enisa
European Network and Information Security Agency

Sécurité des réseaux d'information dans l'éducation

Contribution consolidée de l'ENISA

Janvier 2012

Remerciements

Le présent rapport est le fruit d'un effort collectif du ministère luxembourgeois de l'économie et du commerce extérieur et de l'ENISA. L'ENISA tient à remercier M. François Thill, directeur adjoint des communications, et son équipe pour leur coopération ouverte et constructive qui a abouti à cette publication.

À propos de l'ENISA

L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) est un centre d'expertise sur la sécurité des réseaux et de l'information pour l'Union européenne, ses États membres, le secteur privé et les citoyens européens. L'ENISA œuvre avec ces groupes à la formulation d'avis et de recommandations relatives aux bonnes pratiques en matière de sécurité des informations. Elle prête son assistance aux États membres de l'Union européenne pour appliquer la législation européenne en vigueur et s'efforce d'améliorer la résilience de l'infrastructure et des réseaux de communication critiques de l'Europe. L'ENISA vise à améliorer l'expertise existant au sein des États membres de l'Union en soutenant le développement de communautés transfrontalières engagées dans l'amélioration de la sécurité des réseaux et de l'information partout au sein de l'Union européenne. Des compléments d'information à propos de l'ENISA et de ses travaux sont accessibles à l'adresse www.enisa.europa.eu.

Coordonnées

Pour contacter l'ENISA ou poser des questions d'ordre général sur la sécurité des réseaux d'information dans l'éducation, vous pouvez vous adresser à:

Daria Catalui, Sécurité des réseaux dans l'éducation gestion des parties prenantes, expert national détaché, ENISA

Courriel: daria.catalui@enisa.europa.eu

Louis Marinos, expert en analyse et gestion du risque, ENISA

Courriel: louis.marinos@enisa.europa.eu

Internet: http://www.enisa.europa.eu

Avis juridique

Tables des matières

1 Résumé

Le rapport sur la sécurité des réseaux d'information (SRI) dans l'éducation paraît à un moment où l'éducation et les TIC sont plus interreliées et interconnectée que jamais. Pour le citoyen engagé activement dans le numérique, le défi consiste à rester informé des nouveautés du domaine dynamique des TIC et de la sécurité de l'information en particulier.

L'éducation tout au long de la vie, l'éducation formelle, non formelle et informelle sont à l'ordre du jour des décideurs politiques. Les enfants, les jeunes et leurs camarades, leurs parents et le personnel enseignant font tous partie du débat et il leur est recommandé de coopérer et de s'engager le plus possible.

Par «sécurité des réseaux d'information dans l'éducation», nous entendons la transmission d'informations de base sur la sécurité aux jeunes qui utilisent l'internet.

Notre intention est de mettre en marche le processus de transfert de savoir entre tous les acteurs associés afin d'obtenir des résultats durables ayant une incidence réelle sur le citoyen européen engagé dans le numérique. Une manière d'y parvenir consiste à diffuser les résultats du travail réalisé ces dernières années par l'ENISA en utilisant un langage compréhensible par le groupe cible. Nous avons résumé les conclusions des rapports ENISA au moyen d'informations concises présentées sous la forme de fiches. Les parties intéressées peuvent lire et utiliser ce matériel et, si nécessaire, rechercher des compléments d'information dans les documents intégraux. La sélection des rapports a été effectuée de manière à diffuser un contenu pertinent susceptible d'être directement mis à profit à des fins éducatives.

Outre la fiche, nous souhaiterions attirer l'attention, dans le rapport, sur l'excellent travail réalisé par une série d'organisations (nationales et internationales). Pour être à jour et utiliser les informations les plus pertinentes, nous recommandons certaines lectures dans l'annexe «Travaux connexes» (Annexe III: Travaux connexes).

Dans la politique phare de la Commission européenne dans ce domaine, « Une stratégie numérique pour l'Europe»[1], il est souligné que «*l'engagement des jeunes fera de la stratégie numérique une réalité»*. Les informations contenues dans le présent rapport consolidé soutiennent le processus visant une meilleure information, une meilleure éducation et un meilleur engagement implication dans le domaine de la SRI, contribuant ainsi aux objectifs de la stratégie numérique.

[1] http://blogs.ec.europa.eu/neelie-kroes/youth-engagement-will-make-the-digital-agenda-a-reality/ *(consulté le 25 octobre 2011)*

2 Introduction

Le présent document a pour objectif de fournir une version consolidée des résultats disponibles de l'ENISA sous une forme susceptible d'être utilisée à des fins éducatives. Le matériel vise l'enseignement primaire et, en particulier, le personnel enseignant, les parents et, dans une certaine mesure, les adolescents.

Il s'agissait de simplifier les documents de l'ENISA dans ce domaine et de leur donner une forme facilitant leur adaptation à des objectifs éducatifs, l'identification des compétences nécessaires et/ou une utilisation directe par les acteurs concernés. Notre objectif n'est pas de remplacer un excellent matériel existant dans ce domaine, mais plutôt de retirer des informations concises du travail réalisé par l'ENISA, lesquelles pourront trouver facilement leur place dans le matériel éducatif existant. Le texte utilisé pour les sujets présentés ci-dessous a été extrait de publications de l'ENISA.

Le présent travail est le fruit d'une coopération fructueuse entre le ministère luxembourgeois de l'économie et du commerce extérieur et l'ENISA: sur la base de la structure du matériel éducatif disponible dans les États membres, le matériel existant de l'ENISA a été «digéré» afin d'être utilisé par les États membres. À l'issue d'une interaction avec divers acteurs, nous avons établi une brève liste de documents de l'ENISA dans les domaines suivants:

- intimidation électronique / manipulation psychologique en ligne[2];
- les enfants et les mondes virtuels[3];
- quiz de sensibilisation[4];
- lignes directrices à l'intention des parents, des tuteurs et des éducateurs[5];
- la sécurité sur les réseaux sociaux en ligne[6];
- cookies[7];
- la sécurité dans les mondes virtuels[8]; et
- impression sécurisée[9]

---

[2] https://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/Cyber-Bullying%20and%20Online%20Grooming/

[3] http://www.enisa.europa.eu/act/ar/deliverables/2008/children-on-virtual-worlds

[4] http://www.enisa.europa.eu/act/ar/deliverables/2008/ar-quizzes-templates-en

[5] http://www.enisa.europa.eu/act/ar/deliverables/2009/cop_initiative?searchterm=guidelines+for+parents+%2C+guardians

[6] http://www.enisa.europa.eu/act/it/past-work-areas/social-networks/security-issues-and-recommendations-for-online-social-networks

[7] http://www.enisa.europa.eu/act/it/library/pp/cookies/?searchterm=cookies

[8] http://www.enisa.europa.eu/act/it/past-work-areas/massively-multiplayer-online-games-and-social-and-corporate-virtual-worlds/security-and-privacy-in-virtual-worlds-and-gaming

[9] http://www.enisa.europa.eu/act/ar/deliverables/2008/secure-printing

Le format choisi pour présenter les informations adopte la structure suivante:

- une brève description du thème/domaine,
- une référence aux principales conclusions/recommandations,
- une référence au document intégral, et
- un ensemble de diapositives pouvant être présentées dans le cadre d'un exposé.

