

EXPERT ADVICE PROTECTING YOUR IDENTITY FROM SOCIAL NETWORKING SHYSTERS



By Thomas Oscherwitz
E-Commerce Times
10/12/09 4:00 AM PT

In the 1930s, bank robber Willie Sutton was asked why he robbed banks, to which he famously replied, "Because that's where the money is." Increasingly, fraudsters are targeting social networking because they can convert the information disclosed on social networking sites into cash.

Analyst Report: Keys to Successful eCommerce Projects

With practical insight like, "Top 10 Things To Do Before Kicking Off Your Replatforming Project" and "What To Watch Out For: Common Problems With Platforming Projects," [download the complete report today](#) and ensure your eCommerce success.

Social networking sites like [Twitter](#), [Facebook](#) and [LinkedIn](#) have entered the mainstream -- and fraudsters are taking notice. In recent months, Fox News Network, CNN Anchor Rick Sanchez, and even President Obama have suffered high-profile hacks of their Twitter accounts.

Public figures like Bill Gates and Economist Paul Krugman have seen impersonators create Twitter accounts in their name. Identity thieves have taken over Facebook user accounts and used them as launching pads for fraud scams and phishing attacks. And this is only the tip of the iceberg.

The opportunities for impersonators and identity thieves are increasing as social networking sites grow from a diversion for the technorati to a communication platform relied on by hundreds of millions of users. As of August 2009, Facebook had 120 million unique visitors with 250 million active users; Twitter 45 million unique visitors (the number of active Twitter users is unavailable), and LinkedIn over 14 million unique visitors with 46 million active users.

Phishing Buddies

Social networkers face several types of risks. First, social networking users are vulnerable, like all email users, to a wide variety of Internet fraud schemes. While many of us are familiar with emails about Nigerian fraud scams and being asked to help a winner of the UKlottery, newer scams are far more sophisticated. Fraudsters, for example, are targeting consumers through devious phishing attacks where they make requests to a victim using the online alias of the victim's friends.

Of equal concern is the disclosure of biographical information on social networking sites -- such as a hometown or high school alma mater -- that fraudsters can later use to answer verification questions posed by security authentication systems such as those in use by financial institutions.

According to one study by Professor Alessandro Acquisti of Carnegie Mellon, over 60 percent of student Facebook profiles at his university disclosed the user's birthday, hometown, high school, relationship status, and favorite music, books, or movies. In the hands of a fraudster, this information is even better than a credit report.

So, what is a safety-conscious social networker to do?

Telling the World

First, consumers need to understand that the Internet really is a different medium than the offline world and requires a new level of personal security. While one can shred paper documents, an email or "wall post" is not so easily disposable. An email, text message or posting has a greater imprint than a verbal conversation as one's comments can be forwarded in perpetuity.

When disclosing information online, assume that you are also disclosing the content of your message not just to your friends, but to complete strangers (e.g. potential predators). Do you really want a complete stranger to know things about you that only your close friends and family know?

Social networkers should also remember that identity verification on social networking sites is not particularly robust, so people may not be who they say they are, as it's easy to create a fake persona online.

Finally, never forget that one's actions online have implications offline. The personal information you disclose on your Facebook profile could contain the same type of personal information that banks are using to identify you.

ID Survival Tips

Here are a few common sense security practices:

1. **Use privacy settings.** Facebook and other sites have privacy settings that allow users to restrict public access to their personal profile. Use them.
2. **Be suspicious of anyone, even friends, who ask for money over the Internet.** Impersonation of online social networking accounts is a real issue. Fraudsters are getting more sophisticated in their phishing attacks every day. For example, if a friend makes a financial request that is completely out of character, call your friend up and confirm that he or she really is asking you for money.
3. **Keep your street smarts.** If an offer looks too good to be true, it probably is.
4. **Keep your information to yourself.** Don't post sensitive identifying information such as your Social Security number, phone number, date of birth, address, bank or credit card numbers. Fraudsters commonly rely on this information to apply for credit in your name or gain access to accounts.

Also be careful about sharing biographical information online that companies may later use to verify your identity. These facts include the name of your school, hometown or city where you were born, as well as the name of your favorite sports teams, movies, books or pets.

5. **Keep your social networking account protected.** Use rigorous passwords and change them periodically. Even if there is no money attached to your social networking account, it can be used by others to scam your friends.
6. **Monitor your personal information.** Online risks can lead to real-world credit problems. Get your free annual credit report at AnnualCreditReport.com. You can also regularly check your risk for identity theft for free at [My ID Score](http://MyIDScore.com).

Tom Oscherwitz is vice president of government affairs and chief privacy officer for [ID Analytics](http://IDAnalytics.com), a provider of identity intelligence solutions.