A SECOND LIFE IN A VIRTUAL ENVIRONMENT: FROM SIMPLE SOCIALIZATION TO REVEALING SENSITIVE INFORMATION

Bitdefender®

Sabina-Raluca DATCU

Context

- People are spending increasingly more time online (390% from 2000 to 2009.
- The popularity of social networks amplified as well (FB usage increased by more than 115%- 2007 and 2008)
- The Internet provides space for self-exploration and redefinition of identity, may facilitate accepting facets of one's identity that were suppressed or that only manifest online because of the anonymity
- Everybody can confide in everybody and be everybody's friend

Study idea

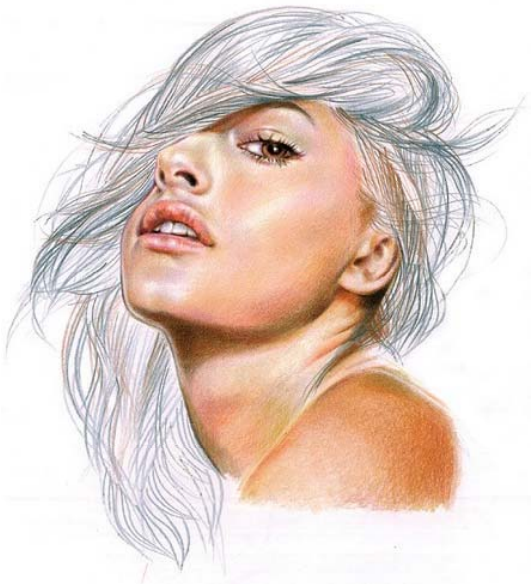
- Part of the “unconventional experiments/studies” series
- Focuses on two specific groups: people working in the IT security industry and hackers
- It observes how easily people make new virtual ‘friends’ by accepting the friend requests of people they don’t know at all, and what kind of information they disclose to these recently made ‘friends’.
- Tries to explain a side of human perception of the virtual world.

Materials and method

- 2 different profiles were created :

  -- a young (25 years) girl, working in IT security industry or as a hacker

  -- profiles were completed by a nice “photo”



… which actually was a drawing…

- A list of 500 Internet users – 250 - IT industry; 250- hackers – was drawn up
- A sub-sample consisting of 50 IT security professionals and of 50 hackers was randomly selected to be interviewed.
- **1st step - get in touch** with the respondents
- **2nd step - a conversation** with these respondents, as 'friends' – in order to see **what information they would be willing to disclose** to an unknown person (apparently interested in the same things as them)
- An analysis of their behaviour by applying the Theory of Planned Behaviour was performed

Results and Discussion

- Both categories (93%, n=100) were, at the beginning, concerned about their personal privacy – more precisely about other individuals viewing their profile, pictures and other information.

- As the conversation continued and trust was gained, this ‘fear’ disappeared in most cases (78%)

1. When socializing on the Internet, **the first impression** counts a lot.
2. **Similar interests** are required in order to start a conversation and to gather the interlocutor's attention.
3. The correlation between the 'level of skepticism' and the job/interests analysis of the respondents revealed that **hackers are more skeptical than the interviewees from the IT security industry**.
4. Time spent chatting with the two categories (percentage of the total time of the experiment dedicated to conversation):

   64% - hackers; 36%-IT security people

- *The study revealed that* ***no matter if working in the IT security industry or as a 'bad guy' (i.e. hacker), everyone can be vulnerable, and can disclose sensitive information to an unknown friend.***

Type of information disclosed

Category of information	IT security people (%)	Hackers (%)
Personal information		
Address	75	69
Phone	84	78
Mother's name	81	77
Father's name	78	92
Where they met their partner	64	35
Info about children	97	94
Other info about their family	63	52

Type of information disclosed

Category of information	IT security people (%)	Hackers (%)
Passwords		
Type of password they are using (letters, numbers, combination, number of characters, etc.)	94	83
Same password for multiple accounts	81	73
Password	13	7

Type of information disclosed

Category of information	IT security people (%)	Hackers (%)
Job/Interests		
Future plans	47	57
Strategies	28	79
Unreleased technology/ software	17	-
Credit card credentials (others')	-	78
Different pieces of software	-	91

- What is more interesting is that, despite the respondents never forgetting the basic tenets of IT security – meaning that they could explain, at any given time, what a strong password looks like or that people should never disclose their mother's maiden name, in practice things are quite different.

- **The power and the influence of friends having the same interests seem to prevail over any knowledge of existing good practices**

Study's Limits

1. Participants were recruited through convenience sampling methods from quite a small pool (500 individuals); this triggers representativity reservations for the two analysed categories, but it does not affect the study's relevance as to human behaviour, in general.
2. Even though the sub-sample was small (50 IT security people; 50 hackers), the sensitive information gained in this experiment can be considered sufficient to draw attention to this topic.
3. It is enough to think that just one person could disclose the credit card credentials of 100 people and then to imagine the results of this action.
4. Because of sample size limitations, in order to describe the interlocutors' behaviour, regression analyses were used instead of more advanced methods such as various mathematical models

Conclusion

- The results of this study suggest not only that people accept unknown people into their group based only on a nice profile and on apparently having the same interests, but
- They are willing to reveal personal, sensitive information to such unknown people in an online conversation.
- -> the Internet serves both as a meeting ground where people can present themselves and communicate,

  but

  also as a space where people develop an artificial idea of anonymity and, therefore, may divulge too much, creating a second, very insecure life for themselves in the virtual environment

THANK YOU!

More “unconventional experiments/studies” on
www.malwarecity.com