Notre objectif est de permettre aux parties prenantes concernées d'extraire les objectifs d'apprentissage des informations consolidées et de les intégrer dans leurs approches. Étant partis de la supposition que les informations contenues dans le présent rapport seront réutilisées et adaptées à des besoins éducatifs particuliers et à des méthodes existantes, nous n'avons pas apporté de soin particulier à la mise en page.

Il convient de noter que le présent matériel est une compilation des travaux de l'ENISA en la matière qui ont été élaborés au cours de ces 3-4 dernières années.

2.1 Public cible

Comme indiqué dans le programme de travail 2011[10], l'Agence soutient un dialogue ouvert avec différentes parties prenantes et, pour cette raison, elle entretient des relations étroites avec l'industrie, le monde académique et les utilisateurs. Aussi, le présent rapport vise tous les groupes de parties prenantes qui ont un intérêt pour la question de la SRI et de l'éducation.

Comme nous l'avons souligné plus haut, le présent rapport s'adresse à toute personne concernée par l'enseignement primaire. Il s'agit notamment des parents, des tuteurs et des éducateurs, des autorités responsables des États membres (par exemple les ministères, les organisations nationales en rapport avec l'éducation, les organisations bénévoles, les groupes d'intérêt, etc.). En outre, le présent matériel peut être utilisé par les adolescents eux-mêmes pour obtenir un aperçu des différentes questions de SRI dans les domaines cités.

[10] http://www.enisa.europa.eu/about-enisa/activities/programmes-reports/work-programme-2011/view *(consulté le 25 octobre 2011)*

3 Travaux

Ces dernières années, une série de rapports et d'articles ont porté sur la question de la SRI dans l'éducation. Nous avons choisi de citer certaines des sources afin de fournir un aperçu général du matériel existant dans ce domaine.

Rapport final du réseau «EU kids online»[11]: évocation des orientations politiques nécessaires dans le domaine

Il s'agit d'un rapport publié par le réseau «EU Kids online». «*'EU Kids online' vise à améliorer la connaissance des expériences et pratiques des enfants européens et de leurs parents concernant l'utilisation à risque de l'internet et des nouvelles technologies en ligne et une utilisation plus sûre de ces technologies, afin de disposer d'informations sur la manière de créer un environnement en ligne plus sûr pour les enfants.»*[11]. Les principales questions abordées sont les suivantes:

- encourager les enfants à se consacrer à davantage d'activités en ligne améliorera leurs compétences numériques;
- l'enseignement de compétences en matière de sécurité est susceptible d'améliorer d'autres compétences, tandis que l'enseignement de compétences instrumentales et informatives améliorera également d'autres compétences en matière de sécurité;
- il existe encore des inégalités en matière de compétences numériques. Des efforts doivent donc être déployés pour les surmonter;
- le manque de compétences chez les plus jeunes enfants est une priorité pour les enseignants et les parents, car les enfants commencent à utiliser l'internet de plus en plus jeunes;
- l'utilisation de l'internet étant devenue courante pour de nombreux enfants en Europe, les priorités politiques ont évolué. Pour les enfants qui n'ont pas encore d'accès à l'internet, il est crucial de consentir des efforts en la matière;
- l'exclusion numérique ne va pas de pair avec l'exclusion sociale. Pour les enfants bénéficiant d'un accès à l'internet, des efforts sont nécessaires afin de garantir une qualité et une étendue d'utilisation suffisantes;

[11] http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/Final%20report.pdf *(consulté le 25 septembre 2011)*

- les efforts déployés pour encourager la citoyenneté numérique des enfants – sur le plan de la sécurité en ligne et des bonnes pratiques – portent leurs fruits et devraient être étendus;

- les parents ne sont pas les seuls responsables des enfants. Les enseignants ont aussi un rôle important à jouer et, pour de nombreux enfants, les camarades représentent également une ressource précieuse: 63 % des Européens de 9 à 16 ans ont reçu des conseils en matière de sécurité sur l'internet de la part de leurs parents, 58 % de la part des enseignants et 44 % de leurs camarades.

Rapport de la CE «Protéger les enfants dans le monde numérique» [12]

Ce document est un rapport de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions sur l'application de la recommandation du Conseil du 24 septembre 1998 concernant la protection des mineurs et de la dignité humaine, et de la recommandation du Parlement européen et du Conseil du 20 décembre 2006 sur la protection des mineurs et de la dignité humaine et sur le droit de réponse en liaison avec la compétitivité de l'industrie européenne des services audiovisuels et d'information en ligne. Il contient la référence suivante à l'enseignement:

- les initiatives d'éducation aux médias et de sensibilisation sont partiellement intégrées à l'enseignement officiel et des efforts sont également déployés pour sensibiliser les parents et les enseignants. Toutefois, il est ressorti d'une évaluation réalisée par la Commission en 2009 que, même si le sujet est inscrit dans les programmes éducatifs nationaux dans 23 pays européens, dans la pratique cet enseignement est dispensé de façon fragmentaire et sans cohérence.

Recherche de l'UIT [13]***, Cibler les jeunes pourrait être la voie du changement***

Il ressort d'une publication par l'UIT des dernières données sur les prix et la pénétration des TIC dans le monde que les technologies de l'information et de la communication (TIC) continuent de gagner du terrain partout dans le monde, bénéficiant de la baisse continue des prix de la téléphonie et des services internet à large bande. Parmi les commentaires à propos des jeunes, on peut citer les références suivantes:

- le rapport «Mesurer la société de l'information 2011» fait apparaître que les principaux obstacles à l'utilisation de l'internet ne sont pas nécessairement liés à l'infrastructure ou aux prix. Les comportements d'utilisation montrent qu'il y a aussi de grandes différences selon le niveau d'éducation, le sexe, le revenu, l'âge et la localisation géographique des

---

[12] http://ec.europa.eu/avpolicy/reg/minors/rec/2011_report/index_fr.htm *(consulté en septembre 2011)*

[13] http://www.itu.int/net/pressoffice/press_releases/2011/31-fr.aspx *(consulté le 16 septembre 2011)*

utilisateurs (zone urbaine/rurale). Par exemple, il y a très peu de différences en termes d'utilisation de l'internet entre habitants des pays en développement et habitants des pays développés ayant un très bon niveau d'éducation et un revenu élevé. Les personnes diplômées de l'enseignement supérieur utilisent l'internet plus que celles qui ont un niveau d'études inférieur; et en moyenne davantage d'hommes que de femmes utilisent l'internet;

- les jeunes gens (moins de 25 ans) sont davantage connectés à l'internet que les personnes plus âgées, et les étudiants utilisent l'internet plus que ceux qui ont terminé leurs études. Si l'on suppose que les personnes habituées à se connecter continueront d'utiliser l'internet, on peut penser que les personnes actuellement inscrites à l'école ou à l'université seront vraisemblablement de futurs internautes. Pour la jeune génération du monde entier, les réseaux sociaux et les contenus créés par l'utilisateur sont devenus des moteurs essentiels du développement de l'internet;

- étant donné que 46 % de la population des pays en développement a moins de 25 ans (soit plus de 2,5 milliards d'individus), le rapport suggère que ces pays pourraient faire augmenter de façon significative l'utilisation de l'internet en ciblant les jeunes générations, par exemple en privilégiant la connectivité des écoles et d'autres établissements d'enseignement et en améliorant les taux de scolarisation.

