l'enfant
4. **Modifiez les informations en ligne** de l'enfant et supprimer ses comptes des réseaux sociaux si nécessaire
5. Signaler l'infraction au fournisseur de services Internet (ISP) et lui **fournir les informations nécessaires sur le délinquant**



# PLAN



# Lois Internet

- L'espace web est un vaste terrain et avec une pléthore de **sites e-commerce, sites analytiques, sites sportifs, sites d'information, sites d'entreprises**, etc.
- Ce grand domaine nécessite une surveillance pour **protéger les internautes contre les criminels de l'Internet, les attaquants**, etc. lois Internet protègent les utilisateurs **contre les actes immoraux / indécentes, violation de la confidentialité**, etc., sur l'Internet

## Pourquoi devriez-vous connaître les lois d'Internet?

- Les utilisateurs d'Internet doivent connaître les lois de l'Internet pour tirer parti des **différends contre les fournisseurs d'e-commerce, les fraudeurs et les criminels d'Internet**, etc.,
- Connaître les lois d'Internet aide les utilisateurs à **comprendre ce qu'ils peuvent et ne peuvent pas poster sur Internet**
- En outre, les utilisateurs ont besoin de connaître les lois de l'Internet pour pouvoir **utiliser légalement le contenu immense présent sur Internet**

## Les lois d'Internet couvrent:

- Diffamation
- propriété intellectuelle
- Brevets
- Droits d'auteur
- confidentialité contrefaçon
- Protection de l'enfance,
- etc.



## Lois importantes::

USA PATRIOT Act  
La Loi sur la protection en ligne des enfants (COPPA)  
Le Digital Millennium Copyright Act  
CAN-SPAM Act  
Computer Misuse Act 1990  
La directive de l'Union Européenne sur la protection des Act 1998

# Directive de l'Union Européenne sur la protection des données (95/46/EC)



La directive 95/46 / CE fournit des lignes directrices aux Etats membres de l'Union Européenne pour **la vie privée et la protection des données des personnes**



La directive réglemente le **traitement des données à caractère personnel** indépendamment du fait que leur traitement est automatisé ou non



La Section 1 de la directive prévoit les principes relatifs à la **qualité des données**, l'article 2 fournit des critères pour des **traitements de données** légitimes et l'article 5 définit le **droit d'accès** aux données de la personne concernée



Selon l'article 1 de la directive, les États membres prévoient que les données personnelles doivent être collectées pour des usages déterminées, explicites et **légitimes** et ne doivent pas être traitées ultérieurement de manière incompatible avec ces usages



La Section 2 dispose que les États membres prévoient que les données personnelles peuvent être traitées que si la personne concernée a **indubitablement** donné son **consentement**



La Section 5 dispose que les États membres garantissent à toute personne concernée le **droit d'obtenir des informations** du contrôleur sans contrainte, à des intervalles raisonnables et sans retard excessif

# Mauvaise utilisation de l'ordinateur: Loi 1990

La loi 1990 sur l'usage illégal de l'ordinateur est une loi du Parlement du Royaume-Uni



**La loi permet certaines activités illégales telles que:**

- Le piratage des ordinateurs d' autres utilisateurs en utilisant des logiciels inappropriés,
- Aider le pirate à avoir accès aux fichiers / documents sécurisés dans l'ordinateur d'un autre utilisateur



**La loi définit trois infractions dans l'usage de l'ordinateur:**

- L'accès non autorisé à du matériel informatique
- L'accès non autorisé avec l'intention de commettre ou faciliter la commission d'autres infractions
- Toute modification non autorisée de matériel informatique



# Résumé

- ❑ La sécurité sur Internet implique la protection des données contre des accès non autorisé lorsque l'utilisateur est connecté à l'Internet
- ❑ Scannez les téléchargements de fichiers avec un antivirus à jour pour vérifier la présence de logiciels malveillants
- ❑ Le jeu en ligne est devenu un passe-temps populaire, surtout en raison de l'Internet haut débit et les nouvelles technologies
- ❑ Si le logiciel sur le serveur de jeu est compromis, les ordinateurs qui sont connectés au serveur peuvent également être compromis
- ❑ Les enfants peuvent être protégés contre les menaces en ligne en installant un logiciel de sécurité approprié sur leur ordinateur
- ❑ Les lois Internet protègent les utilisateurs d'actes immoraux / indécents et violation de la confidentialité sur Internet
- ❑ Connaître les lois d'Internet aide les utilisateurs à comprendre ce qu'ils peuvent et ce qu'ils ne peuvent pas poster sur Internet



## Les listes de contrôle de sécurité Internet

-  Mettre à jour régulièrement votre **système d'exploitation** et les autres applications installées
-  **Configuration d'un pare-feu** pour contrôler le flux d'informations
-  Vérifiez que vous avez la dernière **version du navigateur Web** installée sur le système et le mettre à jour régulièrement
-  **Installez un outil de navigation sécuritaire** qui met en garde contre les sites d'hameçonnage et bloque l'accès aux adresses
-  Assurez-vous que vous **êtes connecté à un réseau sécurisé** lorsque vous utilisez un réseau sans fil
-  Ne jamais répondre à des **offres électroniques non sollicités** ou demandes d'information



## Les listes de contrôle de sécurité Internet



Ne cliquez pas sur les liens envoyés par des **utilisateurs inconnus**



Ne pas télécharger des fichiers provenant de **sources inconnues**



Ne donnez pas **d'informations personnels identifiables** lors de l'enregistrement sur des sites



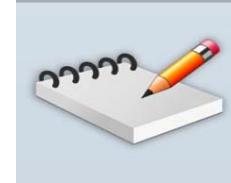
Ne cliquez sur aucun des **pop-ups** qui apparaissent pendant la navigation des sites Web



Régulièrement analysez votre système pour supprimer les virus, vers, chevaux de Troie, logiciels espions, enregistreurs de frappe et autres logiciels malveillants en utilisant antivirus



Mettre à jour l'application **antivirus** sur une base régulière





## Les listes de contrôle de sécurité Internet



Utilisez des **mots de passe forts** et les changer à intervalles réguliers



Déconnectez-vous d'Internet si vous découvrez quelque chose de suspect sur l'ordinateur



Toujours vérifier la barre d'adresses pour les URL correcte



Toujours vérifier le **certificat de site Web**, cadenas SSL et HTTPS



Ne pas activer les fonctionnalités **ActiveX et JavaScript**



Sauvegarder régulièrement les fichiers importants



Retirer **protocoles inutiles** de l'interface Internet



Vérifiez les journaux des routeurs et des pare-feu pour identifier les **connexions de réseau anormales** à l'Internet



## Liste de contrôle pour les parents pour protéger leurs enfants contre les menaces en ligne



**Discuter** avec les enfants de ce qu'ils font sur l'ordinateur



Consultez la **liste des amis** de l'enfant



Être informé des défis sur les réseaux sociaux



Encouragez l'enfant à utiliser l'enfant applications de sécurité telles que  
KidZui



**QUESTIONS ?**