

# Crime at high speed

Don't let Facebook or MySpace open your wallet to the world

By **David Malamed**, CA-IFA, CPA (Illinois), CFE and **Jennifer Fiddian-Green** CA-IFA, CFI, CAMS, CMA, CFE

---

An increasing number of Canadians are voluntarily posting their comings and goings and their personal data on Facebook and MySpace—even as alarms are sounding about the dangers of having personal data stolen and used for identity theft.

Most would agree that people shouldn't put a sign on their front yard or apartment door showing the dates when they'll be away on vacation. However, an increasing number of Canadians are in essence doing just that—and much more—with their Facebook and MySpace accounts. Even as we become more alarmed about the dangers of having our personal data stolen and used for identity theft, many of us are voluntarily posting this same information on the Internet's social networking sites.



Social networking Internet sites, where members post pictures and current information about themselves as a way of keeping in touch and sharing information with “real world” friends, business associates, family and classmates, are a growing phenomenon. Members can also form groups with on-line friends, based on things they have in common such as the school they attended or shared interests. However, these sites are unfortunately making life easier for criminals who practice identity theft and other more traditional crimes.

Let's start with identity theft: a growing threat whereby criminals use personal information to obtain credit and loans in a person's name without their knowledge. The more personal information the fraudster has, the easier it is to impersonate victims and wreak havoc on their finances and credit record. However, some users of Facebook and MySpace routinely place information such as their date of birth, relationship status, locale, workplace and work history or even their address, email and phone number, right in their profile without any restrictions about who sees it.

This not only helps identity thieves, it also allows a potential burglar or stalker to know the whereabouts of a person's home and workplace. And if they've posted an offhand comment about their upcoming weekend in New York, or an on-line friend enthuses about the concert they're both attending tomorrow night, they've just given notice to the whole world about when they're not going to be at home.

Many people's passwords for credit and debit cards or on-line financial services are based on things like their children's or pets' names. These family details are now easily gleaned from many Facebook profiles—either from the information actually posted, or from offhand comments or photo captions on the site. Anyone who has done any banking by phone knows that a common security feature question is the request to give your mother's maiden name. If an individual's extended family appears on their on-line friends list, it's making it a lot easier for criminals to figure this information out. All they have to do is review the profile's friends list and read the comments to determine their relation to each other.

Users of social networking sites will point out that there are options to limit the amount of information that can be seen in your profile by random browsers versus people you have accepted as friends. They're right, and people should definitely be using these options. But, there are two things to bear in mind before becoming too confident about the security features.

Firstly, the most important distinction about on-line friends is that they may not actually know each other in the real world. For example, on its Web site Sophos describes research they conducted with 200 random Facebook members to see how many would accept a "friend" solicitation from a complete stranger, and how readily they would disclose personal information to that person (in this case, a cartoon frog named "Freddi Staur," an anagram for "ID Fraudster").<sup>1</sup> Just under half responded, and in doing so, 87% gave details on their education or employment, 84% provided their date of birth, 78% provided their address or locale, 72% gave a personal email address, 26% divulged their instant-message screen name, and 23% actually gave their current phone number.

People must be wary of a friend solicitation from somebody they don't quite remember but who belongs to a group dedicated to their high school graduation year—it could well be the modern equivalent of the confidence man's "school yearbook scam" whereby a criminal befriends victims by posing as an old schoolmate. Other old scams, such as thieves buying merchandise by mail with fraudulent payment methods, are given new life when more individuals sell through their social networking page.

The second reason not to place too much trust in a social networking site's security features is to remember that large databases full of personal information are very attractive to hackers, since ID thieves will pay for that data. If the world's largest financial institutions and retailers with sophisticated computer encryption can lose data this way, why should on-line social networking sites be immune to data security breaches or hacking?

One of the recurring themes in our work as forensic accountants is the need to persuade both companies and individuals that their personal data should be treated as a valuable commodity. Identity thieves certainly treat it that way, which is why they steal it. More people are becoming aware of the need to safeguard personal information such as addresses, phone numbers, birthdates, SINs, credit card bills and debit card receipts.

Thankfully, many people now have the good sense to feel a twinge of anxiety when they're subjected to an unnecessary request for their SIN. We should be developing that same reaction to an unsolicited on-line overture.

What does this mean for you? Don't feel that you have to avoid being part of the social networking phenomenon, but do be careful about what you reveal and with whom you choose to engage with on-line. Facebook and MySpace are designed to be communities of shared interests, but like all communities there are good and bad citizens. We need to stop making the scammer's job so easy.

**David Malamed CA, IFA, CPA (Illinois), CFE** is a forensic partner with Grant Thornton LLP. He can be reached at (416) 360-3382 or [dmalamed@GrantThornton.ca](mailto:dmalamed@GrantThornton.ca).

**Jennifer Fiddian-Green CA, IFA, CFI, CAMS, CMA, CFE** is a forensic partner with Grant Thornton LLP. She can be reached at (416) 360-4957 or [jfiddian-green@GrantThornton.ca](mailto:jfiddian-green@GrantThornton.ca).

---

#### **About Grant Thornton in Canada**

Grant Thornton LLP is a leading Canadian accounting and advisory firm providing audit, tax and advisory services to private and public organizations. Together with the Quebec firm Raymond Chabot Grant Thornton LLP, Grant Thornton has more than 3,100 people in offices across Canada. Grant Thornton LLP is a Canadian member of Grant Thornton International Ltd (Grant Thornton International), whose member and correspondent firms operate in over 100 countries worldwide.

---

#### **About Grant Thornton International Ltd**

Grant Thornton International and the member firms are not a worldwide partnership. Services are delivered by the member firms independently.

---

<sup>1</sup> Sophos, "Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves," Sophos, <http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html> (accessed September 18, 2007)