

Luxemburg sicher im Netz 2008-2009

Retour d'expérience d'une année de présentations dans des lycées et écoles primaires (environ 200 présentations dispensées à approximativement 7000 enfants et adolescents)

Introduction

Depuis maintenant 4 ans, CASES, structure du Ministère de l'Économie et du Commerce extérieur dédiée à la sécurité de l'information, réalise des campagnes de sensibilisation dans les écoles primaires et lycées du Luxembourg, sous forme de présentations. Ces dernières ont pour objectif d'informer les enfants et adolescents sur les risques liés à l'utilisation d'Internet. En 2008-2009, CASES et LuSI (site luxembourgeois du projet européen Insafe) ont intensifié les formations dans les écoles avec l'apparition de plusieurs sujets supplémentaires abordés lors des présentations :

- les e-mails de menace (ex : "si tu n'envoies pas ce message à 10 amis quelqu'un de ta famille aura un terrible accident avant le 30 avril – une photo ajoutée en pièce jointe montre le visage d'une personne gravement blessée) ;
- les cas de sexting (les enfants s'échangent des photos ou des vidéos de leurs parties intimes) ;
- les cas avérés d'addiction à l'ordinateur ;
- les mobiles avec connexion Internet directe ont fait leur entrée dans les classes dès la 3e primaire ;

Au cours de ces sessions généralement très interactives et d'une durée approximative de deux heures, les formateurs ont recueilli quantité d'impressions et ont documenté certains faits rapportés soit par les élèves, soit par les instituteurs ou les professeurs des lycées.

Après un aperçu des définitions de la sécurité et du risque, le formateur explique les objectifs de sécurité (confidentialité, intégrité, disponibilité). Il dresse alors un panorama des menaces telles que les virus, les vers, les bots, les spams et le phishing. Le formateur met ensuite l'accent sur des menaces plus ciblées, notamment les chevaux de Troie, les dangers liés au chat, à la création de « pages », l'utilisation des réseaux sociaux ou encore le blogging. Il est également expliqué aux enfants pourquoi ils ne doivent pas s'engager dans la voie du piratage informatique ou du harcèlement électronique (cyberbullying).

Pour finir, les contre-mesures appropriées sont présentées et expliquées. Citons notamment les contre-mesures humaines comme la vigilance, la méfiance et le savoir-faire, ainsi que les contre-mesures techniques comme la restriction de fonctionnalités non utilisées et la mise à jour du système d'exploitation, l'antivirus et le firewall.

A la lumière des informations issues des faits rapportés et des réactions provoquées lors de ces présentations, ce rapport dresse un état des lieux de la situation actuelle.

L'e-inclusion et ses conséquences

On constate que la quasi totalité des adolescents et enfants rencontrés a un ordinateur à son domicile ainsi qu'un accès à Internet. Selon le STATEC, 80% des ménages sont connectés à Internet (Statec, 2009). Nombreux sont ceux dont l'ordinateur se trouve dans leur propre chambre à coucher (taux en constante augmentation, spécifiquement chez les plus jeunes). Ils peuvent ainsi surfer sur Internet et jouer sans aucune surveillance. Selon une étude du CEPS, 8% des enfants entre 11 et 13 ans, 18% des adolescents entre 14 et 16 ans et 37% des adolescents entre 17 et 19 ans ont leur propre ordinateur. (CEPS/INSTEAD, 2009)

Les enfants utilisent leurs ordinateurs à des fins multiples. La majorité s'en sert pour jouer, surfer, communiquer dans des réseaux chat ou encore gérer leur page web personnelle ou leurs publications dans un des nombreux réseaux sociaux.

On remarque que les jeunes ont une forte attirance pour la communication via le chat plutôt que via les courriers électroniques. En général, la communication électronique ne se fait qu'avec un nombre de camarades assez restreint. Les forums publics ne sont pas aussi souvent utilisés que les chats via, par exemple, MSN ou ICQ. Beaucoup utilisent conjointement la webcam et le micro pour chatter.