La grande révolution des écoles, The Economist[14]

Dans un rapport portant sur le thème de la réforme de l'éduction, *The Economist* fait référence à des questions concernant l'avenir de l'enseignement, lesquelles donnent des indications à propos du rôle des nouvelles technologies et des compétences des enfants:

- la technologie a également fait une différence. Après une série de faux départs, de nombreuses personnes pensent à présent que l'internet peut faire une réelle différence pour l'éducation des enfants. La nécessité croissante pour les travailleurs de mettre à jour et d'adapter en permanence leurs compétences est un des thèmes développés dans un nouveau ouvrage écrit par Lynda Gratton de la London Business School, intitulé «The Shift: The Future of Work is Already Here». Elle avance qu'avec l'accélération du rythme auquel les changements se succèdent, les personnes devront peut-être acquérir de nouvelles compétences à des intervalles de quelques années si elles veulent faire partie du marché lucratif des talents rares. Elle appelle ce processus «maîtrise séquentielle» et fait

[14] *http://www.economist.com/node/21529014?fsrc=nlw|edh|09-15-11|editors_highlights (consulté le 17 septembre 2011)*

remarquer que le système éducatif actuel de la plupart des pays, de la maternelle à l'université, ne prépare guère les personnes à l'éducation continue. Le domaine de la formation continue connaîtra probablement une vague d'innovations, en particulier sur l'internet, qui répondront à ce besoin de manière plus flexible et personnalisée que les études traditionnelles de deuxième et troisième cycle;

- tandis que l'on constate une convergence au sein des États membres à propos de l'utilité de promouvoir des mesures d'autoréglementation (codes déontologiques), il existe une inquiétude persistante sur le fait que des écarts importants subsistent entre les niveaux de protection atteints dans ce domaine. Aussi, les mesures existantes de lutte contre les contenus illégaux ou nuisibles devraient être sous surveillance constante afin de garantir leur efficacité. Par exemple, des points d'observation pour ce type de contenu mis à la disposition du fournisseur et que les enfants et les parents peuvent utiliser sont élaborés et soutenus par des infrastructures administratives viables, mais toutes ces initiatives manquent de caractères communs et d'économies d'échelle qui amélioreraient leur efficacité.

4 Résumé du matériel de l'ENISA

Dans ce chapitre, nous présentons des fiches qui couvrent les domaines de SRI qui ont été circonscrits et qui présentent un intérêt pédagogique. Veuillez noter que les discussions reproduites ci-après sont le plus souvent directement extraites des rapports de l'ENISA concernés. Nous vous recommandons de consulter les rapports de l'ENISA pour obtenir tous les détails.

4.1 Intimidation et manipulation psychologique en ligne: contribuer à protéger contre les risques

Les enfants sont les éléments les plus précieux de toute société, indépendamment de la culture, de la religion et de l'origine nationale. Ils dépendent de l'attention que leur prodiguent leurs parents, l'école et leur environnement social. Du fait de leur devoir de protection, les parents s'inquiètent des risques que peuvent présenter les activités de leurs enfants, qu'il s'agisse de sports extrêmes ou de l'utilisation des technologies. Ce dernier sujet est une source d'inquiétude particulière pour les parents, étant donné qu'ils se sentent souvent moins à l'aise avec les technologies que leurs enfants, lesquels:

- s'amusent en utilisant les technologies/gadgets;
- utilisent intuitivement les technologies;
- maîtrisent très facilement l'usage des caractéristiques techniques;
- se familiarisent aisément avec les innovations;
- utilisent les TIC comme un outil d'apprentissage;
- utilisent les technologies pour communiquer avec leurs amis.

Qu'est-ce que l'intimidation et la manipulation psychologique?

Une définition envisage l'intimidation sur le plan de l'incidence négative qu'elle a sur la victime, et la considère comme un traitement négatif et nuisible d'autrui, si bien que la personne qui en est la cible souffre et se sent humiliée ou vulnérable, ce qui a un effet néfaste et stressant sur elle. À l'instar du harcèlement, l'intimidation se définit dans une large mesure au travers de l'incidence sur le comportement de la victime, et non sur son intention. L'intimidation peut donc être surtout perçue en termes d'agression, ou de violence prolongée, qu'elle soit physique ou psychologique, exercée par un individu ou un groupe et dirigée contre une personne qui n'est pas capable de se défendre dans cette situation.

L'objectif de la manipulation psychologique est de faire une victime. Elle est faite pour choisir une victime, voir si la personne céderait à la contrainte d'un abus sexuel, en raison d'un déséquilibre des forces et sous l'effet de la coercition. La manipulation psychologique consiste

à rendre une victime potentielle suffisamment à l'aise pour être proche d'un agresseur, pour être seule avec un agresseur, et après l'ABUS, pour garder le secret.

Recommandations

L'ENISA a publié des recommandations pour limiter les risques auxquels les jeunes sont exposés dans le cyberespace. Elles sont classées dans différentes catégories en fonction du groupe auquel elles s'adressent:

Que doivent faire les parents / tuteurs / éducateurs?

- AMÉLIORER LEUR NIVEAU DE CONNAISSANCE COMPORTEMENTALE: améliorer les compétences des parents et des éducateurs concernant la connaissance des modèles comportementaux en ligne des mineurs. Maintenir une communication constante avec les parents/éducateurs. Discuter des irrégularités et consulter des experts dans ce domaine (psychologues comportementalistes) et participer à des activités de partage des connaissances dans ce domaine.

- AMÉLIORER LEUR NIVEAU DE CONNAISSANCES TECHNOLOGIQUES: entreprendre un transfert de connaissances vers les parents/éducateurs en ce qui concerne les questions techniques. Selon le rôle dans l'obligation de soin/d'éducation, différents niveaux de connaissances seraient nécessaires.

- AMÉLIORER LA POSITION ADOPTÉE PAR RAPPORT À LA CONFIDENTIALITÉ: les adolescents, les parents et les éducateurs devraient être tenus informés des questions de sécurité au sein du cybermonde.

- ENCOURAGER LES ÉCHANGES DE CONNAISSANCES: les connaissances technologiques devraient faire l'objet d'un échange régulier entre les parents et les mineurs. En maintenant un contact ouvert avec les adolescents sur les questions technologiques, il est plus facile d'évaluer leurs connaissances, leur niveau d'intérêt, leur niveau d'utilisation et leurs modes d'utilisation.

- UTILISER DES PARAMÈTRES DE SÉCURITÉ SPÉCIFIQUES AUX PARENTS/ÉDUCATEURS: envisager d'utiliser des paramètres de sécurité spécialement adaptés à une utilisation par les parents/éducateurs.

- APPORTER UN SOUTIEN AUX ADOLESCENTS À L'ÉCOLE: il importe d'identifier très rapidement les attaques potentielles de cyber-intimidation et de manipulation psychologique. Pour cette raison, les adolescents devraient avoir un accès immédiat à des postes de conseil spécialisé situés dans les écoles, vers lesquels ils peuvent se tourner en cas de besoin.

Que doivent faire les adolescents?

- UTILISER LES PARAMÈTRES DE SÉCURITÉ SPÉCIFIQUES AUX ADOLESCENTS: envisager le déploiement de paramètres de sécurité dans les dispositifs utilisés par les adolescents afin de compliquer l'accès aux informations.

