Facebook Fraud: Identity Theft through Social Networking

In This Article

- Thieves create fake profiles to impersonate you and target your friends
- Don’t let your guard down even on social networking sites
- Malware tracks your computer use and steal passwords and financial information

Social and professional networking sites have millions of users, all happily sharing details about their lives with friends and contacts. They’re popular for good reason, helping people to connect and keep in touch with a wide variety of people in their lives. But, because of their popularity, identity thieves are turning to these websites as a new tool for identity theft.

Moreover, many privacy experts note that because these websites are built around self-selected networks of friends or colleagues, people using them may be more trusting of communications they receive through the sites—thereby putting themselves at greater risk of getting scammed.

Social Networking Provides a New Venue for Old Frauds

Variations on many well-known email scams have quickly made their way onto networking sites. The sites work hard to identify and prevent misuse of their systems, but phishing scams, malware, and cons for cash have all occurred.

As with other phishing scams, phishing attacks on networking sites also aim to trick individuals into providing sensitive information that can be used to steal their identities. The trick may be delivered through the networking site’s messaging system or through an application designed to look like a harmless quiz, survey, or product giveaway.

Similarly, emails or applications may contain malware: code designed to infect your computer if downloaded, usually with the goal of tracking all of your future activity and giving the thieves access to your IDs and passwords for financial accounts.

Recently, Facebook users have been warned against a clever new con, in which a thief steals one person’s online identity and then sends out a desperate plea for cash to his or her friends. Usually the story goes something like this: “I’m traveling abroad and all of my money and documents have been lost. Please wire me $500 so I can get home.” Concerned and caring friends may be tricked into wiring cash to the scammer, believing they are helping a loved one in need.
**Thieves May Impersonate You to Target Your Friends**

This sort of trusted-friend-based scam may be one of the most disturbing aspects of the intersection between networking sites and identity theft. It’s bad enough that you have to be wary of phishing and malware scams that use these websites to steal your identity in order to rob you. But it may be worse to think that they might steal your identity in order to target your friends.

A thief wanting to impersonate you to trick your friends might do it the “old-fashioned” way by hacking into your account and spamming your network. But, in the same way that some financial identity thieves establish new credit accounts in your name, some social identity thieves may set up whole new profiles impersonating you to gain access to people you know without you finding out about it.

Security experts point out that between social and professional networking sites, many of us have posted more than enough information about our personal and work lives that enterprising identity thieves could easily compile it to create a fake profile that looks authentic to people who know us. If someone were to post a fake profile in your name to a networking site that you don’t actually use, they could build a whole network of your friends, family and coworkers, thereby gaining access to a wealth of information about each of them.

And because people often believe they are sharing the information they post only with people who already know them, they often publish plenty of details that hackers can use to deduce passwords and get around security questions, such as dates and places of birth, parents’ names, details about children or pets, and more.

**Be Proactive to Protect Yourself**

If you use any of the social or professional networking sites, these measures will help you protect yourself—and your friends and colleagues—against identity thefts perpetrated through these websites:

- Review the privacy settings on your accounts to make sure that information you post is only shared with the people you intend to share it with.
- Treat communications received from colleagues or friends on these networks with the same healthy skepticism you apply to other email and phone messages.
- And, just in case one of those quizzes or surveys you may have filled out wasn’t on the up and up, consider an identity protection service like ProtectMyID™, which can help you detect misuse of your personal information and act rapidly to defend yourself.

Copyright 2010, ProtectMyID™. All rights reserved.