Les pages web gérées par les enfants leur servent de « cartes de visite ». Elles leur permettent de faire leur propre « marketing » ou encore de tenir des sites de photos pour que leurs proches résidant à l'étranger puissent suivre leur vie familiale au Luxembourg. Ainsi, nous avons rencontré des enfants, même très jeunes (8 ans), qui gèrent des sites de photos familiales. Même en 2008, qu'ils soient adolescents ou beaucoup plus jeunes, la plupart mettent toujours des images en ligne sans savoir que celles-ci ne sont pas protégées contre la copie. Depuis 2008, on a cependant constaté une très forte augmentation des inscriptions aux réseaux sociaux comme Facebook notamment. Ainsi, des enfants de 10 ans ont déjà ouvert leur propre compte.

Comme les années passées, beaucoup d'adolescents téléchargent des fichiers mp3 ou des vidéos, installent des jeux téléchargés sans se soucier de leur provenance ou de leur contenu réel (chevaux de Troie ou encore spyware). Certains visitent même des sites de type cracking pour récupérer des générateurs de clés ou des crackers de mots de passe, sans pour autant savoir ce qu'ils risquent (voir la cartographie du malweb¹), quand d'autres téléchargent des outils d'attaque (chiffre estimé à 2-3%). Certains savent même comment changer leur adresse IP toutes les trente minutes pour ne pas être repérés.

Les adolescents mais aussi les enfants (de plus en plus jeunes) utilisent les mêmes applications et services web que les adultes, à l'exception de l'e-banking. Ils ont des

¹ <http://www.cases.public.lu/fr/risques/2007/malweb/index.html>

identités électroniques, confient des données très personnelles à leur ordinateur et ne se soucient pas vraiment des dangers liés à l'utilisation de l'Internet. Ils ne sont ni conscients de la valeur des données qu'ils confient à un ordinateur non sécurisé, ni de l'ampleur des risques auxquels ils s'exposent par leur négligence et leur faible niveau de savoir-faire.

La majorité a déjà été confrontée à des malwares sur son ordinateur. Pourtant, ils ont tendance à les ignorer et même à accepter l'existence de ces virus, vers et trojans faute de savoir les éviter, les trouver et les éradiquer.

Quasiment tous les enfants et adolescents ont un téléphone mobile. La plupart de ces téléphones sont équipés de caméras et de la fonctionnalité bluetooth. Beaucoup accèdent même à Internet avec leur téléphone mobile. De nos jours, il n'est pas rare de rencontrer des élèves de classe de 3e (9 ans) qui possèdent déjà leur propre téléphone mobile avec connexion Internet. L'envoi de MMS est également très courant.

L'utilisation excessive de ces moyens de communication, et notamment dans le cadre de plus en plus répandu du harcèlement, a mené de nombreux établissements scolaires à interdire l'utilisation des téléphones mobiles dans leur enceinte. Une étude dans ce domaine a été menée par l'université de Luxembourg en coopération avec CASES. (Georges Steffgen, 2009)

Analyse des expériences rapportées

MOTS DE PASSE

Les enfants et adolescents gèrent plusieurs outils de communication² ou services en ligne³ dont l'accès repose sur un identifiant et un mot de passe. Nombreux sont les jeunes qui ne comprennent pas l'importance de ces codes d'accès. Ils n'ont même jamais pensé aux conséquences que pourrait avoir une divulgation de leurs données personnelles ou à ce qu'un attaquant pourrait faire s'il connaissait leur identifiant et leur mot de passe.

Les jeunes ont toujours tendance à choisir des mots de passe très faciles à deviner. Cette imprudence peut avoir des conséquences très fâcheuses, telles la défiguration de sites Internet, la perte de confidentialité des courriers électroniques et l'atteinte à la réputation due à des injures ou à des propos désobligeants faits en leur nom dans des forums ou des chats. Comme pour les années précédentes, ces cas ont été fréquemment relatés par les jeunes lors des présentations 2008-2009.