- ADAPTER AU PUBLIC ADOLESCENT LES DISPOSITIFS DE SÉCURITÉ SPÉCIALISÉS EXISTANTS: actuellement, dans de nombreux domaines de la vie quotidienne, il existe des dispositifs de sécurité/sûreté qui sont adaptés aux enfants (par exemple dans les voitures, les avions, les bateaux, les jouets, etc.). Une approche similaire devrait être introduite dans le cyberespace. Nous recommandons donc d'envisager le déploiement de dispositifs de sécurité spécialement adaptés à une utilisation par les adolescents/mineurs.

- DÉVELOPPER DES SYSTÈMES DE CLASSIFICATION EN LIGNE: dans le milieu de la télévision et du cinéma, il existe des guides à l'attention des parents permettant de classer les programmes en fonction de critères précis (caractère sexuel explicite, images violentes et langage grossier). Dans le domaine des jeux pour ordinateur et des jeux vidéo, il existe des lignes directrices similaires d'évaluation/de classification de ces jeux. De même, l'établissement de lignes directrices pour les parents concernant le contenu en ligne (services, sites web, applications de réseaux sociaux, etc.) pourrait être envisagé.

- RÉALISER DES ÉVALUATIONS DES FACTEURS RELATIFS À LA VIE PRIVÉE: de nombreuses applications et de nombreux services web traitent des quantités importantes de données personnelles (par exemple les sites de réseaux sociaux). Il est recommandé d'établir des critères visant à identifier les domaines où une évaluation des facteurs relatifs à la vie privée doit être réalisée avant le déploiement du service.

- DÉSACTIVATION DE TOUTES LES COMPOSANTES ACTIVES: il peut arriver que des applications soient installées sur différents appareils portatifs, ordinateurs portables, etc., lesquelles possèdent des composantes actives, c'est-à-dire qu'elles communiquent/traitent des données (par exemple données de localisation, données sur les déplacements, etc.) en arrière-plan. Nous recommandons aux utilisateurs de s'équiper de fonctions leur permettant de désactiver toutes les fonctions d'arrière-plan qui communiquent des données personnelles à certains fournisseurs de services/d'applications.

- AMÉLIORER LE CONTRÔLE D'ACCÈS EN FONCTION DE L'ÂGE: nous recommandons que l'âge des utilisateurs fasse désormais partie intégrante de leurs références dans toute l'infrastructure et, en particulier, dans les mécanismes d'authentification/d'autorisation utilisés.

Afin d'évaluer les risques, nous avons utilisé le scénario «Kristie online» dont vous trouverez tous les détails dans le rapport de l'ENISA.

Pour plus de détails, consulter le site:

https://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/Cyber-Bullying%20and%20Online%20Grooming/

4.2 Les enfants et les mondes virtuels: Guide à l'attention des parents

Chaque jour, de nouveaux sites de réseautage social en ligne semblent apparaître. Les internautes ont l'embarras du choix: de Facebook et Bebo à LinkedIn, orienté carrières, en passant par MySpace et Second Life. Mais il existe un nouveau phénomène, qui prend de l'ampleur sur la toile et qui s'adresse à la jeune génération. L'un des plus grands soucis suscités par les mondes virtuels concerne la sécurité des enfants (jusqu'à 7 ans) et des préadolescents (de 8 à 12 ans) ainsi que la manière de les protéger des cyberprédateurs. Les adultes doivent accompagner les enfants afin de garantir qu'ils aient des expériences positives dans ces environnements tridimensionnels.

Les parents sont naturellement préoccupés par la manière dont leurs enfants utilisent les mondes virtuels et dont ils y évoluent. Il leur est nécessaire de disposer des informations permettant de décider, avec leurs enfants, de ce qui est adéquat et sans danger, et de la façon d'agir de manière responsable au sein des mondes virtuels.

Qu'est-ce qu'un monde virtuel?

Un monde virtuel est un monde créé artificiellement par un programme informatique et hébergeant une communauté d'utilisateurs présents sous forme d'avatars et pouvant s'y déplacer et interagir. Ces avatars sont généralement des représentations graphiques textuelles, en deux ou trois dimensions, mais ils peuvent aussi exister sous d'autres formes (sensations auditives et tactiles, par exemple). Certains mondes virtuels, mais pas tous, sont multi-utilisateurs.

L'ordinateur accède à un monde simulé et soumet les utilisateurs à des stimuli visuels qui les amènent à manipuler des éléments du monde modélisé et donc à vivre des expériences de téléprésence jusqu'à un certain degré. Ces mondes modélisés peuvent ressembler au monde réel ou au contraire représenter des mondes imaginaires. Le monde modélisé peut simuler le monde réel, avec ses lois physiques telles que la gravité, la topographie, la locomotion, les actions et les représentations en temps réel ou un monde imaginaire hybride.

Que cherchent les enfants en accédant à des mondes virtuels?

Les jeunes se connectent à des sites de monde virtuel pour un grand nombre de raisons différentes, notamment pour:

- interagir avec des amis dans un nouvel environnement et en temps réel et partager des intérêts communs;
- créer et rejoindre des communautés ou des groupes d'intérêt, p. ex. la musique, le football, etc.;
- communiquer des idées et des informations sur des domaines d'intérêt dans des blogs, par messagerie instantanée et par le biais d'autres instruments;
- rencontrer de nouvelles personnes et se faire de nouveaux amis;

- créer et partager des informations originales et à caractère personnel, telles que des images, des photos et des vidéos, pour accroître les possibilités d'expression personnelle;
- créer, publier et partager de la musique;
- jouer;
- disposer de leur espace personnel même lorsque leurs parents et leurs éducateurs sont présents;
- expérimenter, avec leur identité virtuelle, de nouveaux espaces sociaux et de nouvelles limites.

Des histoires et une analyse menée par l'ENISA ont mis en lumière quatre grands types de préoccupation:

- intimidation;
- harcèlement;
- contenu illégal;
- maltraitance des enfants.

En outre, les risques sont accrus dans les cas suivants:

- environnements non sécurisés;
- absence de contenu éducatif;
- placement de produits dans les mondes virtuels;
- commercialisation ciblée sur les enfants;
- frais d'engagement:
    - redevances mensuelles,
    - achat de produits,
    - publicité.

Quel soutien les parents et les tuteurs peuvent-ils apporter aux enfants?

- Lire les conditions générales d'utilisation avec leurs enfants avant qu'ils n'accèdent au monde virtuel, discuter avec eux des précautions en matière de sécurité, fixer certaines règles de base et veiller à ce qu'ils les respectent.
- Enseigner aux jeunes utilisateurs un usage responsable de la technologie en général, les encourager à écouter leur instinct et à faire appel à leur bon sens.
- Veiller à utiliser des solutions techniques, par exemple:
    - filtres et contrôles parentaux;
    - historique d'utilisation;
    - confirmation de l'utilisation des méthodes automatiques de modération, telles que le filtrage de texte reconnaissant des séquences de mots et des URL spécifiques ou des filtres plus sophistiqués englobant des moteurs anti-manipulation psychologique (AGE);
    - signalétique: les parents et les éducateurs devraient connaître les pictogrammes et les considérer comme un outil fondamental de protection des jeunes utilisateurs contre les services et les contenus inadéquats;
    - vérification de l'âge.
- Vérifier que le monde virtuel fait l'objet d'une modération intrajeu active et/ou discrète.
- Rester associé aux activités des jeunes utilisateurs dans le monde virtuel.
- Rester calmes et ne pas tirer de conclusions hâtives, si vous entendez ou voyez quoi que ce soit qui vous inquiète à propos du comportement de votre enfant ou de l'un de ses amis virtuels. Si vos enfants craignent que vous ne leur coupiez purement et simplement leurs liens, ils risquent de se montrer de plus en plus réticents à partager leurs problèmes ou préoccupations potentiels.
- Être ouverts aux rapports des équipes de la communauté virtuelle qui indiqueraient une divergence entre le comportement de votre enfant en ligne et celui qu'il adopte avec vous en direct.
- Apprendre la cyberculture pour ne pas se faire piéger par les excuses typiques invoquées par les jeunes lorsqu'ils doivent rendre des comptes sur leur comportement en ligne, telles que «quelqu'un a usurpé mon compte».
- Apprendre à votre enfant à ne pas partager les mots de passe virtuels avec des amis ou des frères et sœurs.

