



Internet, mobiles, WiFi, bluetooth, etc. - Pour plus de sécurité, adoptez les réflexes CASES !

www.cases.lu

EDITO

Tu veux être mon ami ?



facebook

Vu la montée en puissance des sites de networking, le choix du thème de cette 2^e édition du CASESmag s'est naturellement porté vers celui dont tout le monde parle : Facebook.

Nous en verrons les dangers tels que le vol d'identité et la perte en terme d'image, puis, nous vous expliquerons comment vous en protéger.

Dans un registre plus humoristique, mais hélas bien réel, nous exposerons quelques cas de dérives qui resteront dans les annales...

L'objectif est que vous gardiez en tête que, bien qu'Internet tend à déshumaniser les contacts et, de fait, vous incite à plus de libertés, les dangers sont là et sur la Toile, mieux vaut rester sur ses gardes tout comme dans la vraie vie !

François Thill, responsable de CASES

TENDANCE

Le saviez-vous ?

Un utilisateur britannique sur trois a recherché sur des sites dits de socialisation tels que Facebook des informations sur son patron, ses collègues ou des candidats à un emploi (source : étude du gouvernement britannique pour la campagne « Get safe online »).

Malgré toute l'attention portée aux intrusions et aux virus, il y a 72% de (mal)chances que la prochaine attaque réussie provienne de l'intérieur de l'entreprise (source : EuroCACS, conférence européenne sur les politiques de sécurité)

Plus d'un million d'ordinateurs seraient sous l'influence de robots capables d'envoyer pas moins de 100 milliards de spams par jour ! (source : RSA Conference 2008)

Un quart des utilisateurs britanniques des sites de réseaux sociaux tels que Facebook révèlent des informations sensibles sur leurs profils en ligne comme leurs coordonnées de contact (numéro de téléphone, adresse, etc.) ou leur date de naissance (source : étude du gouvernement britannique pour la campagne « Get safe online »).

Facebook : le paradis des voleurs d'identité

Qui ne connaît pas Facebook? Facebook, ce site de réseau social qui est le phénomène du moment. Bénéficiant d'une croissance fulgurante, Facebook comptait en mars 2008 plus de 67 millions de membres à travers le monde et, à ce jour, 22 491, rien que pour le réseau Luxembourg. Ce site déclenche les passions : certains ont déjà tous les symptômes de la dépendance et y passent des heures chaque jour, tandis que d'autres ne lui trouvent qu'un intérêt somme tout négligeable voire inexistant.

Quoiqu'il en soit, Facebook contribue fortement au vent qui souffle sur la Toile : le web 2.0. Seulement, le vent n'est pas toujours de très bonne augure et peut aussi être annonciateur de tempête...En effet, tout comme d'autres sites de socialisation connus, son utilisation présente des risques pour la sécurité des utilisateurs, et par leur biais, des entreprises.

Ce site suscite une levée de boucliers de nombreuses organisations non-gouvernementales de défense des droits de l'homme et de la vie privée, des pétitions circulent, des groupes se créent dénonçant cette violation de la vie privée...Tout ce remue-ménage alors que le danger « number one » n'est autre que l'utilisateur lui-même ! Trop souvent, hélas, les utilisateurs n'ont pas conscience de l'importance des informations qu'ils publient sur Internet, qui n'est autre que la porte d'entrée mondiale vers leur vie privée et personnelle...

Pour expliquer les risques qu'encourent les utilisateurs, nous allons prendre l'exemple

très parlant...ou plutôt croissant de Freddi Staur (l'anagramme d' « ID Fraudster »), le profil créé pour les besoins de l'enquête de Sophos. A partir de celui-ci, 200 « friend requests » ont été envoyés, ces demandes pouvant bien sûr être acceptées ou refusées par les destinataires. Résultat de l'opération: 41 % des utilisateurs de Facebook ont accepté de devenir « amis » avec Freddi Staur et donc, de lui divulguer leurs données personnelles. Freddi a ainsi eu accès à leur e-mail, leur date de naissance, leur numéro de téléphone, leurs photos de

famille ou d'amis, leurs goûts, leurs hobbies, leur parcours scolaire, leur profession et à bien d'autres données privées et personnelles. Cette enquête met parfaitement en lumière le comportement irresponsable des utilisateurs

” Veuillez noter que vous publiez sur ce site à vos risques et périls. ”

(extrait de la politique de confidentialité de Facebook)

des sites de réseaux sociaux.

Ce qui surprend, mais surtout inquiète, est de constater la consternante facilité avec laquelle la plupart des utilisateurs divulguent leurs informations...à une grenouille verte en plastique alors qu'ils refuseraient de les communiquer, et à juste titre, à un inconnu dans la rue. Freddi aura ainsi obtenu assez d'informations pour créer des messages de phishing ou des programmes malveillants personnalisés, deviner des mots de passe, ou même usurper l'identité de ses nouveaux « amis ». Il a maintenant toutes les armes en mains pour devenir un parfait cybercriminel !

Suite de l'article sur www.cases.lu



Dérives de Facebook

Monsieur S., planificateur financier respectable de Montréal a eu la curieuse idée de mettre pour photo de profil : lui-même...jusqu'ici, tout va bien...mais travesti en jolie infirmière blonde et « gonflée ».

Sur le profil de Monsieur L., conseiller financier contrairement à ce que pourrait faire penser sa photo (on le verrait plutôt en culturiste, chippendale ou escort boy), on peut y voir le moindre détail de sa vie : ce qu'il mange, ses films préférés...et les photos de ses conquêtes !

