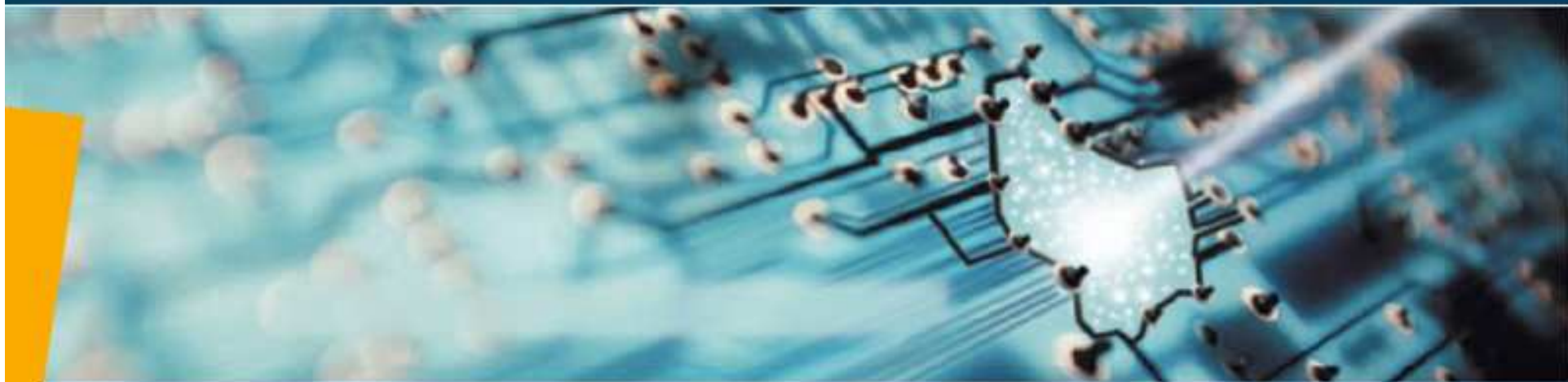




MINISTÈRE DE L'ÉCONOMIE
ET DU COMMERCE EXTÉRIEUR

IILNAS

Grand-Duché de
luxembourg.



Internet Security Day 3.0

-> Portrait du cybercrime contemporain

15 juin 2009



Portrait du cybercrime contemporain

1. Contexte du propos
2. TIC & G-D de Luxembourg
3. Cybercrime contemporain
4. Danger de la « surmédiatisation » et du « *marketing* de la peur »
5. Cybercrime & citoyen



Portrait du cybercrime contemporain

1. Contexte du propos
2. TIC & G-D de Luxembourg
3. Cybercrime contemporain
4. Danger de la « surmédiatisation » et du « *marketing* de la peur »
5. Cybercrime & citoyen



Portrait du cybercrime contemporain

- > **Service de la confiance numérique**
- > Un des services de l'administration ILNAS
[Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services]
- > Administration publique sous tutelle de M. le Ministre de l'Economie et du Commerce extérieur
- > <http://www.ilnas.public.lu>
- > <http://www.ilnas.public.lu/fr/confiance-numerique/index.html>

ILNAS // Luxembourg - Accueil - Windows Internet Explorer

http://www.ilnas.public.lu/fr/index.html

File Edit View Favorites Tools Help

ILNAS // Luxembourg - Accueil

GRAND-DUCHÉ DE LUXEMBOURG

INSTITUT LUXEMBOURGEOIS DE LA NORMALISATION,
DE L'ACCREDITATION, DE LA SÉCURITÉ ET QUALITÉ
DES PRODUITS ET SERVICES

ILNAS

Accessibilité | Aide | A propos du site | Notice légale

Recherche : OK Recherche avancée

Principaux portails publics

Accueil Nouveau sur ce site | Plan du site | Liens | Feed-back | Contact

ILNAS

NORMALISATION

ACCREDITATION DES OEC

SURVEILLANCE DU MARCHÉ

NOTIFICATION DES OEC

MÉTROLOGIE LÉGALE

BONNES PRATIQUES DE LABORATOIRE

NOTIFICATIONS "RÈGLES TECHNIQUES"

AUTORISATIONS POUR ÉLECTRICIENS

PROMOTION DE LA QUALITÉ

CONFIANCE NUMÉRIQUE

ACTUALITÉS

PUBLICATIONS



LÉGISLATION

RÉCLAMATIONS ET OBSERVATIONS

EXTRANETS

Accueil

A la Une


 

Internet Security Day 3.0
15-06-2009
La troisième édition de l'Internet Security Day (ISD 3.0) est programmée le 15 juin 2009. Ce rendez-vous annuel permet d'apporter une mise à jour des connaissances en termes de sécurité de l'information, notamment par rapport au médium Internet.
[Lire la suite](#)

Futures normes internationales : ISO/IEC 27015 & ISO/IEC 27036
11-06-2009
Deux futures normes internationales du domaine de la sécurité de l'information (ISO/IEC 27015 & ISO/IEC 27036) comptent désormais un expert issu du «Comité miroir ISO/IEC/JTC1/SC27 Luxembourg» en tant qu'éditeur.
[Lire la suite](#)

NormaFi-IT
12-06-2009 **Projet de recherche collaborative**
NormaFi-IT constitue un projet de recherche collaborative mené par le CRP Henri Tudor, à l'initiative de l'ILNAS.
[Lire la suite](#)

14ème Congrès International de Métrologie - 22 au 25 juin 2009 / Paris
22-06-2009
Le 14ème Congrès International de Métrologie se tiendra du 22 au 25 juin 2009 au Palais des Congrès de Paris sur le thème «Mesurer pour agir, agir pour progresser».
[Lire la suite](#)

 LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie
et du Commerce extérieur

ACTUALITÉS "PRODUITS NON CONFORMES"

DERNIERS PRODUITS NON-CONFORMES :

- 15.04.2009**
[Rappel des machines à café Philips "Senseo" \(pdf, 492Ko\)](#)

Retrouver la liste complète des "[produits non-conformes](#)"

http://www.ilnas.public.lu/fr/support/recherche-avancee/index.php

Internet 100%

ILNAS - ILNAS // Luxembourg - Windows Internet Explorer

http://www.ilnas.public.lu/fr/ilnas/index.html

File Edit View Favorites Tools Help

ILNAS - ILNAS // Luxembourg

GRAND-DUCHÉ DE LUXEMBOURG

Accessibilité | Aide | A propos du site | Notice légale

INSTITUT LUXEMBOURGEOIS DE LA NORMALISATION, DE L'ACCREDITATION, DE LA SÉCURITÉ ET QUALITÉ DES PRODUITS ET SERVICES

ILNAS

Principaux portails publics

Recherche : OK Recherche avancée

Accueil Nouveau sur ce site | Plan du site | Liens | Feed-back | Contact

ILNAS

- + Annuaire
- + Historique
- + Missions
- + Organisation

NORMALISATION

ACCREDITATION DES OEC

SURVEILLANCE DU MARCHÉ

NOTIFICATION DES OEC

MÉTROLOGIE LÉGALE

BONNES PRATIQUES DE LABORATOIRE

NOTIFICATIONS "RÈGLES TECHNIQUES"

AUTORISATIONS POUR ÉLECTRICIENS

PROMOTION DE LA QUALITÉ

CONFIANCE NUMÉRIQUE

ACTUALITÉS

PUBLICATIONS

LÉGISLATION

RÉCLAMATIONS ET OBSERVATIONS

EXTRANETS

Accueil > ILNAS

ILNAS

Qui sommes-nous?

