Networking sites a honey pot for scammers

The growth of social networking sites such as MySpace, Facebook, Bebo and others has been astronomical. The most popular have gone from obscurity to boasting more than 200 million registered users worldwide in less than five years.

With such ballooning popularity, it is little wonder that scammers are increasingly trying to tap the rich vein of personal information contained on those sites. And many users are all too willing to give it to them.

In late 2008 the ACCC began receiving complaints from social networking site users who had lost thousands of dollars to people they thought were loved ones or friends.

Those friends had freely shared their personal information or had accepted 'friend' requests from other users who they did not know, unwittingly providing scammers with the information they needed to take over their accounts.

Once the scammers had changed the passwords of the legitimate users, they set about sending out messages to the user's contacts saying they had been robbed while on holidays and needed help. Relatives and friends were asked to wire them money to help pay for hotels, flights home and other expenses. The attacks were often timed to coincide with the genuine user going on holidays. Not only did this make the scammer's story more plausible, it also made it less likely the user would be checking their account while away.

With the average Facebook user reported to have around 120 friends, it is easy to see the damage a clever scammer could inflict on a large number of people with access to just a few accounts.

Most of the major networking sites have added extra safety precautions and warnings to their sites in recent years to help prevent such attacks. Yet there is only so much protection the sites themselves can offer to users careless with their personal details.

In 2007 internet security company Sophos set up an identity on a popular networking site, using a picture of a friendly green plastic frog named Freddi Staur (an anagram of 'ID Fraudster') and began sending out random friend requests.

More than a third of those contacted by Freddi accepted his friendship request and happily provided a wide range of personal information, ranging from email addresses, dates of birth, home addresses, phone numbers, employment details, maiden names and, in some cases, complete résumés.

According to Sophos, the information harvested was in many cases more than sufficient for a fraudster to assume that person's profile and, by using their stolen identity, begin defrauding others.

While it is difficult to determine an exact figure, the Australian Federal Police estimate that identity theft costs Australians several billion dollars every year.

Stopping an identity thief once they have your details is incredibly difficult, making prevention the best defence.

The most important way to protect your details on social networking sites is to be careful what you post in the first place. Be aware that even fairly trivial pieces of information, such as where you work or your home phone number, can be harvested and used against you. While a scammer may not find everything they need on your profile, they may be able to find enough scraps of information to allow them to build a convincing profile of you they can use to trick others. Scammers will happily pore over photos and chats between friends, trying to glean useful information from them. Where once they might have rummaged through garbage or unlocked letterboxes for bank statements, today they can gather most of that information using a computer.

Second, choose carefully whom you give access to your profile when accepting friendship requests or modifying privacy settings. If you don't know the user contacting you, and have no way of verifying whether they are a genuine contact, they may be a threat.

Be especially wary of those asking for information about you or seeking to confirm your details.

Social networking sites can be a great way to stay in touch with friends and loved ones. Just take care what you share.