



Criminalité sur Internet L'activité en plein essor

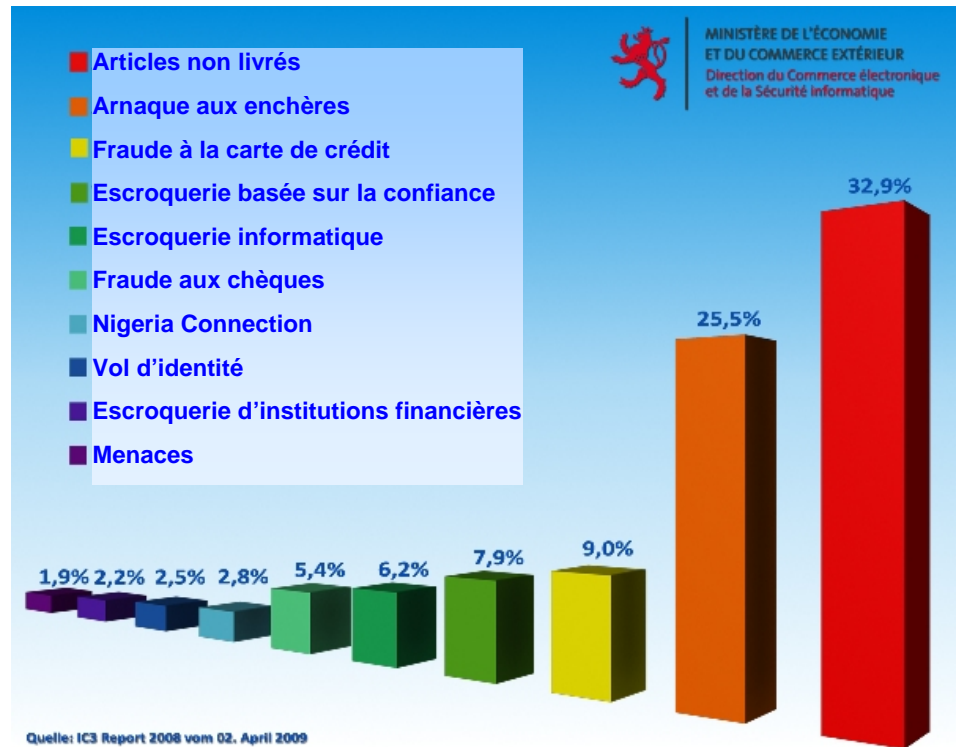
Pour plus de sécurité, adoptez les réflexes CASES !

L'anonymat d'Internet libère les énergies criminelles

La criminalité sur Internet progresse aussi vite qu'Internet. Les idées d'arnaque n'y connaissent pas de limites et l'utilisation des technologies et infrastructures dernier cri joue également un rôle capital. La possibilité de déléster facilement les gens de leur argent renouvelle sans cesse les énergies criminelles. Les tentatives d'escroquerie traditionnelles connaissent une véritable renaissance. Pour cela, les cybercriminels mettent en œuvre de nouvelles méthodes offertes par Internet.

Les internautes se méfient généralement des e-mails contenant des pièces jointes suspectes, mais les escrocs rivalisent d'ingéniosité sur le Net. Ils ont recours aux méthodes les plus modernes pour duper même les utilisateurs avertis et leur nuire.

Le phishing compte parmi les menaces qui connaissent l'essor le plus vigoureux et contre lesquelles les experts en sécurité mettent en garde. Cette forme d'attaque consiste à amener quelqu'un à faire une chose qu'il ne ferait jamais dans des circonstances normales. Dans le monde informatisé actuel, il s'agit, par exemple, de donner ses données d'authentification. Pour cela, les criminels utilisent les e-mails. Le phishing n'est toutefois pas la seule escroquerie en pleine croissance.



Types d'attaque en 2008

Le rapport annuel du centre américain de réclamations sur la criminalité sur Internet, IC3, donne un aperçu des nombreuses tendances et des nouveaux modèles de cybercriminalité à croissance rapide. Comme les années précédentes, le rapport fait état pour 2008 d'une nouvelle hausse de la criminalité sur Internet. L'IC3 a ainsi reçu quelque 275 284 plaintes l'an dernier, soit 68 400 de plus que l'année précédente. Les cas d'escroquerie signalés au centre ont engendré en 2008 264,6 millions de dollars américains de dommages financiers. En 2007, ce chiffre s'élevait à 239,1 millions de dollars.

La majorité des tentatives de contact de criminels avec des victimes potentielles se font par e-mail. 74 % des contacts se font par ce biais, suivi du contact par les sites Internet. Une part déterminante des tentatives d'escroquerie en 2008 est constituée

par l'envoi à des fins d'arnaque d'e-mails non sollicités, les spams.

