Facebook easily infiltrated, mined for personal info

CBC News

Robots can easily pass as real users on Facebook, allowing them to befriend real humans and mine personal information such as birthdates, addresses and phone numbers, Canadian researchers have found. Such information can be used for malicious purposes such as committing identity theft.

About a hundred Facebook profiles automatically generated by a computer program managed to “befriend” over 3,000 users over eight weeks, reports a University of British Columbia study being presented in December at the Computer Security Applications Conference in Orlando, Fla.

The fake profiles were used to collect personal information from about a million users, including “friends” and “friends-of-friends.”

Matei Ripeanu, an associate professor in electrical and computer engineering at UBC who co-authored the paper, said his team has indications that similar automated networks are already at work on social networks such as Facebook. “They are even for sale in various environments,” he said in an interview.

Ripeanu added that the goal of the study was to understand the measures being taken to prevent that kind of infiltration and how to protect users against such entities. In order to do that, they created a network of 102 socialbots controlled by a “bot master.” The fake Facebook profiles were generated using images and other content, such as links, on the internet. The robots “friended” each other and posted links on their own and their friends’ walls.

However, late last week, after the experiment started getting media attention, Facebook blocked 80 per cent of the socialbot accounts.

Facebook explicitly bans providing “false personal information” and using “automated means” to collect users’ content or information. However, Graham Cluley, a senior technology consultant with the internet security company Sophos, said the study “certainly presents an interesting illustration of just how easy it would be to automate identity theft on Facebook.”