



CASES articles

Série d'articles CASES : À poil sur la toile ? – Protégez vos données !

Médias interactifs sécurisés Participez vous aussi !

Pour plus de sécurité, adoptez les réflexes CASES !

Les réseaux sociaux sont certes populaires, mais ne sont pas sans dangers

La popularité des « réseaux sociaux » sur Internet reste entière. Ces réseaux offrent de nouveaux moyens de communication ainsi que des opportunités inédites. Pour de nombreux utilisateurs, ils font partie de la vie de tous les jours, sur le plan professionnel comme sur le plan privé. L'humanité découvre la société de l'information et les réseaux sociaux sont LE phénomène du XXI^{ème} siècle. Ils enthousiasment leurs utilisateurs et leur donnent un sentiment d'appartenance et de reconnaissance. Dans le même temps, la sphère privée des utilisateurs est bien souvent la première à pâtir de cette situation.

Le nombre d'utilisateurs des réseaux sociaux sur Internet a littéralement explosé au cours des deux à trois dernières années. Pour le néophyte, la première visite d'un tel réseau s'accompagne souvent de l'impression que bon nombre de ses utilisateurs y divulguent des données privées selon la devise « Je suis là ! Retrouve-moi ! ». Une récente étude de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) recommande de se méfier des soi-disant « amis » et d'une trop grande insouciance sur l'Internet.

Selon des chiffres fournis par le service Internet Alexa, la page d'accueil du réseau social « MySpace » a accueilli quelque 114 millions de visiteurs en juin 2007, ce qui en fait une des pages web les plus populaires aux États-Unis. Au cours de la même période, le réseau



« Facebook » a connu une augmentation de 270 % du nombre de ses visiteurs au niveau mondial. Les réseaux sociaux sont des secteurs en plein boom sur l'Internet car une toute nouvelle forme de communication y est forgée et entretenue.

Journaux intimes très publics, calendriers et autres profils d'utilisateurs permettent de créer des moyens de communication presque incroyables. Il en résulte un échange d'informations comme l'humanité n'en a jamais connu auparavant. Le XXI^e siècle peut être qualifié de siècle des technologies de l'information. Mais comme toutes les technologies et tous les moyens de communication modernes, ces nouvel-

les possibilités ne sont pas sans dangers.

Dans les réseaux sociaux, la devise affichée est bien souvent : « Ma liste de contacts est longue, je suis donc important, influent et bien meilleur que tous les autres ! ». Les utilisateurs publient très souvent des informations personnelles les concernant, ou concernant leur entourage et même d'autres personnes. Ils ne sont souvent pas conscients du nombre important de lecteurs qui épluchent leurs profils. Une utilisation abusive des données privées par des tiers est donc très vite arrivée.

Selon l'ENISA, un réseau social peut être comparé à une cocktail-party numérique. Les informations divulguées par une personne sur de tels réseaux

se propagent toutefois beaucoup plus largement que lors d'une fête dans le monde réel. Ceci concerne aussi bien les publications volontaires, que fortuites ou involontaires.

Un sentiment de sécurité trompeur

La majorité des utilisateurs de réseaux sociaux s'y sent en sécurité. Ils croient à l'existence d'une sorte d'intimité et de discrétion dans le monde numérique – à tort ! Des révélations intimes faites sur un réseau social de l'Internet, et semblant sans importance aux yeux de l'utilisateur, peuvent avoir des répercussions néfastes, souvent même de nombreuses années plus tard. Lors d'un entretien d'embauche, un dossier numérique créé des années plus tôt par le candidat peut par exemple éveiller des sentiments bien négatifs auprès de l'employeur potentiel.

Les utilisateurs devraient également tenir compte du fait qu'il est aujourd'hui possible de recueillir automatiquement des informations relatives à des personnes en ayant recours à des logiciels spécifiques de reconnaissance faciale ou d'images. Ces informations ne sont alors pas toujours exploitées et utilisées dans l'intérêt de l'utilisateur. Les utilisateurs des réseaux sociaux devraient savoir qu'une fois divulguées sur l'Internet, il n'est plus possible d'effacer des informations. Il existe par exemple des entreprises qui copient et archivent automatiquement des données dans un but commercial ou afin de les préserver.

Si des données privées tombent entre de mauvaises mains, il est fort possible que la réputation de la personne en pâtisse ou qu'elle soit victime d'un vol d'identité. Les célébrités sont des victimes particulièrement populaires. Stalking, mobbing et espionnage industriel sont les fréquentes résultantes du monde virtuel et présentent des dangers pour le monde réel. Bon nombre d'utilisateurs d'Internet deviennent ainsi victimes de stalkers, ceux-ci leur envoyant une multitude d'e-mails et les submergeant avec des commentaires et des messages. Pour la victime, cela peut être synonyme de nuisance physi-

que et morale passagère ou même à long terme.