L'idée d'utiliser les spams pour obtenir des informations personnelles d'utilisateurs n'est pas neuve. Mais la forme a quelque peu changé puisque, aux États-Unis, on rencontre de plus en plus d'e-mails falsifiés prétendument envoyés, par exemple, par la police ou le FBI, dans lesquels sont demandées des données personnelles comme les numéros de compte bancaire. Ces informations sont censées aider l'expéditeur du message dans des enquêtes sur des transactions criminelles. Les e-mails font croire qu'il s'agit d'enquêtes sur des transactions à l'étranger, souvent liées au Nigeria. Il est suggéré aux destinataires des e-mails frauduleux qu'ils pourraient contribuer à la réussite de l'enquête. Naturellement, une récompense est prévue en cas de collaboration aboutissant à une conclusion heureuse des enquêtes.

L'imagination des escrocs est sans limite. D'autres e-mails frauduleux déclarent à leur destinataire qu'il ferait l'objet d'enquêtes terroristes s'il refusait de collaborer. Par cette forme d'e-mails frauduleux, les cybercriminels tentent d'exploiter les faiblesses humaines en jouant avec la serviabilité, la fierté, l'avidité, la compassion ou la peur des utilisateurs, une méthode vieille comme le monde.

Les marchandises non livrées ou les paiements non réalisés ont constitué la plainte la plus fréquente en 2008, détrônant ainsi l'arnaque aux enchères. Cette fraude représentait 32,9 % des plaintes signalées à l'IC3. Le nombre de plaintes relatives à ce type de fraude a ainsi augmenté de 32,1 % par rapport à 2007. Suivent les plaintes pour fraude aux enchères avec 25,5 %, pour lesquelles une diminution a été constatée par rapport à 2007.

La fraude concernant les cartes bancaires et de crédit est passée de la 4^e à la 3^e place du classement des types d'arnaque en 2008, ce qui représente, selon l'IC3, 9 % des plaintes. Cette fraude enregistre ainsi une progression de plus de 40 % par rapport à l'année précédente.

Les types d'arnaque exploitant la confiance ou les faiblesses de l'ordinateur d'un utilisateur sont également en hausse. Les plaintes pour escroquerie basée sur la confiance et pour escroquerie informatique occupent respectivement la quatrième et la cinquième positions avec 7,9 % et 6,2 % des plaintes. D'autres plaintes concernent les arnaques aux chèques, les lettres nigérianes, le vol d'identité, l'escroquerie des institutions financières et les menaces. Les lettres nigérianes et les menaces affichent aussi une progression par rapport à 2007.

D'après les statistiques de l'IC3, ce sont surtout les internautes masculins qui ont subi des pertes financières. Si on s'intéresse aux tranches d'âge, les pertes financières sont essentiellement l'apanage des personnes entre 40 et 49 ans.

Problèmes des poursuites pénales

Les autorités ne sont chargées de la poursuite de tentative d'arnaque que dans un cas sur sept. Les criminels sont incités par là à agir davantage sur Internet puisqu'ils s'y sentent relativement à l'abri de poursuites pénales.

Un facteur important empêchant l'enquête et la poursuite de la cybercriminalité est l'anonymat d'Internet derrière lequel les criminels peuvent se cacher. Les enquêtes et poursuites de délits sont aussi compliquées par le fait que les malfaiteurs et les victimes se trouvent à différents endroits du monde. C'est une caractéristique particulière de la cybercriminalité. Dans la criminalité classique, cette particularité est rare. La réussite des poursuites pénales de cybercriminels nécessite donc la coopération de plusieurs autorités au niveau international, ce qui retarde les enquêtes et réduit l'efficacité des autorités répressives.

L'absence de preuves est un autre problème rencontré en cours d'enquête. Peu d'utilisateurs sont conscients que les données numériques comme les e-mails, les messages ou informations sur les sites Internet doivent être conservées à titre de preuves. Sans preuves, les enquêteurs ne peuvent rien faire.

En outre, pour que les enquêteurs interviennent, l'utilisateur doit porter plainte pour escroquerie. Le fait d'aller voir la police constitue cependant un frein pour certains utilisateurs. Et cela prend du temps. Des internautes hésitent à entamer de telles démarches par honte infondée. Ils ne veulent pas que d'autres sachent qu'il a été possible d'abuser de leur naïveté, peur, avidité ou compassion.

Le montant des dommages financiers représente un autre obstacle à la déclaration. La plupart des utilisateurs se demandent si la perte de 80 EUR mérite réellement les tracas et la perte de temps engendrés par une plainte. Certains utilisateurs hésitent aussi à confier leur ordinateur à un enquêteur. Ce n'est souvent qu'à ce moment que l'utilisateur réalise le nombre de données privées enregistrées sur son ordinateur. Et il ne veut pas que celles-ci soient accessibles à des tiers. Or, sans plainte, pas de poursuite possible.