- Contacter le responsable de la communauté via la page de contact du site web du monde virtuel et lui faire part de vos préoccupations et de vos questions.

- Ne pas partir du principe que votre enfant est une cible pour tous sur l'internet. Les statistiques montrent que les problèmes avec des pédophiles sont beaucoup plus fréquents dans le monde réel qu'en ligne. En général, les sites destinés aux enfants sont sûrs et peuvent faire vivre à votre enfant une merveilleuse expérience créative et éducative, mais seulement si vous restez engagé à ses côtés et attentif.

Pour étayer les informations susmentionnées, l'ENISA a publié une affiche reprenant 10 conseils et astuces à l'attention des parents et des tuteurs (n'hésitez pas à utiliser le lien suivant: affiche).

Pour plus de détails, consulter le site:

http://www.enisa.europa.eu/act/ar/deliverables/2008/children-on-virtual-worlds

4.3 Modèles de quiz de sensibilisation

Contenu du quiz

L'objectif des quiz est de donner aux répondants une indication quant à leur niveau de sensibilisation et, dans le meilleur des cas, de fournir un outil susceptible de stimuler un intérêt accru pour les valeurs et les risques associés à l'utilisation des ordinateurs et des services en ligne sur l'internet. Ces quiz ne doivent donc pas être considérés comme des auto-évaluations exhaustives du niveau de sensibilisation et de connaissances actuel des individus. Ils visent plutôt à indiquer la bonne direction et à épingler les thèmes intéressants à développer pour améliorer la sensibilisation aux questions de sécurité. Les groupes cibles de ce travail de l'ENISA sont les parents, les utilisateurs finaux et les petites et moyennes entreprises (PME).

Ce matériel est disponible dans plusieurs langues (EN, ES, DE, FR, IT, DA, PL), ce qui le rend attrayant à un large éventail d'utilisateurs potentiels.

Étant donné la longueur des quiz, nous ne présentons ci-dessous qu'un aperçu de celui destiné aux parents, et nous invitons les personnes intéressées à se reporter au rapport de l'ENISA et à déterminer les parties intéressantes (pages 13 à 21 du rapport). Nous jugeons que les parties intéressantes peuvent être réutilisées directement étant donné qu'elles sont génériques et exhaustives.

Vue d'ensemble du quiz destiné aux parents

Dans le contexte de la SRI dans l'éducation, le quiz destiné aux parents revêt un intérêt particulier. Le but de ce quiz est de fournir aux parents un moyen de tester leur sensibilisation à, et leurs connaissances concernant un certain nombre d'aspects liés à l'utilisation par leurs enfants de l'ordinateur et des services en ligne sur l'internet. Il peut servir d'outil pour

stimuler l'intérêt envers les valeurs et les risques associés à l'utilisation des ordinateurs et des services en ligne sur l'internet par les enfants.

Le quiz s'adressant aux parents couvre les domaines suivants: activités en ligne des enfants, vie privée et réseaux sociaux, contenu illégal, partage de fichiers et cyber-Intimidation.

Pour obtenir plus de détails et le quiz destiné aux utilisateurs finaux, consulter le site:

http://www.enisa.europa.eu/act/ar/deliverables/2008/ar-quizzes-templates-fr

4.4 «Lignes directrices pour les parents, les tuteurs et les éducateurs», rapport de l'UIT en coopération avec l'ENISA

Comprendre le type d'expérience en ligne que recherche votre enfant

L'internet a un grand potentiel en tant que moyen permettant aux enfants et aux jeunes de trouver des informations par eux-mêmes. Leur apprendre les formes de comportement en ligne positives et responsables est un objectif essentiel. Pour cela, il importe de comprendre le type d'expérience en ligne que votre enfant recherche (voir les pages 12 et 13 du rapport). Cette information est déterminante pour comprendre les types de risque auxquels vos enfants s'exposent et, par conséquent, le type de protection qu'il sera nécessaire de mettre en place.

Ce que de nombreux parents, tuteurs et éducateurs ignorent

Une analyse récente réalisée par l'ENISA a mis en évidence que, dans la plupart des cas, les parents et tuteurs ne sont pas informés des faits précis concernant les expériences en ligne auxquelles leurs enfants sont susceptibles de faire face et les vulnérabilités liées aux différentes activités en ligne. Les enfants peuvent être en ligne à l'aide de différentes plates-formes et équipements, parmi lesquels:

- les ordinateurs personnels;
- les téléphones mobiles;
- les assistants numériques personnels (PDA).

Rôle que peuvent jouer les éducateurs

Il est capital que les éducateurs n'échfaudent pas d'hypothèses sur ce que les enfants et les jeunes savent ou ne savent pas concernant les problèmes de sécurité en ligne. Il y a de nombreux malentendus concernant internet et ce qui est approprié ou non. Par exemple, de nombreux adolescents partagent leurs mots de passe et cela est souvent considéré comme un signe de réelle amitié. L'un des rôles importants des éducateurs est d'apprendre aux enfants et aux jeunes l'importance des mots de passe, comment les garder en sécurité et comment créer un mot de passe efficace. De même, concernant les problèmes de droits d'auteur, de nombreux adultes sont horrifiés de voir l'apparent manque d'intérêt des jeunes utilisateurs concernant le téléchargement illégal de vidéos ou de musique. Les enfants et les jeunes manquent cruellement de connaissances concernant les problèmes de légalité des contenus soumis à des droits d'auteur en ligne. Encore une fois, les éducateurs ont un rôle clair à jouer en expliquant cela à leurs élèves. Les écoles ont l'occasion de transformer l'éducation et d'aider les élèves pour à la fois atteindre leur potentiel et élever les normes des TIC. Toutefois, il importe aussi que les enfants apprennent comment être en sécurité lorsqu'ils utilisent ces nouvelles technologies, en particulier les technologies collaboratives du web 2.0, par exemple les sites de réseautage social, qui deviennent un aspect essentiel de l'apprentissage social

productif et créatif. Les éducateurs peuvent aider les enfants à utiliser la technologie de manière sage et sûre en:

