SOCIAL NETWORKING AND THE ILLUSION OF ANONIMITY

FROM SIMPLE ONLINE SOCIALIZATION TO SENSITIVE INFORMATION DISCLOSURE

SABINA DATCU
E-THREATS ANALYSIS AND COMMUNICATION SPECIALIST

PRIVACY EXPERIMENTS SERIES

bitdefender

Table of contents

According to Internet World Stats, people are spending increasingly more time online, with global Internet usage up by more than 390% between 2000 and 2009. Over this period of time, the popularity of social networks amplified as well, as illustrated by this interesting piece of reading.

This study focuses on how easily social network users make new virtual acquaintances by accepting friend requests sent out by perfect strangers, and on what kind of information they disclose to these recent friends.

Methodology

The methodology of this experiment was very simple. First, a social network was chosen. The choice was based on the fact that the network was large enough to make it possible for the "friends" sample to meet the representativeness criterion.

Second, a test-profile was created in order to analyze a so-called "friendship rate" as a function of sex, age and interests. This test-profile was that of a fair-haired woman, aged 21, acting as a very, very naïve interlocutor.

2,000 users were then selected to become the test-profile's friends. These users were randomly chosen in order to cover different aspects: sex (1,000 females, 1,000 males), age (the sample ranged from 17 to 65 years with a mean age of 27.3 years (SD=5.85), interests, jobs.

The data was collected in two steps. The first step included sending a "friendship" request to the 2,000 users and gathering information about how easily they accept an unknown person as their friend, as a function of sex, age, and interests. The time frame for the first part of the experiment was one week (from Monday morning to Sunday evening).

The second step included a short conversation with a number of selected new friends, in order to see what information they would be willing to disclose to an unknown person, after a 2 hour discussion. The persons in this second group were chosen so as to ensure the heterogeneity of the investigated groups.

Results

After a week, the friendship request form proved very successful: out of the 2,000 requests sent by the test-profile, 1,872 were accepted. The "friendship rate" (number of new friends/day) is illustrated in Figure 1.

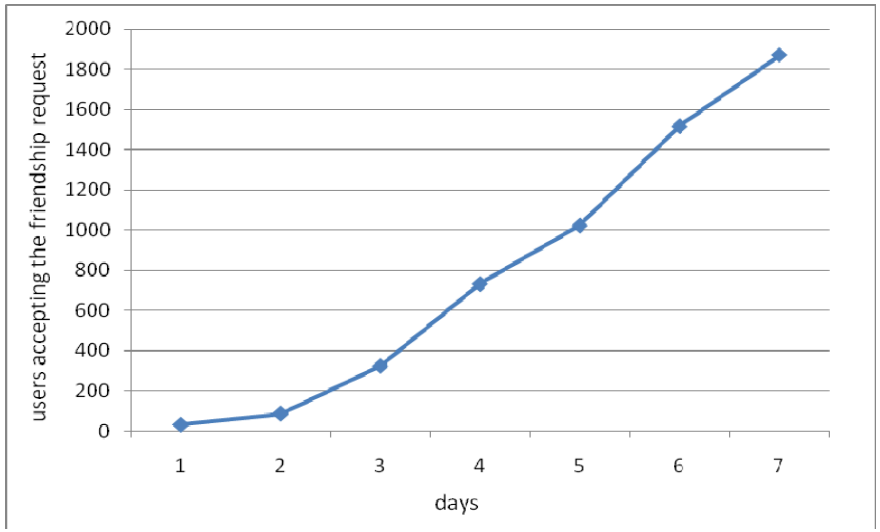

Figure 1: "'Friendship rate" – number of friends/day for the test-profile

The newly acquired friends were from all over the world, and their interests and jobs also covered a wide range of domains. An analysis of these persons' jobs and interests was conducted, in order to understand their behavior. The "IT industry" field was divided into 4 different sub-fields: "IT security", "Entertainment", " Software" and "Hardware". The results of this step are presented in Table 1.

Another investigated aspect was people's reaction to a "friendship request" on the social network, namely whether they are skeptical or whether they accept – without a word – a new unknown friend in their group. Four different "levels of skepticism" were set up:

- ***Level 1:*** very credulous users - they accept the friendship without questions
- ***Level 2:*** credulous users – they accept the friendship after a 1-2 line conversation

- ***Level 3:*** skeptical users - they accept the friendship after a 3-5 line conversation*
- ***Level 4:*** users that don't accept unknown friends

Analysis

A first analysis of the gathered datasets revealed that usually, on a social network, the first impression counts a lot: a very nice looking young woman will always attract a lot of friends. 94% of the 2,000-user experimental sample accepted to become friends with the test-profile.

INDUSTRY		Friends (%)
IT		86
	IT Security – 31	
	Entertainment – 17	
	Software – 16	
	Hardware – 22	
Sales		2
Art		1
Architecture/construction		4
Public organizations		7

Table 1: Friends (%) vs. different jobs/interests

The "level of skepticism" vs. jobs/interests analysis of the "new friends" revealed surprising results: more than 86% of the credulous users who accepted to become the test-profile's friends come from the IT industry, with 31% of them working in IT security. This result was an unexpected one, as almost all IT security companies lay stress on the e-threats associated with social networks.

These outcomes were tested against the motivation of IT security industry users to become friends with the blonde girl, in order to ensure that they didn't accept the friendship request just to have "study material" for their own research.

* Because of the large sample (2,000 users), a conversation longer than 5 lines was considered a time-consuming action, and not a reasonable effort for the co-opting of only one friend. The results showed that when requested by the test-profile (woman, 21) 81% users accepted the friendship without questions.

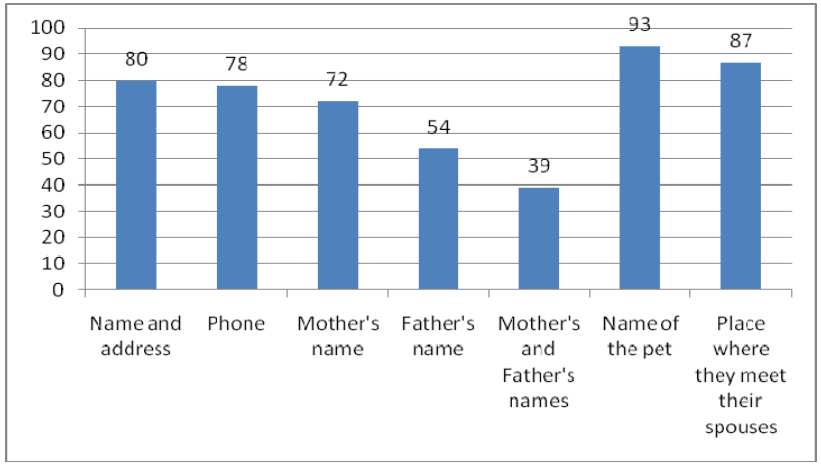

Figure 2: Personal sensitive information disclosed after a half an hour conversation (% from the total interlocutors)

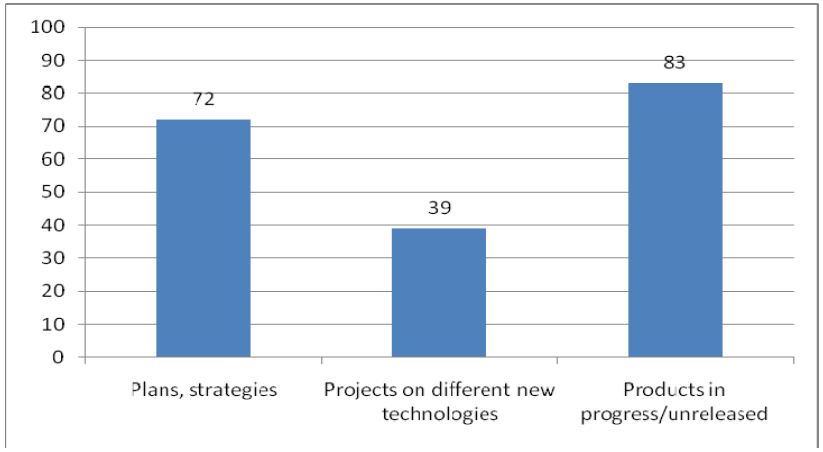

Figure 3: Potential confidential information disclosed after a two hour conversation (% from the total interlocutors)

All these users were asked about their motivation in accepting the girl in their group and here are the answers they provided: it was "a lovely face" (53%), "a known face – but I don't remember the place we've met" (17%), "a person that works in the same industry" (24%), "an interesting profile" (6%).

Further on in the "level of skepticism" analysis, 20 persons that accepted the friendship request were chosen in order to continue the study. These persons were invited to have an individual, real-time, written conversation with the respective young lady using specific software, at the same time.

Some theories, such as 'the social presence theory' and/or 'the social context cues theory', argue that, as social presence decreases, and with an absence of social signs, relationships become less personal and intimate. In contrast, it has been argued that this anonymity allows some people in typing real-time conversations to relate more information than they would in face-to-face relationships (i.e.: Whitty & Gavin, 2000, 2001).

The experiment revealed that the most vulnerable users appeared to be those that worked in the IT industry: after a half an hour conversation, 10% of them disclosed to "the blonde face" personal sensitive information such as: address, phone number, mother's and father's name, etc – information usually used in recovery passwords questions.

In addition to that, after a 2 hour conversation, 73% revealed what appears to be confidential information from their work place, such as future strategies, plans, and unreleased technologies/software.

Conclusion

The results of this study suggest not only that social network users accept unknown persons in their group just based on a nice profile photo, but also that they are willing to reveal personal, sensitive information after a short online conversation. This means that social networks serve both as a meeting ground where people can present themselves and communicate, but also as a starting point for a virtual "friendship", which brings people to divulge too much information because of the illusion of anonymity.

Further readings

Whitty, M., Gavin, J. (2000). *Reality bytes: the suspension of disbelief in the maintenance of online attraction. Narratives for a New Millennium*, Adelaide, 23–27 February.

Whitty, M., Gavin, J. *Age/sex/location: uncovering the social cues in the development of online relationships*, CyberPsychology & Behavior 2001; 4: 623–30.

http://en.wikipedia.org/wiki/Social_presence_theory

http://cmcgroup1.pbworks.com/The-Cuelessness-Model

Nondisclosure statement

No private information from this study will be disclosed or used against the persons that revealed it. No company confidential information will be disclosed or used for personal purposes. The content of the information has not been collected.

bitdefender