Le cyberbullying – ou harcèlement par le biais de moyens de communication modernes – est une autre forme d'agissement qui peut toucher les utilisateurs. Les réseaux sociaux offrent d'innombrables possibilités dans ce domaine. L'exclusion de certains groupes d'utilisateurs ou le vol d'identité et de données au détriment de l'utilisateur ne représentent que quelques exemples issus de la longue liste d'attaques possibles. Dès 2006, le cyberbullying dans un réseau social a mené au suicide d'une jeune fille de 13 ans aux États-Unis.

D'autres formes d'attaques exploitent la crédulité des personnes ou des sociétés afin d'obtenir des informations. Les spécialistes parlent alors d'« attaques de social engineering ». Cette forme d'attaque permet à des tiers d'obtenir des informations et des données qu'ils peuvent exploiter à des fins criminelles. Les réseaux sociaux facilitent le travail des pirates car de nombreux utilisateurs y publient des informations, sans être conscients de leur réelle valeur pour les criminels. Ces utilisateurs devraient savoir que ce ne sont désormais plus seulement les grandes entreprises qui sont touchées par l'espionnage industriel, mais également de nombreuses sociétés de taille moyenne.

Aborder le sujet des dangers potentiels avec les enfants

Une attention toute particulière devrait être portée aux enfants et aux adolescents. Les enfants sont les « digital natives » de demain. Ils grandissent avec un média d'information comme il n'en a encore jamais existé dans l'histoire de l'humanité. Leur créativité s'y développe de façon ludique, mais ils constituent également les victimes privilégiées d'attaques ciblées.

Conseils de sécurité :

Le portail de la sécurité de l'information luxembourgeois CASES propose sur son site www.cases.lu, sous la rubrique Pratique / Solutions, un guide expliquant comment configurer les paramètres de son profil d'utilisateur sur Facebook pour un maximum de sécurité.

L'opération « À poil sur la toile ? Protégez vos données ! », qui a trouvé le soutien de nombreuses institutions luxembourgeoises, se poursuit à travers tout le pays jusqu'au 08.02.2009. Le but de cette campagne est de thématiser le respect de la sphère privée et la protection des données sur l'Internet. Tout un chacun peut y participer. Le matériel de sensibilisation correspondant est disponible sur www.cases.lu.

Des tiers malveillants mettent à profit la naïveté des enfants afin d'obtenir les informations les plus diverses. Cyber-criminels, pédophiles, mais également stalkers et mobbeurs ont ici bien souvent la tâche facile. Les enfants divulguent en effet avec beaucoup de crédulité des informations les concernant eux ou leurs parents, leur entourage ou leurs amis. Ils ne sont alors pas conscients des dangers qui peuvent être liés à ces révélations.

Les ordinateurs et l'Internet sont devenus incontournables dans la vie des enfants d'aujourd'hui. Les médias numériques possèdent d'ores et déjà une grande influence sur la société et il en sera de même dans le futur. Le traitement toujours plus rapide des informations déterminera et influencera de façon décisive la vie des prochaines générations. Les médias numériques exercent d'ailleurs une attirance presque magnétique sur les enfants. Il est donc recommandé d'aborder le plus tôt possible avec les enfants et les adolescents le sujet des dangers possibles, de leurs conséquences, ainsi que des moyens de protection à mettre en œuvre à l'ère du numérique. Les enfants apprendront ainsi à manipuler ces médias de façon sécurisée et responsable.

Ce que les utilisateurs devraient savoir

Les nuisibles d'Internet que sont virus, vers et chevaux de Troie se propagent encore plus rapidement par le biais des réseaux sociaux et peuvent par conséquent causer encore plus de dégâts. La popularité de tels réseaux et le grand nombre d'applications qu'ils proposent en sont les principales causes. Afin de diffuser par exemple des vidéos, des animations ou des présentations en ligne, de nombreux réseaux proposent à leurs utilisateurs d'utiliser des scripts, c'est-à-dire des petits programmes développés en propre. Or, les criminels utilisent ces programmes afin d'y intégrer des codes malveillants, permettant ainsi aux virus, vers et autres chevaux de Troie d'accéder à l'ordinateur de l'utilisateur. Cela peut aboutir à la perturbation du fonctionnement de la machine, à l'espionnage, au vol de données et même à la prise de contrôle à distance par des tiers.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu