



Information Management & Computer Security

Social against social engineering: Concept and development of a Facebook application to raise security and risk awareness

Iwan Gulenko

Article information:

To cite this document:

Iwan Gulenko, (2013), "Social against social engineering", Information Management & Computer Security, Vol. 21 Iss 2 pp. 91 - 101

Permanent link to this document:

<http://dx.doi.org/10.1108/IMCS-09-2012-0053>

Downloaded on: 22 September 2016, At: 04:43 (PT)

References: this document contains references to 21 other documents.

To copy this document: permissions@emeraldinsight.com

The fulltext of this document has been downloaded 1477 times since 2013*

Users who downloaded this article also downloaded:

(2012), "Flying under the radar: social engineering", International Journal of Accounting & Information Management, Vol. 20 Iss 4 pp. 335-347 <http://dx.doi.org/10.1108/18347641211272731>

(2008), "A test of interventions for security threats from social engineering", Information Management & Computer Security, Vol. 16 Iss 5 pp. 463-483 <http://dx.doi.org/10.1108/09685220810920549>

(2014), "Information security: Critical review and future directions for research", Information Management & Computer Security, Vol. 22 Iss 3 pp. 279-308 <http://dx.doi.org/10.1108/IMCS-05-2013-0041>



Access to this document was granted through an Emerald subscription provided by emerald-srm:194764 []

For Authors

If you would like to write for this, or any other Emerald publication, then please use our Emerald for Authors service information about how to choose which publication to write for and submission guidelines are available for all. Please visit www.emeraldinsight.com/authors for more information.

About Emerald www.emeraldinsight.com

Emerald is a global publisher linking research and practice to the benefit of society. The company manages a portfolio of more than 290 journals and over 2,350 books and book series volumes, as well as providing an extensive range of online products and additional customer resources and services.

Emerald is both COUNTER 4 and TRANSFER compliant. The organization is a partner of the Committee on Publication Ethics (COPE) and also works with Portico and the LOCKSS initiative for digital archive preservation.

*Related content and download information correct at time of download.



Social against social engineering

Concept and development of a Facebook application to raise security and risk awareness

Social against
social
engineering

91

Iwan Gulenko

*Department of Information Systems, University of Technology,
Munich, Munich, Germany*

Received 19 September 2012
Accepted 29 January 2013

Abstract

Purpose – This study attempts to develop an efficient concept to mitigate the risks of social engineering in the era of social networks. For instance friend requests on Facebook are often accepted blindly, thus granting unknown people access to profile details. These problems fuel requirements for an application, developed in this study, that raises awareness of security issues in Facebook.

Design/methodology/approach – The “Theory of Planned Behaviour” (TPB), a model from psychology to predict behaviour, is used as a theoretical foundation for the application. Attitudes, perceived behavioural control and social norms are the main variables of this model. Social norms can be massively affected by the Facebook friends and therefore an application is developed which uses this in order to raise awareness.

Findings – The application propagated itself virally. Out of 117 users of the application, 15 took action to change the public-search option visibility from public to private. The use of the application took on average 10.5 minutes.

Originality/value – Applications that scan a Facebook profile for fishy content already exist. However, at the time of writing this paper, no application specifically written against social engineering was known to the author.

Keywords Social networks, Social engineering, Privacy, Psychology, Security, Education, Training, Information security

Paper type Research paper

1. Introduction

The field of research is the phenomenon social engineering in times of the biggest social network “Facebook”. In a few years it gained nearly one billion members (Anonymous, 2011). It is the biggest system within the internet. More than one fifth of the time spent online, people are on Facebook. It is step by step replacing instant messaging and e-mail as means of communication (Meredith, 2010).

Attackers consider social engineering as the most efficient method to reach their goals. According to social engineering is moving to Facebook. Due to this, it became interesting to information security of companies. 43 per cent of 853 polled IT-experts stated, that they became at least once victims of social engineering. 33 per cent of firms having more than 5,000 employees were attacked 50 times or more using social engineering methods during the last two years. 30 per cent of incidents costed more than US\$100,000. Social engineering via Web 2.0 is – after phishing – the most used method of criminals to attack businesses (Dimensional-Research, 2011, pp. 1-5). In literature social networks are described as “a dream come true for social engineers” (Hadnagy, 2010, p. 138). According to other surveys companies are increasingly concerned:



[...] over 72% of firms believe that employees' behaviour on social networking sites could endanger their business's security. This has increased from 66% in the previous study.

It is possible to use the social aspect in order to raise risk and security awareness. The first research question is:

RQ1. How can risk and security awareness of users be raised regarding social engineering through Facebook using the social aspect?

A Facebook application is integral part the research. Thus, the second research question is:

RQ2. What are the effects of a Facebook application regarding risk and security awareness, which includes the social circle?

2. Computer-based social engineering

Social engineering is defined in different ways in literature. The following definition suffices for this paper:

Social Engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation (Mitnick, 2003).

Computer-based social engineering is not defined properly in literature. However, the term is mostly used when social engineering is done with a computer. Phishing and clickjacking can be named as examples. Costs per victim are low (Irani *et al.*, 2011, p. 3). Phishing is a way to acquire data like passwords and credit card details. It is done via a website that looks like the web site of a trustworthy party (e.g. a bank). According to Herkanaidu (2011) phishing is getting more and more sophisticated, since social networks can be used to get individual information.

Clickjacking attacks are based on manipulated websites, where HTML elements had been made invisible and put over other HTML elements. Thus, tricking the user into clicking hidden links. Likejacking is a special case of clickjacking, where users are lured into liking elements on Facebook and consequently spreading spam or scam via their Facebook wall.