Une activité lucrative :

l'arnaque aux enchères en ligne

Selon le site d'enchères en ligne Ebay, Ebay Allemagne compte 20 millions d'utilisateurs inscrits qui y négocient chaque année des marchandises pour une valeur de 8,5 milliards de dollars. Les rapports d'escroquerie se multiplient. La porte-parole d'Ebay, Maïke Fuest, souligne néanmoins dans le *Süddeutsche Zeitung* que les problèmes ne concernent qu'une fraction d'un pour cent. Sur un volume de vente de 8,5 milliards de dollars, une fraction d'un pour cent représente toutefois quand même un chiffre encore considérable.

Parents et jeux informatiques

L'enfant ne doit pas être laissé sans surveillance ni accompagnement face à l'ordinateur, aux jeux, aux consoles, à Internet ou au téléphone mobile. Il est généralement si absorbé par le monde virtuel qu'il ne remarque pas le temps qu'il passe devant un appareil.

Mais la durée n'est pas le seul aspect à prendre en compte dans les règles régissant l'utilisation des médias numériques. Les parents devraient se familiariser avec les logiciels de jeu et d'apprentissage adaptés. Il leur est recommandé de connaître les différents types de jeu et les objectifs du jeu, comme pour un jeu de société. Ils peuvent ainsi mieux diriger la consommation de jeu sur ordinateur ou console et donner à l'enfant l'orientation nécessaire. Les parents sont alors mieux en mesure de fournir à leur enfant des jeux adaptés à leur âge.

Accompagner les enfants dans l'utilisation des nouveaux médias signifie aussi jouer de temps en temps ensemble à l'ordinateur. Les parents doivent demander à leurs enfants de leur expliquer les jeux avec lesquels ils jouent volontiers et régulièrement. Les enfants sont fiers quand ils peuvent expliquer quelque chose à leurs parents.

Comme pour un jeu de plateau habituel autour duquel toute la famille se réunit, les parents devraient jouer avec leurs enfants aux jeux informatiques, les games. Les enfants

ne devraient pas jouer à des jeux non adaptés à leur tranche d'âge. Les enfants en âge préscolaire ou fréquentant l'école primaire ne peuvent pas encore faire clairement la distinction entre réalité et fiction, par exemple. La tranche d'âge recommandée est indiquée sur l'emballage des jeux. Les parents devraient aussi s'informer à l'aide de critiques et de recommandations de jeu. À ce propos, les parents doivent aussi savoir avec qui, où et à quelle fréquence l'enfant retrouve des amis pour jouer à l'ordinateur.

Les enfants accèdent aussi souvent à des jeux via des adultes, des jeunes de leur entourage ou des frères et sœurs plus âgés. La prudence est ici de rigueur. Un jeu de tir à la première personne ne devrait pas se retrouver entre les mains d'un enfant. Cependant, lors des formations d'enfants au Luxembourg, les collaborateurs du portail luxembourgeois de la sécurité de l'information CASES sont très souvent confrontés à des enfants qui parlent de leurs expériences avec des jeux absolument pas recommandés pour leur âge.

Il est important de montrer aux enfants des alternatives attrayantes aux jeux informatiques. Jouer sur l'ordinateur ne doit pas être leur seul

passer-temps. Les enfants doivent avoir une activité physique et intellectuelle pour compenser les longues heures passées devant l'écran. L'équilibre peut être trouvé en alternant jeux informatiques et jeux et activités en plein air.

Les parents ne doivent pas utiliser les jeux informatiques comme récompense, punition ou baby-sitter. Ils doivent aussi discuter entre eux pour partager leurs observations et expériences sur les jeux sur ordinateur et console.

L'accompagnement des enfants dans le monde numérique nécessite une certaine connaissance de ce milieu. Comme pour un jeu de société, les parents peuvent définir des règles d'utilisation de ces médias numériques pour les enfants. Ils peuvent ainsi découvrir ensemble le monde numérique en s'amusant.

De façon générale, les utilisateurs devraient se tenir au courant des types d'arnaque qui sévissent dans notre société du savoir. L'application des règles de sécurité informatique, comme un ordinateur protégé, est indispensable. Ces mesures de protection devraient devenir des réflexes comme verrouiller la porte de sa maison ou boucler sa ceinture en voiture.

Conseil de sécurité :

informer les enfants

Les enfants et les adolescents passent énormément de temps sur Internet. À cause de leur naïveté et de leur besoin de communiquer et de jouer, ils constituent une cible privilégiée des cybercriminels. Les enfants et adolescents réalisent rarement qu'ils sont victimes d'actes criminels. De plus, ils se sentent souvent coupables ou hésitent à en parler avec leurs parents parce qu'ils craignent d'être privés d'Internet. Par ailleurs, se rendre dans un bureau de police représente un frein immense pour les enfants et les adolescents. Or, sans plainte, pas de poursuite possible. Les criminels peuvent poursuivre leurs méfaits sur Internet sans craindre de sanction. Il est donc recommandé aux parents d'accompagner leurs enfants sur Internet et de discuter avec eux des dangers possibles sur le réseau. Ni les enfants ni les parents ne devraient répondre aux criminels par e-mail, MSN ou autres voies. Ils doivent plutôt enregistrer des preuves et dénoncer les agissements criminels.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu