

Lions Gate Investigations Group

This article and the information contained here-in, is posted for the interest and education of clients of the Lions Gate Investigations Group, as well as others who are frequent users of social networking sites.



Seven Deadly Sins of Social Networking Security

To users of LinkedIn, Facebook, Myspace, Twitter or all of the above: Are you guilty of one of these security oversights?

By [Bill Brenner](#), Senior Editor - June 30, 2009

Admit it: You are currently addicted to social networking. Your drug of choice might be Facebook or Twitter, or maybe Myspace or LinkedIn. Some of you are using all of the above, and using them hard, [even IT security practitioners who know better](#).

While it's impossible to escape every social networking threat out there, there are steps one can take to significantly reduce the risks. [CSO online](#) recently checked in with dozens of IT security professionals (ironically, using more than one social networking platform to do so) to pinpoint seven typical security mistakes people make; and how to avoid them.

1

Over-sharing company activities

This is a sin of pride, when someone gets excited about something their company is working on and simply must tell everyone about it. Maybe you work for a drug company that is on the verge of developing the cure for cancer. Maybe the company is developing a new car that runs on curbside trash -- in other words, something everyone will want. (See also: [Intellectual Property Security: Don't Lose Your Head](#))

By sharing too much about your employer's intellectual property, you threaten to put it out of business by tipping off a competitor who could then find a way to duplicate the effort or find a way to spoil what they can't have by hiring a hacker to penetrate the network or by [sneaking a spy into the building](#).

Then there are hackers controlling [legions of botnets](#) that could be programmed to scour a company's defenses and, upon finding a weakness, exploit it to access data on the intellectual property. With the data in hand, the hacker can then sell what they have to the highest bidder, which just might be your biggest competitor.

"Sharing this kind of information could lead to targeted attacks on specific technology-producing enterprises," says Souheil Mouhammad, a senior security expert at Altran Technologies.

This sin has sparked a debate in the security industry about whether companies need to revise their employee computer use policies with more specific language on what is/isn't allowed in the social networking arena (see also: [Debate: Does Social Networking Require User Policy Changes?](#)).

To reign in the urge to share too much, it might be useful to repeat this saying, which has started to appear in the public domain: "[Loose Tweets Sink Fleets](#)."

2

Mixing personal with professional

This sin is closely related to the first, but extends beyond the mere disclosure of company data. This is the case where someone uses a social network for both business and pleasure, most commonly on Facebook, where one's friends include business associates, family members and friends (see also: [Slapped in the Facebook: Social Networking Dangers Exposed](#)).

The problem is that the language and images one shares with friends and family may be entirely inappropriate on the professional side. A prospective employer may choose to skip to the next candidate after seeing pictures of you drunk or showing off a little too much leg at someone's birthday party. In sharing such things, you also stand a good chance of making the company you represent look bad.

"In my view one of the major rules when engaging in social networking is to be aware that your words belong in the public domain," says Paul V. de Souza, chief security engineer at AT&T. "You may be quoted all over the Internet, so make sure to choose your words carefully. Be diplomatic and extremely professional."

In some cases, it's nearly impossible to separate business from the personal on a social networking site. Those who work for media companies, for example, are sometimes required to use all their social networking portals to proliferate content in an effort to boost page views which, in turn, attract potential advertisers. But wherever and whenever possible, security practitioners work to keep each locked in their respective boxes.

"You have to understand very clearly what the objective of your presence on any given social network is. If it is for work, keep it for work only. If it is for personal/fun use, keep it for personal use only," says Benjamin Fellows, a senior IT security and risk consultant at Ernst & Young. "I can't tell you how many times I have been invited to Facebook by a work colleague only to find things on their wall or profile that are definitely not politically correct or are downright offensive. I keep all my work friends in LinkedIn and my personal friends in Facebook. Even then, I am very careful what I say on either site. I guess you could also put this under the heading of know your audience."

3

Engaging in Tweet (or Facebook/LinkedIn/Myspace) rage

For the person who has just been laid off or had their professional integrity called into question online, the urge to fire back with a stream of vitriol can be irresistible. Call this a sin of wrath.

"You don't want to get into a flame war," says John Bruggeman, a Cincinnati-based IT director. "Be mindful of what you say and imagine you are at a party where everyone is listening, including your boss, spouse or future employer."

Scott Hayes, president and CEO of Database-Brothers Inc., agrees, saying, "Posting any content when angry is about as dangerous as sending flaming emails, if not more so. Think twice about clicking 'submit' because the world may be looking at your angry, immature rant for years."

4

Believing he/she who dies with the most connections wins

For some social networkers, it's all about accumulating as many connections as possible. Folks on LinkedIn are notorious for doing this, especially those in such LinkedIn groups as TopLinked and LION. This may seem harmless enough or, at the worst, just annoying. But when the name of the game is quantity over quality, it's easy to link or "friend" a scam artist, terrorist or identity thief.

"Always verify the person who wants to get in contact with you," says Ruud van den Bercken, a security specialist at XS4ALL Internet in the Netherlands. "Do you know him or her? If not, why is the person trying to connect with you? Check if the profile of the other person is secured. If you can't retrieve a list of that person's connections, you have to ask yourself" if you really want to go down that road.

As San Francisco-based network and security architect/engineer Jatinder Thukral puts it: "I'd rather have 50 relevant contacts than 500 unknowns."

5

Password sloth

Another common sin is one of laziness, in this case picking passwords for your social networks that you're least likely to forget. In many cases, that means using the same password for LinkedIn and Facebook that you're using for your online bank account or work machine. If someone with malicious intent figures out the password for one social network, that person can now go and access everything else.

"Using the same password on several sites is like trusting the weakest link in a chain to carry the same weight. Every site has vulnerabilities, plan for them to be exploited," says Daniel Philpott, information security engineer at OnPoint Consulting Inc.

6

Trigger finger (clicking everything, especially on Facebook)

Facebook in particular is notorious as a place where inboxes are stuffed with everything from drink requests to cause requests. For some social networkers, clicking on such requests is as natural as breathing. Unfortunately, the bad guys know this and will send you links that appear to be from legitimate friends. Open the link and you're inviting a piece of malware to infect your machine. Christophe Veltsos, president of Prudent Security, describes this as being "click-happy" and warns, "Don't click unless you're ready to deal with drive-by downloads and zero-day attacks."

7

Endangering yourself and others

All of the above tie into the seventh and perhaps most serious sin, which is that reckless social networking can literally put someone's life in danger. It could be a relative or co-worker. Or it could be yourself.

Security experts advise extreme caution when posting birthday information, too much detail on your spouse and children, etc. Otherwise, they could become the target of an identity thief or even a kidnapper.

At the [CSO Executive Seminar on Data Loss Prevention](#) in Chicago, last month, [Motorola CSO Bill Boni expressed his reservations about using Twitter, calling it a great way to get one's self kidnapped](#). "Don't be a twit," Boni said to those who might feel the need to divulge every detail about their location and what they're doing (see also: [The Final 5 Tweets of Harold Wigginbottom, Tech-Savvy CEO](#)).

The Lions Gate Investigations Group can be contacted by calling 604-684-7753 / 7313 or by emailing Scot Filer at scotfiler@lgig.ca or fredpinnock@lgig.ca .