Beaucoup d'enfants vont même jusqu'à échanger leur mot de passe avec leurs amis. La grande majorité des cas nous a été rapportée par des filles. Les enfants ne sont pas conscient que ces pratiques peuvent avoir des conséquences très graves. Beaucoup ont

² Ordinateur, GSM

³ MSN, facebook, e-mail, homepage, blogg, jeux en ligne, forums, etc.

rapporté avoir eu des problèmes par après puisque l'ami auquel ils avaient confié le mot de passe en avait profité pour les espionner ou pour se venger.

Les jeunes ne connaissent pas les techniques existantes pour récupérer les mots de passe comme l'attaque par dictionnaire, l'attaque ciblée par le social engineering, le « shoulder surfing » ou encore les programmes tels que les keyloggers ou chevaux de Troie.

La naïveté sur laquelle repose ce problème est directement imputable à l'âge des utilisateurs. Ce n'est qu'à partir de 14-15 ans qu'ils commencent à se rendre compte de certains dangers, c'est-à-dire après sept ans d'utilisation d'Internet...

MALWARES

Presque tous les enfants et les jeunes savent qu'il existe des virus en informatique. A contrario, peu connaissent l'existence des vers et ce qui les différencie des virus. Quasiment aucun ne peut associer un concept aux malwares. Le nombre de jeunes tend vers zéro lorsqu'il s'agit de définir comment fonctionnent ces malwares, et plus précisément, quelles vulnérabilités ils exploitent. La plupart d'entre eux ont déjà subi les conséquences d'infections de vers, de virus ou de trojans. Celles-ci sont souvent perçues comme une « fatalité » à laquelle on ne peut échapper. Les jeunes considèrent que la destruction des fichiers qui se trouvent sur leur ordinateur est l'impact maximal d'une telle infection. Cependant, ils ne prennent que trop rarement en considération les conséquences découlant d'une perte de confidentialité, d'intégrité et du vol d'identité.

Ce comportement « fataliste » peut, bien sûr, avoir des retombées catastrophiques, particulièrement en cas d'infection par un trojan, malware conçu pour espionner discrètement et non pour détruire. Une telle infection ne se détecte pas aussi rapidement que celle initiée par un ver destructeur, surtout si l'on sait que dans de nombreux foyers, les différents membres utilisent un même ordinateur familial et que tous ont des droits d'administrateur qu'allègrement ils lèguent aux malwares qu'ils attrapent.

Comme l'année dernière, des cas nous ont été rapportés où des jeunes utilisent des trojans pour espionner leurs camarades, par exemple, pour contrôler leur webcam et pour lancer de vrais espionnages à l'insu de la victime. De plus en plus de jeunes prennent conscience de ces moyens d'espionnage, mais nombreux sont encore ceux qui les ignorent, ceux-ci ont été stupéfaits d'apprendre qu'il était possible d'être surveillé de la sorte.

Les vecteurs d'infection les plus répandus sont le téléchargement via Internet de fichiers infectés, la visite de sites distribuant du malware (Provos, McNamee, Mavrommatis, Wang, & Modadugu, 2007) et le fait d'accepter des fichiers depuis MSN ou des forums de chat. Comme nous l'avons vu, le courrier électronique n'est pas très utilisé et, de ce fait, n'est pas un vecteur d'infection fréquent.

CHAT

L'utilisation du chat est très populaire parmi les jeunes et dès l'école primaire, MSN est l'outil le plus utilisé. L'avantage de cet outil est la possibilité de ne chatter qu'avec des personnes qu'ils ont accepté auparavant comme ami (white listing). Tous connaissent aussi la possibilité de pouvoir bloquer des personnes avec lesquelles ils ne veulent plus chatter. En grandissant, les jeunes commencent à fréquenter des forums en ligne ouverts.