L'Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services est une administration sous la tutelle du ministre ayant l'Économie dans ses attributions. Elle a été créée sur base de la loi du 20 mai 2008 et a démarré ses activités le 1er juin 2008.

```

graph TD
    Center(( )) --- Normalisation[Normalisation]
    Center --- Surveillance[Surveillance du marché]
    Center --- Accreditation[Accréditation]
    Center --- Metrology[Métrologie légale]
    Center --- Quality[Promotion de la qualité]
  
```

Pour des raisons de complémentarité, d'efficacité, de transparence et dans le cadre de la simplification administrative, l'ILNAS rassemble sous une même structure plusieurs missions administratives et techniques qui étaient auparavant dans les attributions de plusieurs structures publiques. Ces missions sont renforcées et de nouvelles tâches sont également attribuées à l'ILNAS. L'ILNAS correspond à un réseau de compétences au service de la compétitivité et de la protection du consommateur.

Une [loi spécifique \(pdf, 129Ko\)](#) a été rédigée en ce sens, et adoptée par la Chambre des Députés le 24/04/2008, constituant la feuille de route des missions à respecter par ILNAS.

Pour en savoir plus

SERVICES

- "Organisme Luxembourgeois de Normalisation" (OLN),
- "Surveillance du Marché",
- "Accréditation",
- "Métrologie légale",
- "Promotion de la qualité",
- "Confiance numérique".

Internet 100%

Confiance numérique - ILNAS // Luxembourg - Windows Internet Explorer

http://www.ilnas.public.lu/fr/confiance-numerique/index.html

File Edit View Favorites Tools Help

Confiance numérique - ILNAS // Luxembourg

GRAND-DUCHÉ DE LUXEMBOURG

Accessibilité | Aide | A propos du site | Notice légale

INSTITUT LUXEMBOURGEOIS DE LA NORMALISATION, DE L'ACCREDITATION, DE LA SÉCURITÉ ET QUALITÉ DES PRODUITS ET SERVICES

ILNAS

Principaux portails publics

Recherche : OK Recherche avancée

Accueil Nouveau sur ce site | Plan du site | Liens | Feed-back | Contact

ILNAS

NORMALISATION

ACCREDITATION DES OEC

SURVEILLANCE DU MARCHÉ

NOTIFICATION DES OEC

MÉTROLOGIE LÉGALE

BONNES PRATIQUES DE LABORATOIRE

NOTIFICATIONS "RÈGLES TECHNIQUES"

AUTORISATIONS POUR ÉLECTRICIENS

PROMOTION DE LA QUALITÉ

CONFIANCE NUMÉRIQUE

+ Collaborations

+ Etudes et développement

+ Normalisation et domaine IT

+ Veille technologique

+ PKI

+ Documents d'accréditation et de notification PKI

ACTUALITÉS

PUBLICATIONS

LÉGISLATION

RÉCLAMATIONS ET OBSERVATIONS

Accueil > Confiance numérique

Confiance numérique

Chaque utilisateur doit pouvoir profiter pleinement du domaine des Technologies de l'Information et de la Communication ("TIC"), mais en connaissance de cause. Interagir **inconsciemment** avec les TIC, peut se révéler dangereux à terme. Pour y répondre, la confiance relative aux TIC, qui n'existe pas par défaut, doit s'acquérir, et dans certains cas, peut se démontrer également.

Le fondement du domaine de la "confiance numérique" repose sur la **bonne perception des problématiques** sous-jacentes à l'utilisation des TIC, dans divers contextes, d'en percevoir clairement les risques, et de connaître, comprendre et mesurer l'intérêt de divers instruments et/ou informations relatives permettant d'agir alors dans un climat de confiance. La chaîne de valeur de la confiance numérique repose principalement sur les domaines de la qualité et de la sécurité appliquées aux TIC.

Le monde numérique ne s'est pas développé avec des spécifications de sécurité fortes dès le départ, mais surtout avec l'objectif d'accroître les capacités d'information et de communication au niveau mondial. Entre-temps de nombreuses menaces ont été mises en évidence, exploitant de nombreuses **failles**, pouvant entraîner des impacts préjudiciables non négligeables quant au tissu économique. La réalité des menaces, et l'importance de leurs représentations sociales, des vulnérabilités et des risques véritables convoquent principalement l'importance de la confiance numérique.

Face aux dangers, aujourd'hui, plus que jamais, la promotion et la connaissance du domaine de la "confiance numérique" s'imposent pour supporter et favoriser, *via* les TIC, le développement économique (numérique), ainsi que la vie quotidienne des usagers concernés.

La confiance numérique vise l'excellence des TIC, et en ce sens, elle constitue un des instruments, au sein d'ILNAS, au service de la compétitivité nationale. Ainsi, le service confiance numérique participe au développement de ce concept en veillant, au Luxembourg, aux missions suivantes :

- **Accréditation, notification et surveillance des Prestataires de Services de Certification** (selon la loi modifiée du 14 août 2000 relative au commerce électronique)
- **Suivi et développement du domaine des Public Key Infrastructure** ([rubrique "PKI"](#))
- **Etudes de projets nationaux relatifs au développement de la confiance numérique** (nouveaux schémas d'accréditation et/ou de certification)
- **Suivi et gestion nationale : ISO/IEC/Joint Technical Committee 1** (*Information Technology - Inscription P. Member - LU*)
 - Mise en place du "Consortium Luxembourgeois JTC1"

L'ACTUALITÉ DE LA CONFIANCE NUMÉRIQUE

Derniers événements liés à la Confiance Numérique :

- **15.06.2009**, [Internet Security Day 3.0](#)
- **05.05.2009**, [Un guide du numérique pour les consommateurs en ligne](#)

Pour plus d'informations sur l'ensemble des événements liés à l'ILNAS, veuillez consulter notre rubrique [actualités](#).

DOCUMENTS PUBLIC KEY INFRASTRUCTURE

[Documents d'accréditation et de notification PKI](#)



Portrait du cybercrime contemporain

-> **Service de la confiance numérique - ILNAS**

-> **Fondement de la Confiance numérique** : la recherche de l'*Excellence* des TIC *via* la qualité et la sécurité :

- Suivi et promotion des instruments d'accréditation et de certification de la confiance numérique
- Gestion et développement des instruments d'accréditation et de notification de la confiance numérique
- Relais d'informations et d'échanges de la connaissance normative du domaine TIC :
 - > pour viser l'*Excellence* TIC



Portrait du cybercrime contemporain

-> **Service de la confiance numérique - ILNAS**

- > **Accréditation**, notification et surveillance des Prestataires de Services de Certification [selon la loi modifiée du 14 août 2000 relative au commerce électronique]
- > **Promotion** et veille des instruments garantissant la confiance numérique [certifications ISO/IEC 27001, ISO/IEC 15408, ...]
- > **Etudes de projets nationaux** relatifs au développement de la confiance numérique [schémas d'accréditation et/ou de certification]
- > **Membre permanent** : ISO/IEC/JTC1
[« *Joint Technical Committee 1* » - JTC1 : organe de référence pour la normalisation des TIC au niveau international]



Portrait du cybercrime contemporain

-> **Service de la confiance numérique - ILNAS**

- > **Projet de recherche** « NormaFi-IT » - CRP Henri Tudor [Production d'un « livre blanc de la confiance numérique » en 2010]
- > **Suivi spécifique** du sous-comité JTC1/SC27 (série « 2700x » et groupes *ad hoc*...)
- > **Collaboration avec le projet CASES** (*Cyberworld Awareness and Security Enhancement Structure* – <http://www.cases.public.lu>)

NormaFi-IT - ILNAS // Luxembourg - Juin 2009 - Windows Internet Explorer

http://www.ilnas.public.lu/fr/actualites/evenements/2009/06/normafi-it/index.html

File Edit View Favorites Tools Help

NormaFi-IT - ILNAS // Luxembourg - Juin 2009

GRAND-DUCHÉ DE LUXEMBOURG

INSTITUT LUXEMBOURGEOIS DE LA NORMALISATION, DE L'ACCREDITATION, DE LA SÉCURITÉ ET QUALITÉ DES PRODUITS ET SERVICES

ILNAS

Accessibilité | Aide | A propos du site | Notice légale

Recherche : Recherche avancée

Principaux portails publics

Accueil Nouveau sur ce site | Plan du site | Liens | Feed-back | Contact

ILNAS

NORMALISATION

ACCREDITATION DES OEC

SURVEILLANCE DU MARCHÉ

NOTIFICATION DES OEC

MÉTROLOGIE LÉGALE

BONNES PRATIQUES DE LABORATOIRE

NOTIFICATIONS "RÈGLES TECHNIQUES"

AUTORISATIONS POUR ÉLECTRICIENS

PROMOTION DE LA QUALITÉ

CONFIANCE NUMÉRIQUE

ACTUALITÉS

+ Articles de presse

+ Événements

PUBLICATIONS

LÉGISLATION

RÉCLAMATIONS ET OBSERVATIONS

EXTRANETS

Accueil > Actualités > Événements > Juin 2009 > NormaFi-IT

Confiance numérique

NormaFi-IT

Projet de recherche collaborative

12-06-2009

NormaFi-IT constitue un [projet de recherche collaborative](#) mené par le [CRP Henri Tudor](#), à l'initiative de l'ILNAS.

Conscients du rôle incontournable des technologies de l'information et de la communication (TIC) au cœur de l'économie luxembourgeoise, et de l'impact que la confiance des utilisateurs, tant professionnels que privés, peut avoir dans l'utilisation de ces technologies, l'ILNAS et le CRP Henri Tudor ont souhaité analyser en profondeur la problématique de la confiance numérique.

Ce projet a pour objectif d'explorer le domaine de la confiance numérique sous différents angles.

Les objectifs du projet sont les suivants :

1. Investiguer et développer les domaines de la confiance numérique où l'apport de normes et de standards constitue, a priori, des vecteurs d'innovation et de compétitivité au niveau national ;
2. Développer une approche d'économie de la connaissance normative afin d'établir les liens entre normes, confiance numérique, innovation et compétitivité ;
3. Supporter et développer les activités de normalisation actuellement en cours au Grand-Duché de Luxembourg, dans le domaine des TIC, tant du point de vue des experts intervenants dans des comités de normalisation que de la sensibilisation au niveau des bénéficiaires et potentiels utilisateurs de normes et standards ;
4. Fédérer l'ensemble des parties prenantes du secteur financier afin d'élaborer une stratégie de normalisation pour ce secteur à horizon 3-5 ans ;
5. Investiguer l'opportunité de création de normes nationales spécifiques.

Concrètement, le projet a notamment pour ambition la création d'un état de l'art relatif aux instruments de la confiance numérique, tant au niveau technique qu'au niveau organisationnel. Parmi les instruments étudiés, le domaine des infrastructures à clés publiques (PKI), ainsi que l'archivage électronique bénéficieront d'une attention toute particulière.

Si l'étude spécifique en confirme l'intérêt et la valeur ajoutée, ces travaux pourront servir de support à la création d'une norme nationale, notamment à destination du secteur financier.

Enfin, afin d'atteindre ces objectifs, une recherche doctorale sur la problématique de «*la relation entre confiance numérique et performance numérique*» sera réalisée. Cette recherche s'articulera autour de trois axes principaux :

1. L'évaluation de la valeur des instruments de confiance numérique ;
2. La mesure de la confiance numérique ;

Internet 100%

Futures normes internationales : ISO/IEC 27015 & ISO/IEC 27036 - ILNAS // Luxembourg - Juin 200 - Windows Internet Explorer

http://www.ilnas.public.lu/fr/actualites/evenements/2009/06/normes/index.html

File Edit View Favorites Tools Help

Accueil | Nouveaux sur ce site | Plan du site | Liens | Feed-back | Contact

Principaux portails publics

Recherche : OK Recherche avancée

GRAND-DUCHÉ DE LUXEMBOURG

INSTITUT LUXEMBOURGEOIS DE LA NORMALISATION, DE L'ACCREDITATION, DE LA SECURITE ET QUALITE DES PRODUITS ET SERVICES

ILNAS

Accessibilité | Aide | A propos du site | Notice légale

Accueil > Actualités > Evénements > Juin 2009 > Futures normes internationales : ISO/IEC 27015 & ISO/IEC 27036

Confiance numérique

Futures normes internationales : ISO/IEC 27015 & ISO/IEC 27036

11-06-2009

Un expert du «Comité miroir ISO/IEC/JTC1/SC27 Luxembourg», éditeur de deux futures normes internationales

Deux futures normes internationales (ISO/IEC 27015 & ISO/IEC 27036), du domaine de la sécurité de l'information, comptent désormais un expert du Luxembourg, en tant qu'éditeur.

En effet, à l'issue de la session plénière du comité international ISO/IEC/JTC1/SC 27 «IT Security Techniques» qui s'est déroulée à Beijing (Chine) en mai 2009, M. Benoit Poletti a été nommé, par les pays membres du comité international, éditeur des normes suivantes, d'importance stratégique pour le Grand-Duché du Luxembourg :

- **ISO/IEC 27015 «Information security management guidelines for financial and insurance service»**

Cette norme a pour objectif de décrire les exigences et contrôles d'un système de gestion de la sécurité de l'information spécifiques aux secteurs de la finance et de l'assurance.

- **ISO/IEC 27036 «Guidelines for security of outsourcing»**

Cette norme a pour objectif d'adresser la gestion des risques inhérents aux activités d'outsourcing (l'acquisition et l'usage de services déportés).

Tous ces travaux normatifs sont menés au sein du sous-comité "ISO/IEC/JTC1/SC27" qui traite des développements techniques et organisationnels de la sécurité de l'information, encadrant et permettant de faire évoluer, entre autres, le standard "ISO/IEC 27001" (le certificat associé étant un des instruments essentiels et actuels de la confiance numérique).

