



## 7 Hazards of Social Networking

By John Sileo

[www.Sileo.com](http://www.Sileo.com)

Most of the risks of social networking fall into one of the following categories, which I call the 7 Hazards of Social Networking:

1. **Impersonation.** Does the social networking account (e.g., Twitter Account) belong to the actual person or company it is representing? For example, if you look at the Twitter account [@johnsileo](#), you will see that my name is used to send business to a gentleman who is also an identity theft speaker. My actual account is [@john\\_sileo](#). Whether this is considered social networking squatting or social networking identity theft, it's impersonation.

2. **Ownership.** Who owns the data on the social networking sites' servers? Do you own what you post on Facebook, what you email through GoogleMail or the financials you backup off-site on someone else's servers? The fact that you don't know should trouble you as much as it does me.

3. **Breach.** How is your social networking site protecting your profile and posting data? Are they susceptible to bots like [ZombieSmiles](#) that allow hackers into your Facebook profile through Facebook's own client interface? Is it easy for a hacker to post something or appeal to your friends as if the hacker is actually you (account takeover impersonation)?

4. **Fraud.** Social networking is based in relationships of trust. You trust the people you befriend. Unfortunately, some studies suggest that 25% of the users accept friend requests from total strangers. This, along with account takeover impersonation, opens you up to "friend in distress" scams, information gathering and other forms of social networking fraud.

5. **Disclosure.** We are far bolder and far less discretionary with what we share online versus what we share in person. This means we risk giving out information that, given a second thought, we didn't want to. Think of the [New York Times reporters](#) who tweeted about a closed-door meeting where they discussed charging for online content.

6. **Human Error.** Have you ever hit the button on an email that was meant to go to someone else? The same phenomenon happens on social networking sites, but the damage is exponential because of the medium - you might have just sent it to hundreds or thousands of followers or friends. I call this phenomenon [Tweet Breach](#).

7. **Underestimation.** Because social networking started out as a personal application and still has the flavor of being controlled by individuals (as opposed to corporations), we often underestimate the sheer destruction caused by mishandling this tool. I believe that this is what happened to the military. They originally underestimated the data leakage taking place in the social networking sphere and have since, wisely, begun to rethink their strategy.

Until we recognize that anything posted on the internet (especially if social networking is involved) is Public, Permanent and Admissible in court, we will continue to underestimate the hazards of social networking.

**About the author:** John Sileo became America's leading [Identity Theft Speaker & Expert](#) after he lost his business and more than \$300,000 to identity theft and data breach. His clients include the Department of Defense, Pfizer and the FDIC. To further bulletproof yourself and your business, visit John's blog at [Sileo.com](#) and receive a free white-paper: *Privacy Means Profit: Safe Data = Profitable*