- s'assurant que l'école dispose d'un ensemble de politiques et de pratiques résilientes et que leur efficacité est contrôlée et évaluée de manière régulière;
- s'assurant que tout le monde est au courant de la politique d'utilisation acceptable (PUA) et de son usage. Il importe d'avoir une PUA qui, en outre, soit adaptée à l'âge;
- vérifiant que la politique anti-harcèlement et brimade de l'école inclut des références au harcèlement sur l'internet via téléphone ou tout autre équipement mobile, et qu'il existe des sanctions effectives pour ceux qui enfreignent cette politique;
- désignant un coordonnateur de la sécurité en ligne;
- s'assurant que le réseau de l'école est sécurisé;
- s'assurant qu'un fournisseur d'accès à l'internet accrédité est utilisé;
- utilisant un dispostitif de filtrage/contrôle;
- fournissant une éducation en matière de sécurité en ligne à tous les enfants et en indiquant où, comment et quand elle sera proposée;
- s'assurant que tout le personnel (y compris le personnel de soutien) a déjà été correctement formé et que leur formation est mise à jour de manière régulière;
- ayant un unique point de contact dans l'école. Et en étant capable de rassembler et d'enregistrer les incidents concernant la sécurité en ligne, ce qui donnera à l'école une meilleure vision des problèmes ou tendances qu'il faut gérer;
- s'assurant que l'équipe de direction et les responsables de l'école ont une compréhension adéquate du problème de la sécurité en ligne;
- en faisant réaliser un audit à intervalle régulier de toutes les mesures concernant la sécurité en ligne.

Quels sont les éléments propices à un environnement d'apprentissage des TIC sûr?

Créer un environnement d'apprentissage sécurisé des TIC repose sur plusieurs éléments importants, parmi lesquels:

- les responsabilités, politiques et procédures;

- un éventail efficace d'outils technologiques;
- une éducation globale sur la sécurité en ligne;
- un programme pour chacun dans l'établissement;
- un processus d'examen qui contrôle en permanence l'efficacité de ce qui précède.

Il est donc crucial que les parents et les éducateurs soient capables de décider avec les enfants de ce qui est approprié et sûr pour eux, ainsi que le comportement responsable à adopter face aux TIC. En travaillant ensemble, les parents, les éducateurs et les enfants peuvent récolter les bénéfices des TIC, en même temps qu'ils réduisent les dangers possibles pour les enfants.

Pour plus de détails, consulter le site:

http://www.enisa.europa.eu/act/ar/deliverables/2009/cop_initiative?searchterm=guidelines+for+parents+%2C+guardians

4.5 Questions et recommandations en matière de sécurité pour les réseaux sociaux en ligne

Quels sont les points faibles des réseaux sociaux?

Les réseaux sociaux en ligne ou sites de réseaux sociaux (SRS) sont un des phénomènes technologiques les plus remarquables du XXIe siècle, plusieurs d'entre eux faisant aujourd'hui partie des sites internet les plus visités au monde.

L'incidence du cyber-harcèlement et de la cyber-intimidation sur la personne qui en est victime est bien connue et peut varier de l'intimidation légère et de la violation de la vie privée à l'atteinte grave à l'intégrité physique et au préjudice psychologique. Divers facteurs rendent les SRS particulièrement vulnérables à ce type d'exploitation:

- de nombreuses écoles interdisent l'utilisation des SRS à l'école, ce qui est un facteur dissuasif notable pour le signalement d'actes d'intimidation;
- la facilité à garder l'anonymat (en utilisant un faux profil);
- la facilité à communiquer avec des groupes restreints de personnes (une fonctionnalité qui peut être très intéressante si elle est utilisée à bon escient);
- l'effet «guichet unique». Le SRS fournit tous les outils et toutes les attaques utilisés par le cyber-intimidateur, qui plus est, en un seul espace d'interface (IM, messagerie mobile, faux profils, diffamation, etc.). Les enseignants et les adultes sont souvent incapables d'intervenir parce qu'ils ne maîtrisent pas bien la technologie utilisée.

Formes de cyber-intimidation susceptible de se produire sur les SRS

Divers types d'activités peuvent être considérés comme de la cyber-intimidation. Leur identification précoce permettrait de conceptualiser efficacement l'effet négatif produit sur les victimes:

- fusillade: combat en ligne utilisant des messages électroniques chargés de colère et de vulgarité;
- harcèlement: par exemple, envoyer continuellement des messages blessants ou cruels et insultants; accéder au nom d'utilisateur et au mot de passe d'une autre personne pour envoyer des messages inappropriés à ses contacts;
- dénigrement: créer des comptes pour usurper l'identité d'une personne afin de l'humilier; envoyer ou afficher des ragots ou des rumeurs à propos d'une personne dans le but de nuire à sa réputation ou à ses amis, par exemple, créer des sites internet à contenu haineux, afficher des plaisanteries, des dessins, des ragots et des rumeurs, dirigés contre

une victime particulière; afficher des déclarations ou des images nuisibles et/ou cruelles, et inviter d'autres à faire de même ou à partager leurs commentaires;

- usurpation d'identité: prétendre être quelqu'un d'autre et envoyer ou afficher du matériel pour lui créer des ennuis, pour le mettre en danger ou nuire à sa réputation ou ses amis;
- révélation: partager les secrets de quelqu'un ou publier des informations ou des images embarrassantes en ligne;
- tromperie: se faire confier des secrets ou des informations embarrassantes par quelqu'un, puis les partager en ligne;
- exclusion: exclure intentionnellement et avec cruauté quelqu'un d'un groupe en ligne, par exemple, un groupe d'amis dans le monde réel qui décident d'ignorer intentionnellement un des leurs en guise de punition;
- traque: typiquement liée à une relation intime problématique, harcèlement et dénigrement intenses et répétés qui comprennent des menaces ou inspirent une crainte réelle;
- comportement menaçant: direct ou indirect.

Décourager l'interdiction des SRS à l'école

Un nombre croissant d'écoles interdisent ou restreignent l'utilisation des SRS. Il est recommandé aux écoles et aux responsables politiques de l'éducation d'examiner soigneusement les conséquences d'une interdiction des SRS dans les écoles, puisque cela dissuade de rapporter des faits d'intimidation. Cela signifie aussi que les enseignants et les adultes sont moins susceptibles d'acquérir les compétences nécessaires pour encadrer et superviser les jeunes dans ce domaine. Enfin, cela signifie aussi la perte d'une précieuse ressource éducative.

Les SRS devraient être utilisés de manière ouverte et contrôlée (c'est-à-dire que leur utilisation ne doit être ni interdite, ni découragée), dans le cadre de campagnes coordonnées visant à sensibiliser les enfants, les enseignants et les parents.

Ce ne sont pas les technologies en tant que telles qui sont responsables des comportements d'intimidation, mais les individus, qui les détournent. Pour cette raison, l'éducation, la modélisation de l'utilisation positive de la technologie par les camarades, les enseignants et les adultes ainsi que des dispositifs d'autocontrôle dans la société sont autant de moyens de lutter efficacement contre la cyber-intimidation.

Pour plus de détails, consulter le site:

http://www.enisa.europa.eu/act/it/past-work-areas/social-networks/security-issues-and-recommendations-for-online-social-networks

4.6 À propos des cookies

Qu'est-ce qu'un cookie?

Les cookies sont de petites unités d'information stockées dans les ordinateurs et très souvent utilisées par les fournisseurs de services en ligne pour faire fonctionner leurs services, découvrir les préférences de l'utilisateur (langue, mise en page, références, etc.), procéder à une identification afin d'établir une liste de contrôle, etc. N'importe quel site internet peut éditer des cookies qui sont stockés sur l'ordinateur des utilisateurs. Toutes les activités relatives au stockage et à l'envoi de cookies sont invisibles pour l'utilisateur et gérées par le site internet visité.