Ces travaux sont actuellement supportés, au Luxembourg, par le comité miroir ISO/IEC/JTC1/SC27 Luxembourg, reconnu en tant que tel par ILNAS, et qui compte 12 experts actifs (travail de commentaires, votes, et suivi de l'évolution de ces normes dédiées au domaine de la sécurité de l'information).

ILNAS, en tant qu'Organisme Luxembourgeois de Normalisation, est responsable de la gestion des experts inscrits, et observe notamment attentivement les développements et les travaux actifs du comité miroir ISO/IEC/JTC1/SC27 Luxembourg, via son service de la confiance numérique.

Haut de page

Done Internet 100%



Portrait du cybercrime contemporain

1. Contexte du propos
2. TIC & G-D de Luxembourg
3. Cybercrime contemporain
4. Danger de la « surmédiation » et du « marketing de la peur »
5. Cybercrime & citoyen



Portrait du cybercrime contemporain

Technologies de l'information et de la communication (TIC)

TIC : regroupent les techniques utilisées dans le traitement et la transmission des informations, principalement de l'informatique, de l'Internet et des télécommunications

- > **Un citoyen de la planète sur deux** fait aujourd'hui usage des TIC, de manière active
- > **La majorité de la population mondiale** y est quotidiennement confrontée (active ou passive)

Téléphones mobiles

Internet

Appareils divers (loisirs, santé, enseignement, administrations,...)



Portrait du cybercrime contemporain

Technologies de l'information et de la communication (TIC)

Situation Grand-Duché de Luxembourg

(Source : Statnews n°4/2009 – Statec)

Enquête communautaire sur l'utilisation des TIC par les ménages et les entreprises en 2008

- Près de **80% des ménages** sont connectés à Internet
- G-D de Luxembourg est au **quatrième rang** de l'UE27
- **76% des ménages** disposent d'un accès **large bande**



Portrait du cybercrime contemporain

Technologies de l'information et de la communication (TIC)

Situation Grand-Duché de Luxembourg

(Source : Statnews n°4/2009 – Statec)

Enquête communautaire sur l'utilisation des TIC par les ménages et les entreprises en 2008

- **98% des entreprises informatisées** (10 salariés ou plus) sont connectées à Internet
- Un tiers des entreprises se connectent sans fil à Internet
- **91% avec utilisation large bande**
- **93% des entreprises utilisent l'administration en ligne**



Portrait du cybercrime contemporain

1. Contexte du propos
2. TIC & G-D de Luxembourg
3. **Cybercrime contemporain**
4. Danger de la « surmédiation » et du « *marketing* de la peur »
5. Cybercrime & citoyen



Portrait du cybercrime contemporain

-> Cybercriminalité :

« Ensemble des infractions pénales commises sur les réseaux de télécommunication, en particulier Internet. On distingue les infractions liées aux technologies (virus, piratage, etc.), celles liées aux contenus (racisme, pédophilie, etc.) et celles facilitées par les réseaux (copies illicites de logiciels ou d'œuvres audiovisuelles, etc...) »

Petit Larousse

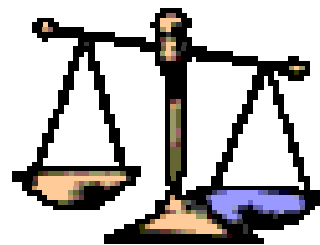


Portrait du cybercrime contemporain

-> Question générale :

Internet

Confiance ou méfiance?





Portrait du cybercrime contemporain

Types d'actions « *underground* » connues – Généralités :

- Accès et maintien frauduleux dans un système d'information
- Lecture illégale des logiciels, fichiers et données
- Altération illégale des données, du fonctionnement du système
- Suppression illégale des données
- Introduction illégale de programmes pirates
- Infraction se rapportant au contenu [pédophilie, ...]
- Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes
- Etc...



Portrait du cybercrime contemporain

Types d'actions « *underground* » connues - Les grandes familles :

- Virus, vers, & chevaux de Troie
- *Adwares, spywares et rootkits*
- Canulars (le *hoax*)
- Tentatives de fraude (fraude dite « à la nigériane »)
- Attaques Web (*defacing*, déni de service distribué, ...)
- Attaques sur la messagerie (*Spam, mass mailing, mail bombing, phishing, pharming*)
- *Botnets* (PC *zombies* suite à une infection virale – estimation de plusieurs millions dans le monde...)
- Le chantage...
- Etc...



Portrait du cybercrime contemporain

- Types d'actions « *underground* » connues

Des statistiques éprouvées

- Explosion d'Internet & développement du « tout numérique » :
- > les relevés d'incidents se sont constamment multipliés, de manière exponentielle
- Plusieurs **indicateurs** permettent de rendre compte de cette activité et d'en dresser le bilan, souvent en termes d'impacts financiers



Portrait du cybercrime contemporain

- Types d'actions « *underground* » connues

Des statistiques éprouvées [Résultats]

- ***Consumer Reports National Research Center*** (cabinet de recherche indépendant américain) qui présente le coût associé au cybercrime en milliards de dollars aux Etats-Unis (8 milliards en 2008 / 7,1 milliards en 2007)

- Etudes du CERT-CC estimant globalement que les pertes associées à des **actes de criminalité** informatique ont **tendance à augmenter**. Les menaces les plus significatives sont généralement externes à l'entité concernée



Portrait du cybercrime contemporain

- Types d'actions « *underground* » connues

Des statistiques éprouvées [Résultats]

- De nombreuses autres études informatives sont aussi disponibles
- > « **Panorama de la cybercriminalité** » édité chaque année par le Club de la Sécurité de l'Information Français (<http://www.clusif.fr>)
- > Enquête annuelle du **CSI/FBI**
 - 2007 : 66 930 950 dollars pertes [198 répondants]
(Accès illicites : 25% ; Attaques « internes » : 59% - [436 répondants – Total : 494])
 - 2008 : 41 560 992 dollars pertes [144 répondants]
(Accès illicites: 29%; Attaques « internes » : 44% - [433 répondants – Total : 522])



Portrait du cybercrime contemporain

- Evolution du cybercrime :

- **Les années 1980 – Le temps des pionniers**
-> 1988 : prise de conscience internationale
- **Les années 1990 – Prise de conscience du phénomène**
-> seconde arrestation de Kevin Mitnick, recherché par le FBI pendant 7 ans
- **Les années 2000 – Le champ de bataille « Internet »**
-> des centaines de milliers d'internautes dans le monde reçoivent une déclaration d'amour : « *I Love You* » (virus de type ver)
- **Les années 2010 – Le cybercrime contemporain**
-> le cybercrime devient réellement « organisé »...



Portrait du cybercrime contemporain

- Les années 2010 – Le cybercrime contemporain (ou la cybercriminalité aujourd'hui)
- De quoi parle t-on?
 - Cyberpetitedélinquance
 - Cyberdélit
 - **Cybercrime**
 - *Hackers*
 - **Crackers -> cybercriminels**
 - *Script kiddies*



Portrait du cybercrime contemporain

- **Les années 2010 – Le cybercrime contemporain**
(ou la cybercriminalité aujourd'hui)
- > le cybercrime devient réellement « organisé »...
- Les pratiques et technologies de cybercrime apparaissent de plus en plus sophistiquées
- Les attaques semblent de plus en plus nombreuses
- Les systèmes d'information et de communication sont exposés et potentiellement vulnérables
- Le nombre d'incidents de sécurité progresses
- Le vol d'informations [personnelles, confidentielles] et l'appât du gain : **nouvelles convoitises**



Portrait du cybercrime contemporain

- **Les années 2010 – Le cybercrime contemporain**
-> **le cybercrime fait partie de la vie quotidienne...**
- **Fragilité des sites de réseaux sociaux**
[associé au nouveau « terrain de chasse » représenté par Web 2.0]
-> Espionnages divers aussi en augmentation, facilités par les informations disponibles facilement *via* les **sites communautaires**
- **Explosion**
du nombre de **virus** [le cap de 1 million de logiciels malveillants (*malware*) franchi fin juillet 2008, selon F-Secure (rapport de sécurité premier trimestre 2009)]. Avec un taux de 2 300 nouvelles détections par jour, le nombre de *trojans*, *backdoors*, *exploits* et autres menaces a été doublé depuis la fin 2007...
- **Le piratage rapporte désormais plus que le trafic de drogue!**



Portrait du cybercrime contemporain

- **Les années 2010 – Le cybercrime contemporain**
 - > le cybercrime fait partie de la vie quotidienne... [car les TIC font partie de la vie quotidienne]
 - > Internet connaît donc aussi le crime organisé : transposition de la société « classique »
 - > Le cybercrime contemporain apparaît structuré :
 - **Des réseaux**
 - **Des organisations**
 - **Une économie souterraine qui rapporte**
 - > Une véritable économie de services



Portrait du cybercrime contemporain

- Les années 2010 – Le cybercrime contemporain

-> Le cybercrime d'aujourd'hui

Un véritable « *business* » :

- Une activité pratiquée d'abord pour l'argent : une source de rémunération
- Loin des années 1990 et 2000 : actes de piratages souvent ludiques, parfois politiques [virus pandémiques sans charge malicieuse; des pirates amateurs agissant par révolte, passion ou *ego*]
- Ces actes d'hier n'ont pas disparu mais ont été dépassés par l'appât du gain



Portrait du cybercrime contemporain

- Les années 2010 – Le cybercrime contemporain

-> Le cybercrime d'aujourd'hui

Caractéristiques des cybercriminels contemporains :

- Souvent d'anciens informaticiens ayant perdus leur travail
- Ou encore avec des niveaux de salaires très faibles
 - > Se sont laissés tenter par la fraude et l'appât du gain
 - > Ont développé une économie parallèle
 - > Aidés d'une véritable chaîne logistique



Portrait du cybercrime contemporain

- Les années 2010 – Le cybercrime contemporain

-> Le cybercrime d'aujourd'hui

Caractéristiques des actes de cybercrime contemporain :

- Hébergement illicite (*Spam...*)
- Contrefaçon (logicielle et matérielle)
- Codes malicieux (*Malwares*)
- Fraude aux moyens de paiement
- Fraude aux jeux
- ...



Portrait du cybercrime contemporain

- Les années 2010 – Le cybercrime contemporain

-> Le cybercrime d'aujourd'hui

- Hébergement illicite (*Spam...*)

-> Au niveau international : existence de nombreux hébergeurs « malhonnêtes »

-> Souvent hébergement de contrôleur de « botnets », de contenu « illégal » (fichiers protégés par des droits d'auteurs, *phishing*, pédophilie, ...), serveur dédié d'envoi de *spams* clé en main...

-> Coupures d'accès par les *providers* Internet à ces sites « illégaux » : une baisse du *spam* au niveau international de 50-60% + baisse des transactions bancaires frauduleuses...



Portrait du cybercrime contemporain

- **Les années 2010 – Le cybercrime contemporain**
 - > Le cybercrime d'aujourd'hui
 - Contrefaçon (logicielle et matérielle)
 - > Domaine généralisé sur Internet
 - > Facilité de se procurer très rapidement :
 - Des logiciels contrefaits
 - Des objets de tout type également : médicaments, vêtements de luxe, lunettes de marque...
 - Musique et films piratés...



Portrait du cybercrime contemporain

- **Les années 2010 – Le cybercrime contemporain**
 - > Le cybercrime d'aujourd'hui
 - Codes malicieux (*malwares*)
 - > Nouvelles versions d'attaques *via* les téléphones portables
 - > Attention aux « *Rogue Software* » : exemple de faux logiciels de lutte contre les virii/malwares
 - > Redirection vers des sites à contenu illicite ou introduction illégale dans d'autres systèmes informatiques



Portrait du cybercrime contemporain

- **Les années 2010 – Le cybercrime contemporain**
 - > Le cybercrime d'aujourd'hui
 - Fraude aux jeux
 - > Faux sites de paris en ligne
 - > Fausse loterie
 - > Souvent il est illégalement demandé au « gagnant » de s'acquitter d'une certaine somme
 - > Signalement général de ces fraudes (Microsoft, Yahoo!, ...)

De : Francoise Maguerite [structure.megamillion@yahoo.co.th]

Date : mar. 05/05/2009 14:44

À : structure.megamillion@yahoo.co.th

Cc :

Objet : RECLAMATION DE VOTRE GAIN !!!!!!!!!!!

Pièces jointes : FORMULAIRE MEGAMILLIONNAIRE 2009.doc

!!!!!! MEGAMILLIONS MARC ANDERSSEEN PRICE EUROPE AFRIQUE LOTERIE !!!!!!!

Nous avons le plaisir de vous informer du tirage au sort du programme de la LOTERIE MEGAMILLION MARC ANDERSSEN PRICE qui s'est tenu le 14 janvier 2009 à Londres. Votre adresse électronique attachée à un numéro de ticket: 69475600545-721 avec Numéro de série : 8867/04 a tiré les chiffres gagnants : MMAP-007823-11-03-V, qui vous ont par la suite permis de gagner dans la 2ème catégorie. Vous avez donc, été tiré au sort pour bénéficier d'une somme totale 50.000 € en liquide, crédité au fichier KPC/9080118308/02.

PROEDURE DE REMISE DE GAIN

Veuillez envoyer vos coordonnées par mail a l'adresse électronique de Maître JEAN ERIC FRANCOIS huissier chargé de vous indiquer les conditions générales de remise de votre gain

Email : cabinet_juridique_eric@yahoo.co.th

Tel : 00225 45 59 95 33

Si vous ne souhaitez pas que vos données soient transmises à nos partenaires à des fins de prospection commerciale, écrivez - nous au Siège Social.