Tout comme les soldats américains en Irak, des soldats de Tsahal, l'armée israélienne se sont, récemment, affichés sur Facebook révélant des décors et des paysages de bases et sites classés top secret...ils se sont faits bien sûr réprimander comme il se doit!

Un jeune étudiant, Adam Morrison, a été soupçonné de vouloir commettre une tuerie similaire à celle de l'école Columbine en raison d'un faux profil publié sur Facebook. En créant son profil sur le site Facebook, il ne se doutait pas que quelqu'un utiliserait ensuite sa photographie et son identité pour créer un faux compte à son nom. Il s'est alors retrouvé en interrogatoire au poste de police...Adam a depuis annulé son compte.

Il y a peu, une récente faille de sécurité de Facebook a rendu accessible à tous les photos de certains utilisateurs paramétrés pour n'être visibles qu'aux amis...dont celles de son fondateur, Mark Zuckerberg.

...et le plus triste, c'est que c'est vrai !



Le cybersquatting en plein en...vol !

Selon l'organisation mondiale de la propriété intellectuelle (OMPI), le cybersquatting, en passant la barre des 2000 litiges, a atteint en 2007 un niveau sans précédent. En effet, l'année dernière, l'association a dû gérer 2156 plaintes pour cybersquatting, soit une augmentation de 18% par rapport à 2006 et de 48% par rapport à 2005. Loin devant, le champion toutes catégories des noms de domaines les plus « cybersquattés », le « .com » compte à lui tout seul 73,6% de l'ensemble des attaques.

Dans le trio de tête des activités les plus touchées se trouvent la biotechnologie et les produits pharmaceutiques, suivis de près par le secteur de la banque et de la finance, puis celui de l'Internet et de l'informatique.

Un quart de ces litiges a été réglé à l'amiable. Pour les autres, dans 85% des cas, il a été ordonné de transférer le nom de domaine concerné au plaignant et pour les 15% restants, le nom de domaine est resté aux mains du titulaire de l'enregistrement.

Le cybersquatting, c'est quoi ?

Le cybersquatting est une pratique qui consiste à être le premier à déposer un nom de domaine choisi en fonction de l'actualité, des entreprises réputées, des modes et tendances à venir, etc., en spéculant sur la prochaine notoriété du nom de domaine déposé. L'objectif est soit de détourner le trafic et donc, de tirer profit de la renommée de l'entreprise concernée, soit de le lui revendre au prix fort.

Les gouvernements contre-attaquent !

Que ce soit l'envoi de spams, la défiguration de sites, le piratage d'ordinateurs, etc., le maître-mot des gouvernements est dorénavant la lutte contre la cybercriminalité et ils n'y vont pas de main morte ! En effet, grâce à leur arsenal de lois toujours plus pointues, les tribunaux n'hésitent plus à prononcer d'importantes sanctions.

Nom : Robert Soloway dit le « King of Spam »
Nationalité : américaine
Méfait(s) : envoi de plusieurs dizaines de millions de spams. Dans sa base de données figureraient plus 157,8 millions d'adresses.
Antécédents judiciaires : condamnation en 2003 suite à une plainte de Microsoft et en 2006 Signe particulier : considéré comme le 8ème plus grand spammeur de tous les temps
Verdict : à venir. Risque jusqu'à **26 ans de prison**

Nom : Owen Thor Walker
Age : 18 ans
Pays : néo-zélandais
Méfait(s) : piratage des données bancaires, escroquerie d'envergure internationale ayant visé 1,3 millions d'ordinateurs
Préjudice : plus d'un million de victimes, les pertes se chiffrent en millions de dollars
Signe particulier : opère en bande organisée
Verdict : le 28 mai prochain. Pour l'instant, il attend en prison. Risque jusqu'à **5 ans de prison ferme**

Nom : Fouad Mortada
Profession : informaticien
Age : 26 ans
Nationalité : marocaine
Méfait(s) : usurpation de l'identité du Prince Moulay Rachid, frère du souverain Mohammed VI sur le site communautaire Facebook. Il a créé un compte au nom du premier.
Verdict : **3 ans de prison et une amende de 10 000 dirhams soit environ 880 euros**

De quoi faire réfléchir...

Suite de l'article sur www.cases.lu



Comment se protéger sur Facebook?

Comme tout outil mis entre les mains de quelqu'un qui ne sait pas s'en servir, Facebook peut devenir risqué pour qui ne suivrait pas ces quelques conseils :

1- Réglez les paramètres de confidentialité de Facebook (voir le [guide pratique "Comment configurer les paramètres de confidentialité de Facebook"](#))

2- Ne publiez pas d'informations personnelles telles que votre date de naissance ou votre numéro de téléphone, vos dates de congé qui pourraient vous exposer à des risques d'infractions, ainsi que des éléments - photos, vidéos ou autres - qui pourraient nuire à vos éventuelles opportunités de carrière (voir Dérives de Facebook)

3- Réfléchissez bien aux personnes que vous acceptez comme « amis »

Si, toutefois, vous avez commis une erreur de jugement, rappelez-vous qu'à tout moment vous pouvez supprimer un ami en cliquant simplement sur la croix à côté de son nom dans votre liste d'amis.

...et une dernière recommandation : se méfier de tout le monde ! Les photos et les profils exposés sont souvent trompeurs...

Inscrivez-vous pour recevoir les prochains numéros de CASESmag et consultez les dossiers, fiches thématiques, alertes et actualités sur :

www.cases.lu