Quels sont les avantages liés à l'utilisation de cookies?

D'un point de vue fonctionnel, les cookies peuvent être utilisés pour:

- identifier et authentifier un utilisateur (c'est-à-dire éviter de recommencer la procédure d'identification);
- établir des statistiques, par exemple sur les sites visités, le nombre de visites effectuées, etc.;
- stocker les préférences et les paramètres.

Du point de vue du marketing et de la publicité en ligne, ils pourraient être utilisés pour:

- quantifier/évaluer l'efficacité des publicités (c'est-à-dire permettre de déterminer combien de visiteurs individuels se sont rendus sur un site en réaction directe à une publicité);
- dresser le profil des utilisateurs et utiliser ce profil pour envoyer des publicités ciblées (c'est-à-dire ciblage comportemental);
- améliorer la gestion des publicités (adaptation au profil de l'utilisateur, rotation et non-redondance).

Quelles sont les principales préoccupations en matière de sécurité?

Les principales préoccupations en matière de sécurité concernent la protection des données à caractère personnel des utilisateurs et les attaques courantes commises sur la base des informations trouvées dans les cookies:

- collecte d'informations privées sur les préférences des utilisateurs, sites visités, statistiques;
- modification d'informations (par exemple les résultats de recherches);

- usurpation d'identité conduisant à l'accès aux comptes de l'utilisateur avec une intention malveillante (par exemple banque, courriels, etc.).

Pour plus de détails, consulter le site:

http://www.enisa.europa.eu/act/it/library/pp/cookies/?searchterm=cookies

4.7 Mondes virtuels – Argent réel

En quoi consiste la sécurité des mondes virtuels?

La fraude dans les sites de jeu (et le monde virtuel) est une violation des informations relatives à l'utilisateur en rapport avec les jeux en ligne. Ces manœuvres frauduleuses prennent pour cible l'argent réel et se basent sur l'utilisation croissante de programmes malveillants visant spécifiquement les sites de jeux en ligne et les mondes virtuels, et sur l'émergence de milliers de nouveaux programmes visant à voler les mots de passe donnant accès aux jeux en ligne.

Les attaques visent à dérober des objets et des biens virtuels et à les vendre sur un marché gris émergent existant.

Quels sont les cinq principaux risques auxquels les mondes virtuels sont exposés?

Les cinq principaux risques auxquels les mondes virtuels sont exposés sont les suivants:

Risques en matière de protection de la vie privée: les utilisateurs dévoileront même peut-être davantage de données à caractère personnel, parce que l'environnement virtuel procure un faux sentiment de sécurité. On assiste aussi à une tendance au marketing comportemental, qui passe par une «surveillance» des avatars;

Usurpation d'identité d'avatar et fraude à l'identité: vol des références du compte (nom d'utilisateur et mot de passe). La principale motivation est le bénéfice financier en argent réel, mais la fraude à l'identité peut également être utilisée pour nuire à la réputation de quelqu'un;

Attaques commerciales et financières – rejets de débit pour les paiements par carte de crédit: à chaque fois qu'un achat intrajeu est effectué à l'aide d'un service de paiement en ligne (par exemple par carte de crédit ou PayPal), il est possible de réclamer un remboursement total à la société de paiement (généralement dans un délai d'un mois). Si un rejet de débit est émis, il est techniquement et administrativement très compliqué d'inverser les transactions effectuées;

Risques au niveau de la propriété intellectuelle: des œuvres originales peuvent être créées dans les mondes virtuels en utilisant des outils officiels fournis par le fournisseur de service. Les droits réels détenus par l'utilisateur sont souvent définis de façon approximative et peuvent être invalidés par des droits sous-jacents. De même, les utilisateurs de mondes virtuels importent souvent du contenu protégé par le droit d'auteur sans la permission du titulaire;

Risques en matière de sécurité auxquels les mineurs sont exposés: les mineurs peuvent être exposés à des contenus inadéquats dans les jeux MMO/mondes virtuels, soit par le contournement des techniques de vérification de l'âge, soit par l'échec des systèmes de

classement des contenus. Cela les expose à des risques tels que le dévoilement de données de contact réelles.

Veuillez noter que le rapport de l'ENISA présente d'autres risques.

Quelles sont les recommandations les plus importantes?

Ces recommandations concernent tous les groupes de personnes évoluant dans les mondes virtuels. Des éléments importants contenus dans ces recommandations sont des indices permettant de détecter si leurs données sont en danger. La liste de contrôle suivante pourrait être utilisée à cette fin:

- vos références ne se trouvent pas à la même place que lorsque vous vous êtes déconnecté;
- certains de vos articles sont manquants;
- votre mot de passe est incorrect;
- de nouvelles personnes figurent dans votre liste d'amis;
- certaines de vos références sont manquantes ou d'autres sont apparues;
- le dernier nom d'utilisateur saisi dans la page de gestion de compte ne concorde pas avec le vôtre;

  vous avez reçu un courrier électronique des maîtres du jeu vous avertissant d'un événement survenu pendant que vous étiez déconnecté;

- vos acolytes de jeu disent vous avoir vu en ligne alors que vous n'étiez pas en train de jouer.

L'ensemble des recommandations se trouvent dans le rapport.

Pour plus de détails, consulter le site:

http://www.enisa.europa.eu/act/it/past-work-areas/massively-multiplayer-online-games-and-social-and-corporate-virtual-worlds/security-and-privacy-in-virtual-worlds-and-gaming

4.8 Impression sécurisée

Qu'est-ce que l'impression sécurisée?

L'impression sécurisée signifie toute démarche entreprise par l'organisation pour s'assurer que: les appareils d'impression restent sécurisés; les données imprimées ou transmises resteront confidentielles, intégrales et disponibles; l'organisation recevra une aide lui permettant de se conformer à certaines normes de sécurité.

Quelles sont les recommandations les plus importantes?

1. Définir un flux et une gestion des documents
2. Garantir la sécurité physique des appareils d'impression
3. Garantir la sécurité logique des appareils d'impression
4. Garantir la sécurité des données d'impression sur disque dur ou envoyées aux appareils d'impression
5. Vérifier la résistance de l'environnement d'impression
6. Suivre les documents imprimés, photocopiés et numérisés pour télécopie ou courrier électronique
7. Établir un flux de rapports sur les impressions
8. Définir une politique ou des procédures d'entreprise pour maîtriser l'utilisation des appareils d'impression
9. Organiser une formation de sensibilisation
10. Établir une stratégie d'impression sécurisée
11. Définir des indicateurs pour mesurer le succès et les avantages d'une stratégie d'impression sécurisée
12. Dresser un bilan en vue d'une évaluation
13. Documenter les enseignements tirés

Quels avantages l'impression sécurisée peut-elle apporter?

Un aperçu des nombreux avantages associés à un environnement d'impression sécurisé permettra d'amener les entreprises à prendre de meilleures décisions. Les avantages suivants ont été identifiés:

- sécurité améliorée;
- flexibilité accrue associée à des solutions;
- diminution des coûts d'impression (par exemple argent dépensé/appareil; taux utilisateur/appareil et utilisateur/fournitures d'impression);

- diminution des cas de fraudes;
- mobilité et flexibilité des utilisateurs accrues, en passant de ce qui était un poste de coûts à un facilitateur d'affaires;
- parvenir à la conformité (par exemple audits de sécurité contre des normes telles qu'ISO 27002 ou PCI DSS;
- renforcement des contrôles centraux du réseau;
- traçabilité complète des impressions;
- flexibilité pour la révocation ou l'autorisation de droits aux utilisateurs;
- diminution du nombre d'incidents rapportés et liés à des problèmes d'impression informatique;
- conformité générale de l'environnement d'impression avec les meilleures pratiques en matière de sécurité concernant la confidentialité, l'intégrité et la disponibilité.

Conclusions

Les appareils d'impression traitent souvent des informations confidentielles telles que des factures, des formulaires, des documents relatifs aux travailleurs et des données client. Ces appareils et les documents qu'ils produisent restent en majeure partie non protégés, laissant ainsi les documents commerciaux et sur les transactions imprimés sujets à des lacunes de sécurité. C'est pourquoi il est primordial que les gestionnaires des actifs informatiques se préparent, eux-mêmes, ainsi que leur organisation, à gérer l'impression de façon proactive, puisqu'assurer un environnement d'impression sécurisé constitue un facteur clé pour toute organisation, quelle que soit sa taille. La sécurité des environnements d'impression et de capture d'image fait partie intégrante de la stratégie de sécurité générale de l'organisation.

Pour plus de détails, consulter le site:

http://www.enisa.europa.eu/act/ar/deliverables/2008/secure-printing

5 Conclusions / Recommandations

Étant donné que l'éducation nous concerne tous, que nous soyons étudiant ou élève, parent ou éducateur, l'ENISA invite le lecteur à garder en tête toutes les informations de sécurité relayées par tous les canaux de communication, de les utiliser le plus possible et de les diffuser avec pertinence.

Nous vous proposons de suivre les publications de l'ENISA, car des questions de sécurité en rapport avec l'éducation sont susceptibles d'émerger l'année prochaine. L'ENISA essaiera d'actualiser le présent document en conséquence en insérant des fiches relatives au nouveau matériel afférent.

6 Annexe I: Références

- ENISA. Work Programme 2011 for ENISA, the European Network and Information Security Agency(ENISA website) http://www.enisa.europa.eu/about-enisa/activities/programmes-reports/work-programme-2011/view (accessed 25 October 2011)
- ENISA and UIT. Guidelines for Parents, Guardians and Educators on Child Online Protection, European Network and Information Security Agency (ENISA website)

  http://www.enisa.europa.eu/act/ar/deliverables/2009/cop_initiative?searchterm=guidelines+for+parents+%2C+guardians (accessed September 2011)
- EUKids Online. Final Report EUKids Online including all findings and recommendations http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/Final%20report.pdf, (accessed 25 September 2011)
- European Commission. 2011 Implementation Report on the Protection of Minors and Human Dignity Recommendations, PROTECTING CHILDREN IN THE DIGITAL WORLD,

  http://ec.europa.eu/avpolicy/reg/minors/rec/2011_report/index_en.htm(accessed September 2011)
- UIT. Measuring the Information Society 2011

  http://www.itu.int/net/pressoffice/press_releases/2011/31.aspx (accessed 16.09.2011)
- The Economist. The great schools revolution, Ed.,17th September 2011,

  http://www.economist.com/node/21529014?fsrc=nlw|edh|09-15-11|editors_highlights (accessed on 17 September 2011)
- Hogben, Giles, Recommendations for Online Social Networks, European Network and Information Security Agency (ENISA website)

  http://www.enisa.europa.eu/act/it/past-work-areas/social-networks/security-issues-and-recommendations-for-online-social-networks (accessed August 2011)
- Hogben, Giles, Recommendations for Online Social Networks, European Network and Information Security Agency (ENISA website)

  http://www.enisa.europa.eu/act/it/past-work-areas/social-networks/security-issues-and-recommendations-for-online-social-networks (accessed August 2011)
- Hogben, Giles, Editor, Online Games and Virtual Worlds, European Network and Information Security Agency (ENISA website)

http://www.enisa.europa.eu/act/it/past-work-areas/massively-multiplayer-online-games-and-social-and-corporate-virtual-worlds/security-and-privacy-in-virtual-worlds-and-gaming (accessed October 2011)

- Kalmelid, Kjell, Awareness raising quizzes templates: Targeting parents, end-users and SMEs, European Network and Information Security Agency (ENISA website)

  http://www.enisa.europa.eu/act/ar/deliverables/2008/ar-quizzes-templates-en, (accessed September 2011)

- Marinos, Louis, Cyber-bullying and online grooming: helping to protect against the risks, European Network and Information Security Agency (ENISA website)

  https://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/Cyber-Bullying%20and%20Online%20Grooming/ (accessed October 2011)

- Santa, Isabella, Children on virtual worlds - What parents should know, European Network and Information Security Agency (ENISA website)

  http://www.enisa.europa.eu/act/ar/deliverables/2008/children-on-virtual-worlds (accessed September 2011)

- Santa, Isabella, Secure printing, European Network and Information Security Agency (ENISA website)

  http://www.enisa.europa.eu/act/ar/deliverables/2008/secure-printing (accessed October 2011)

- Tirtea, Rodica – ENISA; Castelluccia, Claude – INRIA; Ikonomou, Demosthenes – ENISA, Bittersweet cookies. Some security and privacy considerations, European Network and Information Security Agency (ENISA website)

  http://www.enisa.europa.eu/act/it/library/pp/cookies/?searchterm=cookies, (accessed October 2011)

7 Annexe II: Abréviations

ENISA	Agence européenne chargée de la sécurité des réseaux et de l'information
UE	Union européenne
UIT	Union internationale des télécommunications
PT	Programme de travail
EM	État membre
SRI	Sécurité des réseaux et de l'information
SRS	Sites de réseaux sociaux

8 Annexe III: Travaux connexes

Affiliation Name		Link
COE	Manuel de maîtrise de l'internet	http://book.coe.int/FR/ficheouvrage.php?PAGEID=36&lang=FR&produit_aliasid=2023
Eurydice	Chiffres clés de l'utilisation des TIC pour l'apprentissage et l'innovation à l'école en Europe	http://eacea.ec.europa.eu/education/eurydice/documents/key_data_series/129FR.pdf

9 Annexe IV: Diapositives de présentation

Diapositives sur l'intimidation et la manipulation psychologique en ligne:


1 Cyber bullying.pptx

Diapositives sur les enfants et les mondes virtuels:


2 Children on virtual worlds - What parent

Diapositives sur les quiz de sensibilisation:


3 Awareness Raising Quiz Templates.pptx

Diapositives sur les lignes directrices pour les parents, les tuteurs et les éducateurs:


4 Guidelines for Parents, Guardians ai

Diapositives sur les questions en matière de sécurité sur les réseaux sociaux en ligne:


5 Security Issues and Recommendation


6 Cookies.pptx

Diapositives sur les cookies:

Diapositives sur les questions de sécurité dans les mondes virtuels:


7 Virtual worlds-real money.pptx

Diapositives sur l'impression sécurisée:


8 Secure printing.pptx

P.O. Box 1309, 71001 Héraklion, Grèce
www.enisa.europa.eu