Avec le début de la puberté, certains jeunes, en majorité des filles, commencent à fréquenter des forums ouverts en ligne, ce qui les expose à un très grand danger. Lorsqu'ils sont confrontés par les formateurs à ces dangers, beaucoup ne prennent pas au sérieux les mises-en-garde et estiment qu'ils maîtrisent la situation. Ce fait est très alarmant et les formateurs ont souvent dû parler aux responsables des classes pour que ceux-ci mettent à leur tour les enfants en garde.

L'utilisation massive de MSN amène parfois des parents à interdire son utilisation, ce qui pousse les enfants vers des forums ouverts, non limités à leurs pairs, et souvent fréquentés par des adultes.

L'usurpation de mots de passe est un problème que de nombreux jeunes ont déjà rencontré. Celui-ci est lié soit au choix d'un mauvais mot de passe, soit à l'échange de celui-ci entre camarades.

Dans les forums de chat, les injures, diffamations et calomnies sont légion. À cela s'ajoute un langage assez cru, particulièrement dans les forums ouverts. En outre, beaucoup de jeunes n'ont pas conscience que le choix de leur pseudonyme peut leur attirer des ennuis⁴.

Les programmes de chat comme MSN sont employés comme canaux de distribution des malwares, notamment les trojans. De plus en plus de jeunes n'ont aucun scrupule à utiliser ces programmes pour espionner, brancher des caméras (webcam) ou prendre le contrôle des téléphones portables de leurs camarades.

Les jeunes utilisateurs sont conscients qu'ils doivent être prudents dans les chat rooms. Ils savent qu'ils ne doivent révéler ni leur vrai nom, ni leur adresse, ni leur numéro de téléphone. Toutefois, certains cas ont été relevés où certains avaient physiquement rencontré des personnes qu'ils ne connaissaient que via Internet, et ce, en toute connaissance de cause. Les raisons invoquées restent floues. Quelques-uns disent qu'ils sont « tombés amoureux » et d'autres qu'ils voulaient rencontrer la personne « par curiosité ». La confiance que les jeunes ont en ces nouvelles formes de communication est alarmante et met en danger ceux qui ne sont pas conscients des dangers réels. Avec la forte adoption de Facebook en tant que site communicatif par les jeunes, ces tendances risquent de fortement s'intensifier. Depuis 2008, les formateurs insistent d'ailleurs beaucoup sur le sujet.

⁴ Lolita13, aimée12, bunny14

Parfois, les jeunes rencontrent des personnes qu'ils ne connaissent que par l'intermédiaire des forums de chat, pour réaliser des achats ou des ventes. On peut citer le cas d'un élève d'une école primaire fixant un rendez-vous à une personne adulte sensée lui acheter ses jeux.

Il arrive qu'un adolescent s'invente un personnage fictif sur Internet afin de se venger de camarades qui, selon ses dires, lui auraient causé du tort, ou même simplement pour le "fun".

Le harcèlement sexuel à tout âge via le chat est un fait très souvent rapporté. Les harceleurs essaient d'envoyer aux victimes des images pornographiques, respectivement les incitent à faire des images d'elles-mêmes ou à prendre physiquement contact avec eux. Vu que de nombreux enfants chattent, avec comme pseudonyme une adresse de courrier électronique, beaucoup d'entre eux reçoivent aussi des courriers électroniques de harcèlement. La gêne qu'ils éprouvent leur interdit souvent de parler de ces faits à un adulte. Ces enfants souffrent très souvent seuls et essaient de résoudre personnellement le problème. Lorsque les parents sont informés, ceux-ci réagissent généralement de façon incorrecte et interdisent l'utilisation du chat ou punissent même l'enfant victime. Durant les cours, les enfants ne se sont généralement adressés qu'à nos formatrices plutôt qu'aux formateurs. De plus, les enfants ne s'ouvrent que si l'on aborde directement le problème du harcèlement sexuel. Ainsi, dans chaque classe ayant suivi la formation, des cas de harcèlement ont été révélés.

INTERNET

Très rares sont les jeunes - enfants et adolescents - qui n'ont pas encore surfé sur Internet. La plupart l'utilisent sans l'assistance d'un adulte. Inconscients des dangers, insouciants et naïfs, ils visitent de nombreux sites et téléchargent quantité de fichiers.

Comme l'année passée, entre 10 % et 20% des lycéens nous ont rapporté être devenus eux-mêmes victimes d'escroqueries liées à des abonnements. Ainsi le Centre Européen des Consommateurs nous a rapporté qu'en une seule année, ils reçoivent plus de 500 appels liés aux fraudes concernant les abonnements d'enfants devenus victimes de sites allemands. Cette tendance est, selon le CEC, toujours croissante. Depuis 2008, et avec l'aide du CEC, les formateurs ont donc commencé à attirer l'attention des jeunes sur l'existence de ces pièges et à les informer en conséquences.

La fréquentation de sites pornographiques apporte également son lot de problèmes aux jeunes qui les fréquentent. En effet, ces visites sont suivies d'envois de spams qui polluent leur boîte mail et font naître chez eux la crainte que leurs parents finissent par s'en apercevoir et les punissent sévèrement.

Internet est aussi un moyen pour beaucoup de jeunes de se procurer des jeux qui ne sont pas destinés à leur catégorie d'âge. En effet, ils peuvent télécharger des jeux qui sont interdits à la vente, se trouvent sur l'index et ne sont pas vendus ou qui le sont uniquement aux adultes. Des problèmes liés à la consommation de vidéos violentes, voire extrêmement violentes, nous ont encore été signalés par des enfants d'écoles primaires.

Nombre des jeux que les jeunes se procurent illégalement sont infestés de malware.

Très peu connaissent les sites qui correspondent à leur âge de même qu'ils utilisent peu les portails de recherche pour enfants. Les sites tels que "Blinde Kuh" sont inconnus. Malheureusement ces sites sont aussi inconnus des enseignants des écoles primaires qui pourraient pourtant transmettre ce savoir à leurs élèves. Les enfants utilisent les mêmes moteurs de recherche que les adultes et tombent donc sur les mêmes sites.

Même les structures étatiques qui accueillent des enfants n'ont que très rarement des filtres installés. Ceci est vrai pour les écoles primaires, mais aussi pour beaucoup de lycées. Seules les maisons de jeunes ont déployé un projet qui met en place des mesures de sécurité comme des filtres, des anti-virus ou encore des pare-feu.

HOMEPAGE ET SOCIAL NETWORKING

Nombreux sont les jeunes qui réalisent des sites web ou qui se présentent sur des plateformes comme Hi5⁵ ou Facebook⁶. Dès l'école primaire, beaucoup d'enfants débutent un projet de site web (environ un quart). Ces sites regorgent de marques protégées, d'images et de fichiers mp3. En fait, les jeunes utilisent ces sites pour se faire leur propre publicité. Certains, particulièrement les enfants de familles immigrées, utilisent Internet pour rester en contact avec les membres de leur famille restés dans leur pays d'origine.

En 2009, le nombre d'enfants qui utilisent Facebook comme plate-forme de communication a nettement augmenté. Cependant, beaucoup sont inconscients des nombreux dangers qu'engendrent les profils non protégés. La course aux amis est un phénomène dangereux qui illustre bien l'insouciance des enfants. Beaucoup ont plus de 300 "amis" Facebook, et ils acceptent toutes les demandes d'ajouts à des liste d'amis, sans se soucier de l'identité de celui qui envoie l'invitation. Ils ne sont pas conscients que chacun de ces "amis" peut voir leur profil, analyser leur habitudes et saura en fait les localiser physiquement s'il le veut.

Peu d'entre eux sont conscients du fait que n'importe quel internaute peut consulter leur page web. Ils ignorent d'une part ce qu'est le Word Wide Web et le confondent le plus souvent avec le « white listing » de MSN.

Tous sont inconscients de la législation en vigueur sur les marques et œuvres d'art et ne comprennent pas pourquoi ils devraient demander l'autorisation des personnes concernées avant de placer des photos sur Internet. Certains jeunes publient des détails très privés ou encore des photos lascives sans se rendre compte des conséquences d'un tel acte. En outre, beaucoup croient qu'il est possible de protéger les images ou photos de leur site contre la copie.

⁵ <http://www.hi5.com/>

⁶ <http://www.FacebookFacebook.com/>

Malheureusement, Internet est aussi souvent utilisé afin de propager des diffamations et des calomnies. Les jeunes ne connaissent pas les lois qui protègent le droit à la vie privée et ne se fient pas aux adultes ou à la police pour faire cesser ces agissements s'ils en sont victimes.

TELEPHONES MOBILES

Quasiment tous les enfants (généralement à partir de la première communion) ont un téléphone mobile. Ces téléphones sont généralement équipés, en plus des fonctionnalités voix, d'un appareil photo, d'écrans couleurs, d'une connectivité vers Internet (GPRS, WiFi), de Bluetooth, MMS, SMS, de capacités plus ou moins grandes permettant de stocker des fichiers mp3, photos et vidéos. Certains forfaits payés par les parents donnent accès à Internet 24h/24. De ce fait, ceux qui disposent de ce genre de forfait échappent à la vigilance et au contrôle parental dès lors qu'ils se trouvent par exemple dans l'enceinte de l'école ou à l'extérieur. Dans ce cas précis, l'accompagnement des parents n'est plus possible.

Les jeunes se servent de leur téléphone pour communiquer entre eux et organiser leur vie privée. Beaucoup l'utilisent aussi pour exécuter toutes formes inimaginables de harcèlement. A titre d'exemple, citons la prise de photos "sensibles" d'élèves et/ou professeurs dans des salles de classe ou les vestiaires et qui a mené de nombreuses écoles à interdire l'utilisation des téléphones mobiles dans leur enceinte.

Le partage de films extrêmement violents (happy slapping, snuff, exécutions, etc.) ou à contenus pornographiques est à la mode, même parmi les enfants des écoles primaires qui, pour certains, déclarent en souffrir. Dans quelques cas, les enfants ou adolescents ont même été forcés de regarder ces films ou de les stocker sur leur téléphone portable.

L'utilisation de « super bluetooth », application java tournant sur les téléphones mobiles destinée à prendre le contrôle d'autres appareils munis de bluetooth, se répand encore et toujours d'un lycée à l'autre. Cet outil d'attaque très efficace peut causer des dommages conséquents en cas de compromission d'outils de plus en plus performants disposant d'informations hautement confidentielles et personnelles.

Analyse des compétences

Les jeunes et enfants adoptent facilement les nouvelles technologies, et particulièrement celles employées pour communiquer, se présentant sous forme d'accessoires ou d'applications à prix modique ou même gratuits, et qui leur permettent de faire leur propre « promotion ». La rapide adoption de Facebook en est un bon exemple.

On constate toujours chez eux de faibles compétences techniques. Au-delà de l'utilisation de ces accessoires et applications, leur fonctionnement leur est totalement méconnu. En outre, très rares sont ceux qui cherchent à en comprendre la technologie.

Ils ne connaissent pas les dangers du web et visitent les sites qui offrent ou promettent des contenus gratuits susceptibles de les intéresser. Beaucoup téléchargent des petits jeux ou des applications sans se soucier du malware qui pourrait s'y dissimuler.

Les jeunes ne se rendent pas compte qu'Internet est un gigantesque réseau informatique qui connecte plus de 1.5 milliards de personnes. Ils ne sont pas conscients de l'ampleur du réseau et des différents profils des personnes qui l'utilisent. À ce titre, ils sont vulnérables à différents types d'attaques.

Prévention et application de contre-mesures

REPRESSION

Les enfants ne se doutent pas qu'ils peuvent faire appel à la police s'ils deviennent victimes ou sont témoins d'une attaque de cyberbullying, de harcèlement sexuel, d'arnaques, etc. Ils ne savent pas que les lois ont été créées pour protéger les citoyens et non pas pour les punir.

Ils doivent apprendre que contacter la police ou même se confier simplement à un adulte, ce n'est pas « donner » quelqu'un, mais que c'est un acte de défense ou un appel aux secours tout à fait légitime.

MOTS DE PASSE

Les mots de passe choisis par les jeunes sont le plus souvent très faciles à deviner : noms propres ou numéros de téléphone. Le même mot de passe est souvent utilisé pour chaque système, ce qui implique que si quelqu'un trouve un mot de passe, il aura accès à tous les services utilisés par cette personne.

Malheureusement, beaucoup de jeunes confient leurs mots de passe aux navigateurs tels qu'Internet Explorer ou Firefox ou même à des copains et ne se doutent pas des dangers que cela induit.

Souvent, ils ignorent qu'ils doivent sortir des applications web par le bouton « se déconnecter » pour empêcher qu'un tiers (à la bibliothèque ou dans un cybercafé par exemple) puisse avoir accès aux applications en restaurant les sessions interrompues.

ANTIVIRUS

Tous les jeunes savent qu'il est important d'avoir un antivirus, mais beaucoup ne savent pas qu'il faut le mettre à jour régulièrement, c'est-à-dire tous les jours. On en rencontre souvent qui prétendent avoir un antivirus, mais la licence est périmée et ils ne reçoivent plus les mises à jour. Ils n'ont pas connaissance du fait qu'un citoyen peut avoir accès à des produits gratuits. Les tests effectués lors des séances ont montré que les jeunes ne savent pas où chercher pour trouver l'antivirus sur leur ordinateur. Quant aux enfants ils ne sont pas du tout sensibles à cette notion et c'est alors aux adultes de s'en charger. L'expérience montre malheureusement que souvent ceux-ci n'ont pas de connaissances assez développées en la matière ou n'ont pas les réflexes appropriés.

Nombreux pourtant sont les enfants et les jeunes qui ont déjà subi une attaque de malware.

Beaucoup d'enfants téléchargent de façon illégale des jeux commerciaux sur des réseaux d'échange. Puisque ces jeux sont souvent infestés de codes malicieux, les jeunes désactivent consciemment l'antivirus afin de pouvoir installer ces jeux et s'exposent à des risques sérieux.

FIREWALL

L'utilisation de firewall personnel est très rare. Ce concept est méconnu de la plupart des jeunes.

PATCH

L'importance des mises à jour est sous-estimée. Beaucoup pensent que ce sont des rappels dont ils ont déjà connaissance. Ils les ferment donc dès qu'ils les voient. Aucun jeune ne connaît la raison pour laquelle il est indispensable de faire les mises à jour et aucun ne sait qu'elles doivent être installées pour toutes les applications se trouvant sur l'ordinateur.

Spyware remover

Peu de jeunes utilisent des logiciels de spyware remover.

Conclusion

Les enfants et adolescents adoptent rapidement toutes les technologies de l'information et de la communication et les utilisent à toutes fins utiles. Cependant, leur manque de connaissances et de méfiance les rend vulnérables à de très nombreux dangers issus de la société de l'information. Ainsi, le vol d'identité, le harcèlement sexuel, les e-mails de menace, les malwares ou encore le cyberbullying sont des menaces qui s'avèrent très communes dans le monde des jeunes.

Il est réellement impératif et urgent d'accompagner et d'encadrer les enfants et les jeunes dans leur découverte de ces technologies, mais il importe aussi d'aider les parents, éducateurs et formateurs à suivre et à comprendre cette mouvance.

Les enfants tout comme leur entourage doivent être formés à l'utilisation correcte des nouvelles technologies de l'information. Les structures accueillant les enfants, comme notamment les écoles, lycées et foyers d'accueil devraient suivre l'exemple des maisons de jeunes et intégrer l'aspect sécuritaire tant au niveau formation, éducation qu'infrastructure.