PRESIDENT DU CONSEIL EXECUTIF
MEGAMILLIONS MARC ANDERSSEEN PRICE
EUROPE AFRIQUE CARAIBES LOTERIE ET CASINO
MIKKI HAROLD



Portrait du cybercrime contemporain

- **Les années 2010 – Le cybercrime contemporain**
 - Autre dimension
 - > Des spécialistes cybercriminels selon activité
 - > Gestion des compétences entre cybercriminels
 - > Echanges de compétences entre cybercriminels
 - > Transferts et regroupements en diverses communautés de cybercriminels



Portrait du cybercrime contemporain

- **Les années 2010 – Le cybercrime contemporain**
 - Autre dimension
 - > Cybercrime adopte le modèle traditionnel de l'entreprise
 - > Gestion de l'offre, de la demande, gestion de commandes, de ressources humaines
 - > Réseau de sous-traitance
 - > Offre de cyberemplois... : experts en faille, créateurs de chevaux de Troie, ...
 - > Services de qualité offerts par des « hébergeurs malhonnêtes » : mais plus coûteux...



Portrait du cybercrime contemporain

- **Les années 2010 – Le cybercrime contemporain**
 - Autre dimension
 - > Succès des ventes illégales :
 - > données de cartes de crédit
 - > données personnelles (compte de messagerie)
 - > données bancaires
 - > jeux piratés
 - > ...



Portrait du cybercrime contemporain

- **Les années 2010 – Le cybercrime contemporain**

-> Le cybercrime d'aujourd'hui

Deux axes d'actions :

- **Les attaques ciblées**
- **Les attaques massives**



Portrait du cybercrime contemporain

- Les années 2010 – Le cybercrime contemporain

-> Le cybercrime d'aujourd'hui

Les attaques ciblées :

- Cibles : les ordinateurs des particuliers
- Cibles : les entreprises (ou autres entités économiques)



Portrait du cybercrime contemporain

- **Les années 2010 – Le cybercrime contemporain**

-> Le cybercrime d'aujourd'hui

Les attaques ciblées :

- Cibles : les ordinateurs des particuliers
- Automatisation et propagation (vers, *mass-mailing...*)
- Intégration de la machine dans un réseau de *zombies*
- Collectes d'informations personnelles monnayables
- Chiffrement de fichiers en vue de chantage



Portrait du cybercrime contemporain

- **Les années 2010 – Le cybercrime contemporain**

-> Le cybercrime d'aujourd'hui

Les attaques ciblées :

- Cibles : les entreprises
- Attaques vers les ressources critiques :
 - > Données confidentielles
 - > Flux financiers
 - > Disponibilités de service
- Attaques plus complexe que pour un particulier



Portrait du cybercrime contemporain

- **Les années 2010 – Le cybercrime contemporain**

-> Le cybercrime d'aujourd'hui

Les attaques massives :

- Cybercriminels contemporains : adeptes des opérations massives
- Attaques au hasard - A grande échelle
- Statistique veut que sur un grand nombre d'attaques, il existe un certain taux de succès, même mince
- Des outils à la hauteur des moyens engagés



Portrait du cybercrime contemporain

- Les années 2010 – Le cybercrime contemporain

Les attaques massives :

- Cybercriminels contemporains :
- Proposition de kits de piratage « prêts à l'emploi »
 - > Chevaux de Troie conçus sur mesure et vendus en kit
 - > Diffusion de chevaux de Troie s'appuyant sur des outils d'infection automatisés
 - > Sites de *phishing* vendus entièrement packagés



Portrait du cybercrime contemporain

- Les années 2010 – Le cybercrime contemporain

Les attaques massives :

- Niveau des attaques peu évolué reposant sur des outils de piratages classiques

Exemples :

- De type *phishing*
- De type attaque de serveurs e-commerce (recherche d'identifiants)

Rentabilité par nature, même une faible proportion de victimes finales permettra des bénéfices conséquents



Portrait du cybercrime contemporain

1. Contexte du propos
2. TIC & G-D de Luxembourg
3. Cybercrime contemporain
4. Danger de la « surmédiation » et du « *marketing* de la peur »
5. Cybercrime & citoyen



Portrait du cybercrime contemporain

-> Le *marketing* de la peur entraîne et renforce la méfiance par rapport aux TIC

-> Ce *marketing* est souvent peu fondé, mal construit voire complètement faux dans certains cas

-> « *Pearl Harbor électronique* »

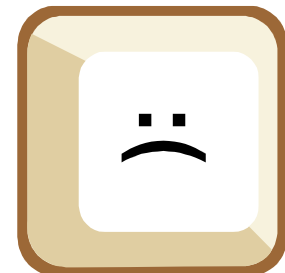
-> « *Shutdown général d'Internet* »

-> « *Cyberguerres* »

-> « *Bataillon de cyberguerriers* »

-> « *Absence de solutions efficaces* »

-> ...





Portrait du cybercrime contemporain

-> L'effet de « *Buzz* »...

-> Monde journalistique reprend souvent « trop » rapidement les informations « à sensation » et relatives à Internet

-> Notamment lorsque l'effet d'annonce « Internet va s'écrouler » est en vogue

-> Exemple récent : faille DNS (*Domain Name System*) révélée « trop tôt » en juillet 2008

-> Reprise exponentielle journalistique de ces données

-> En se basant sur les stricts propos du « découvreur » de la faille en question

-> Problème réel, technique, concernant exclusivement les fournisseurs d'accès Internet et leurs administrateurs réseaux



Portrait du cybercrime contemporain

-> L'effet de « *Buzz* »...

-> Quasiment chaque année le monde journalistique évoque :

« *C'est très grave... Internet va s'effondrer...* »

« *Nous sommes impuissants, qu'allons-nous devenir ?...* »

-> Contexte de mélange malsain

- Entre compétences techniques, réalité des risques afférents à toute technologie de pointe

- Avec les représentations sociales / Internet « destabilisées » par ces effets d'annonce proches du « sensationnel recherché »...



Portrait du cybercrime contemporain

2008 fut l'occasion de nombreuses allégations de presse « malheureuses » :

- Faille TCP (*Transmission Control Protocol*) exagérément relayée
 - Dans la boucle, faille SNMP (*Simple Network Management Protocol*) déjà connue fut aussi relayée
 - Entraînant des « surenchères » jusqu'à l'annonce par le monde journalistique du « *Lundi noir des virus* »
- > Il ne s'est rien passé...



Portrait du cybercrime contemporain

Souvent les failles « côté client » sont bien plus dangereuses que celles « côté serveur » :

- > Car « clients » plus nombreux
- > Pas sous surveillance constante de l'administrateur
- > Absence de sensibilisation, de vigilance
- > Cibles potentielles de choix pour les pirates informatiques
 - > Avis importants des failles des systèmes d'exploitation, souvent traités à un même niveau d'importance, alors que certains sont jugés critiques pour les utilisateurs finaux
 - > D'autres failles « HTTPS », « RFID », ... passent ainsi inaperçues...



Portrait du cybercrime contemporain

Pourtant le rôle du monde journalistique est primordial pour la sensibilisation des utilisateurs finaux et pour le grand public

- > Un acteur du monde de la sécurité de l'information
- > Un acteur de l'information sur la sécurité
- > Pour atteindre efficacement la « couche 8 »...
- > La connaissance des couches inférieures peut s'avérer importante, voire nécessaire
- > Privilégier l'information des problèmes réels du citoyen pouvant se poser quant aux usages d'Internet, par exemple
- > Rejoint la problématique des « *forçats de l'information* » (sites d'informations en ligne) qui fonctionnent comme du journalisme continu (de type radio (parfois en lien direct avec le téléspecteur) – sans réellement avoir le temps de vérifier avec pertinence l'information



Portrait du cybercrime contemporain

-> Donc : attention aux articles vite rédigés par des journalistes, que certains vulgarisent sous le vocable : « *low-cost* »...

-> Exemple du témoignage récent de ce type de journaliste

- Travail de rédaction souvent bâclé
- « Copier-coller » des dépêches d'agences « *...en reformulant vaguement, sans jamais vérifier, faute de temps ...* »
- Logique d'être les premiers à mettre l'information en ligne « *afin d'être repéré par Google ...* »
- « *Le plus important est de faire le boulot à toute vitesse* »...



Portrait du cybercrime contemporain

-> Sans vouloir généraliser, ni diaboliser

-> Internet n'est pas « uniquement » un outil dangereux colporteur de « rumeurs »

-> Le journalisme sur Internet dispose d'un formidable potentiel qui demeure en attente de moyens adaptés

-> Vers du journalisme de type professionnel...

-> Souvent des journalistes professionnels qui rédigent de très bons articles

-> Ces derniers sont bien informés et participent par le fait aux campagnes de sensibilisation vers le grand public



Portrait du cybercrime contemporain

-> Exemple de « bizarrerie » d'un article de la presse :

- Reprenant l'âge approximatif des « cybercriminels » :
 - « Créateurs de chevaux de Troie » : environ 26 ans
 - « Expert en failles » : environ 23 ans
 - « Cyberescroc » : 18-45 ans
 - « Vendeur de trafic web » : environ 32 ans
 - « Hébergeur sans scrupules » : environ 45 ans

-> Source citée, mais :

- Crédibilité?
- Peut-on affecter une classe d'âge à une catégorie virtuelle de pirates informatiques?
- Données d'une recherche scientifique en criminologie et/ou en statistique?



Portrait du cybercrime contemporain

1. Contexte du propos
2. TIC & G-D de Luxembourg
3. Cybercrime contemporain
4. Danger de la « surmédiatisation » et du « *marketing* de la peur »
5. **Cybercrime & citoyen**



Portrait du cybercrime contemporain

-> Question générale :

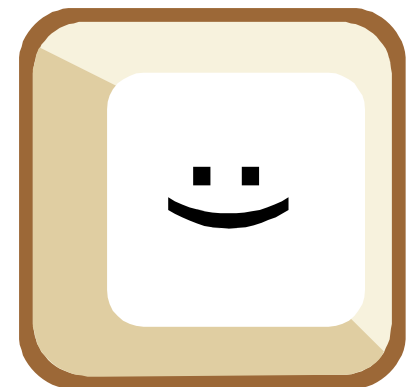
Internet



Confiance!

=

[Vigilance + connaissance]





Portrait du cybercrime contemporain

Le cybercrime contemporain et le citoyen :

- > Le cybercrime n'est pas de la responsabilité du citoyen
- > La mission de lutte contre cette menace est du ressort des pouvoirs publics
- > Le citoyen doit être conscient du fait, de son existence
- > Des outils et structures, au plan national, sont à disposition :
 - > La législation
 - > La sensibilisation
 - > L'attention citoyenne



Portrait du cybercrime contemporain

-> Des outils à disposition

Le cadre de loi luxembourgeois :

« *Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement ou de transmission automatisé de données sera puni d'un emprisonnement de deux mois à deux ans et d'une amende de 500 euros à 25000 euros ou de l'une de ces deux peines* »
[article 509-1 du Code pénal]

+ « *modification ou suppression de données* » [articles 509-1 al. 2 et 509-3 du Code pénal]

+ « *le fait d'entravé ou faussé le fonctionnement d'un système de traitement ou de transmission automatisé de données* » [article 509-2 du Code pénal]



Portrait du cybercrime contemporain

-> Des outils à disposition

Le cadre de loi luxembourgeois :

« La tentative des délits prévus par les articles 509-1 à 509-5 est punie des mêmes peines que le délit lui-même » [article 509-6 du Code Pénal]

+ « Association de malfaiteurs informatiques » [article 509-7 du Code Pénal]



Portrait du cybercrime contemporain

-> Des outils à disposition

Le cadre de loi luxembourgeois :

-> http://www.cases.public.lu/fr/publications/fiches/pdf/Depot_de_plainte.pdf

- Procédure de dépôt de plainte :

- En se déplaçant dans un commissariat de police

- Par écrit au procureur d'Etat

Il faut porter plainte auprès du procureur d'Etat du lieu où l'infraction a été commise :

Pour l'arrondissement judiciaire de Luxembourg (cantons de Luxembourg, Capellen, Esch, Grevenmacher, Mersch et Remich)
Procureur d'Etat
Palais de Justice de Luxembourg
B.P.15
L-2010 Luxembourg

Pour l'arrondissement judiciaire de Diekirch (cantons de Diekirch, Clervaux, Echternach, Redange, Vianden et Wiltz)
Procureur d'Etat
Tribunal d'Arrondissement de Diekirch
B.P. 164
L-9202 Diekirch



Portrait du cybercrime contemporain

-> Des outils à disposition

Le cadre de loi luxembourgeois :

- Possibilité d'une plainte avec constitution de partie civile (en vue d'obtenir réparation du préjudice subi)
- http://www.cases.public.lu/fr/publications/fiches/pdf/Depot_de_plainte.pdf

Il faut se constituer partie civile auprès du juge d'instruction (article 56 du Code d'instruction criminelle).

Pour l'arrondissement judiciaire de Luxembourg (cantons de Luxembourg, Capellen, Esch, Grevenmacher, Mersch et Remich)
Cabinet d'instruction Palais de Justice de Luxembourg
B.P.15
L-2010 Luxembourg

Pour l'arrondissement judiciaire de Diekirch (cantons de Diekirch, Clervaux, Echternach, Redange, Vianden et Wiltz)
Cabinet d'instruction Tribunal d'Arrondissement de Diekirch
B.P. 164
L-9202 Diekirch



Portrait du cybercrime contemporain

-> Des outils à disposition

La sensibilisation :

-> Le projet *Cyberworld Awareness and Security Enhancement Structure* – <http://www.cases.public.lu> (Ministère de l'Économie et du Commerce extérieur)

-> Le service de la confiance numérique ILNAS (Ministère de l'Économie et du Commerce extérieur)

-> Le Club de la Sécurité des Systèmes d'Information Luxembourgeois (CLUSSIL – <http://www.clussil.lu>)

-> Le Comité de Normalisation Luxembourgeois pour la Sécurité de l'Information (CNLSI – <http://www.ansil.eu>)

-> Centre de Recherche Public Henri Tudor, Université du Luxembourg...



Portrait du cybercrime contemporain

-> Des outils à disposition

L'attention citoyenne :

- La **vigilance**
- L'adoption des **bonnes pratiques de sécurité**
- La mise en place d'une **stratégie de protection**
- Le **principe de précaution**
- Les « **10 commandements de la sécurité sur Internet** »
[<http://www.securite-informatique.gouv.fr>]



Portrait du cybercrime contemporain

-> Des outils à disposition

L'attention citoyenne :

-> « 10 commandements de la sécurité sur Internet »

« - *Utiliser des mots de passe de qualité*

- *Avoir un système d'exploitation et des logiciels à jour : navigateur, antivirus, bureautique, pare-feu personnel*

- *Effectuer des sauvegardes régulières*

- *Désactiver par défaut les composants ActiveX et Javascript*

- *Ne pas cliquer trop vite sur des liens*



Portrait du cybercrime contemporain

-> Des outils à disposition

L'attention citoyenne :

-> « 10 commandements de la sécurité sur Internet »

- *Ne jamais utiliser un compte administrateur pour naviguer*

- *Contrôler la diffusion d'informations personnelles*

- *Ne jamais relayer de canulars*

- *Soyez prudents : Internet est une rue peuplée d'inconnus!*

- *Soyez vigilant avant d'ouvrir des pièces jointes à un courriel : elles colportent souvent des codes malveillants »*



Accueil A propos Contact Plan du site Liens

Accueil

Objectifs de LISA Stop Line

Le projet LISA Stopline a pour objectifs de fournir une structure de signalement anonyme pour les contenus illégaux rencontrés sur Internet, et de traiter ces signalements en collaboration avec les autorités compétentes au niveau national et international.

Au travers de son site web et de sa hotline gratuite, LISA Stopline propose ainsi au public deux moyens d'agir civiquement contre les contenus illégaux visible dans cet espace public qu'est Internet.



Signalez aussi votre contenu via notre hotline 8002-6767

LISA Stopline vous propose également de signaler votre contenu illégal via sa hotline gratuite et anonyme, ouverte du lundi au vendredi, de 9:00 à 12:00 et de 14:00 à 17:00.

Retrouvez toutes les informations relatives aux signalements sur notre page «signalement, mode d'emploi»
[En savoir plus](#)

Qu'est-ce qu'un contenu illégal ?

Internet permet aujourd'hui à tout un chacun de mettre en ligne ses propres contenus.

Il existe cependant certains types de contenus qui sont contraires à la Loi : pornographie infantile, racisme, discrimination.
[En savoir plus](#)

Qui sommes-nous ?

LISA Stopline est un projet géré par un consortium national et subventionné par la Commission Européenne dans le cadre du programme Safer Internet Plus.
[En savoir plus](#)

Suivez l'état de votre signalement ▶



▶ [Signalement, mode d'emploi](#)

Pour un Internet plus sûr



Internet est une formidable source d'informations et de divertissements pour les jeunes, mais non dénuée de risque.

LuSI est là pour vous aider à y voir plus clair.

[Visiter le site web de LuSI](#)

Avec le soutien de





- ILNAS
- NORMALISATION
- ACCREDITATION DES OEC
- SURVEILLANCE DU MARCHÉ
- NOTIFICATION DES OEC
- MÉTÉOROLOGIE LÉGALE
- BONNES PRATIQUES DE LABORATOIRE
- NOTIFICATIONS "RÈGLES TECHNIQUES"
- AUTORISATIONS POUR ÉLECTRICIENS
- PROMOTION DE LA QUALITÉ
- CONFIANCE NUMÉRIQUE

ACTUALITÉS

- Articles de presse
- Événements
- PUBLICATIONS
- LÉGISLATION
- RÉCLAMATIONS ET OBSERVATIONS
- EXTRANETS

Accueil > Actualités > Événements > Mai 2009 > Un guide du numérique pour les consommateurs en ligne : le "eYou Guide"

Confiance numérique

Un guide du numérique pour les consommateurs en ligne : le "eYou Guide"

05-05-2009

L'Union européenne a présenté, en date du 05 mai 2009, le "eYou Guide", permettant aux consommateurs de connaître leurs droits et obligations sur Internet, tels qu'ils existent actuellement au sein des lois européennes.

Actuellement, bien que le commerce électronique progresse en Europe (la proportion des consommateurs, qui ont acheté au moins un article sur Internet, est passée de 27% en 2007 à 33% en 2008), la méfiance semble encore, cependant, de mise quant à des achats faisant l'objet de transactions en ligne, notamment hors des frontières.

"A l'intérieur de l'Union européenne, les droits des consommateurs effectuant des achats en ligne ne doivent pas diverger en fonction du pays dans lequel l'entreprise ou le site Internet est implanté", a expliqué Mme Viviane Reding, commissaire en charge de la société de l'information et des médias. De même, Mme Meglena Kuneva, commissaire responsable de la protection des consommateurs, a indiqué : "Si nous voulons que les consommateurs fassent des achats hors des frontières et exploitent le potentiel des communications digitales, alors nous devons leur donner l'assurance que leurs droits sont garantis".

Actuellement, "39% des consommateurs ont des doutes quant à la sécurité des achats en ligne et 42% n'osent pas acheter sur Internet", a précisé Mme Viviane Reding. Selon la Commission européenne, le "eYou Guide" devrait permettre d'instaurer la confiance et donner une impulsion nouvelle au commerce en ligne transfrontalier.

Le site Internet "eYou Guide" permet donc d'apporter une vue d'ensemble des droits et obligations sur Internet, selon les lois européennes et nationales, mais également des informations dans les domaines suivants :

- La sécurité sur Internet,
- La protection de la vie privée et des données personnelles sur Internet,
- Les règles sur les publicités en ligne,
- Les obligations des prestataires de services ou des vendeurs, en regard des utilisateurs et des consommateurs,
- Les droits d'auteurs sur Internet...
- Le site Internet "eYou Guide" sera continuellement mis à jour par la Commission européenne.

Pour en savoir plus

→ [Article publié sur le portail cases.lu : "eYou Guide - Une initiative européenne bienvenue"](#)



Portrait du cybercrime contemporain - Conclusion

- Des dangers sont réels : le cybercrime s'est installé pour durer
- Le cybercrime est désormais une activité rentable
- En réponse : des compétences et des solutions techniques existent
- Nécessité de se tenir informé [domaine sécurité]
- Développez une approche « critique » et « objective »
- « *Ne pas noircir le tableau* » [sans raison]
- Profitez « pleinement » de l'économie numérique [mais en connaissance de cause]
- **Utilisez Internet et les technologies de l'information!**
- **Informez-vous sur le sujet!**
- Privilégiez les marqueurs de la confiance [si possible] en restant attentifs à leur développement...



MINISTÈRE DE L'ÉCONOMIE
ET DU COMMERCE EXTÉRIEUR

ILNAS

Grand-Duché de
luxembourg.

Portrait du cybercrime contemporain

Merci pour votre attention

jean-philippe.humbert@ilnas.etat.lu

*

«Les mondes de la cyberdélinquance et images sociales du pirate informatique»

[<http://www.ilnas.public.lu/fr/publications/confiance-numerique/etudes-nationales/memoire-phd-jp-humbert.pdf>]

[http://www.cases.public.lu/fr/publications/recherche/these_jph/Memoire_PHD_JP_Humbert.pdf]