Social engineering attacks often work because trust is exploited. This can only happen if trust is built up first. Proper authentication is still rarely seen online.

According to Acquisti and Gross (2006) users are not aware how privacy settings have to be set and which entities on Facebook are visible to whom: "[...] we find significant misconceptions among some members about the online community's reach and the visibility of their profiles". Entities on Facebook are becoming increasingly visible. The privacy setting public-search on Facebook leads to an indexation of profiles in the Facebook directory and search engines. It was activated in November 2009 for all profiles of adults. However, minors cannot activate this option, which should protect them. Bowe (2010) made a torrent file consisting of 171 million datasets of users from the Facebook directory. At that time Facebook had 500 million users. Thus, about $171/500 \approx 34$ per cent user profiles could be extracted. It is clear that 171 million public profiles can be abused by social engineers in various ways.

3. Social networks against social engineering

The strength of Facebook, the social circle, should be used to mitigate its weaknesses. According to the social media expert Christian Funk from Kaspersky, Facebook is actively working on the security of it is users. However, third-parties develop so-called

Facebook security applications. ReclaimPrivacy.org (<http://reclaimprivacy.org>) offers a Javascript code that can be pasted into the address bar. The code adjusts the privacy settings automatically. Javascript in general is dependent on the browser and if Facebook changes their HTML code, than the application has to change, too. Thus, our application should be programmed in a different way.

Applications, which scan the Facebook wall for malicious content, use the Facebook Graph API. Norton Safe Web (<http://safeweb.norton.com/>) has 873,000 users and Defensio (www.defensio.com/) has 5,000 users. The application that is going to be developed should get the permissions gradually like Norton Safe Web.

3.1 Subjective perception of risks

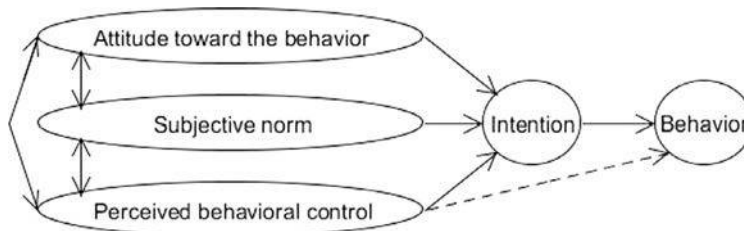
According to Schneier (2008) it is useless to ask, whether a certain measurement is effective against a threat or not. Yet, it is useful to ask whether a certain trade-off is appropriate. Schneier (2008, p. 2) draws an analogy to a rabbit, who eats and then sees a fox. The rabbit has to do a trade-off, whether to run away or to keep on eating. If the rabbit runs away too often he will starve, if he keeps on eating too long, he will be eaten. The rabbits survive, which can do this security trade-offs successfully on a long-term basis. Schneier (2008, p. 4) presents different biases for the perception of risks:

- *Optimism bias.* Humans tend to think that they will perform better in a certain behaviour than average people (Schneier, 2008, p. 11).
- *Control bias.* People are less afraid, when they assume they are in control of the situation (going by car), and more afraid when they think, they have no control over them (going by airplane) (Schneier, 2008, p. 12).
- *Social bias.* When see others in danger, our risk awareness goes up. Schneier (2008, p. 12) cites Gilbert (2006): “We are social mammals whose brains are highly specialized for thinking about others [. . .] We think about people and their intentions; talk about them; look for and remember them”.

Consequently, the application shall raise risk awareness through the correct perception of risks. However, perception is not enough. A certain behaviour has to be induced. For this purpose the “theory of planned behaviour”, a state-of-the-art model from psychology, is used.

3.2 Theory of planned behaviour

The “theory of planned behaviour” (TPB) is a model from psychology to predict behaviour. The TPB is shown in Figure 1:



Source: Adapted from Ajzen (1991, p. 182)

Figure 1.
Theory of planned
behaviour

- *Attitude toward the behavior.* Attitudes describe all motivating factors, e.g. how much effort a person is willing to put in, in order to perform a certain behaviour. According to Acquisti and Gross (2006) the influence from this predictor can be low. A Facebook user can be willing to protect his privacy but at the same time participate actively in social networks, where his privacy may be constantly endangered.
- *Subjective norm.* A person aligns his behaviour to the behaviour of the social circle. According to this bias, a person will behave in a more aware way if the social circle behaves in such a way.
- *Perceived behavioral control.* This predictor tells how much control the person thinks he has regarding a certain behaviour.

The TPB was applied widely; it was to find out how “Littering” can be reduced. Littering describes the behaviour of throwing away trash on the street, etc. Mattarelli (2007) claims that the TPB was very helpful to describe why people litter and how to reduce it.

Littering is similar to security aware behaviour. Both indicate to which degree a person is aware of actions that he does alongside to his daily issues. Therefore, the TPB and the biases, which we described before, can be used to answer the first research question:

Optimism-, Social-, Control-Biases and the three predictors of TPB can be used to fuel requirements towards a Facebook application.

4. Development of the Facebook security awareness application

In order to put the theory into practice our Facebook application is developed (Schermann *et al.*, 2009). Its aim is to help users to find out whether their Facebook profiles are secure and how their friends are doing regarding security and privacy.

Six requirements are formulated as follows (Table I):

- *No 1.* The public-search option in Facebook shall be disabled.
- *No 2.* Clickjacking is rarely noticed by users, thus the application shall notice this and inform the user.

Req. no.	Bias	Reason for bias	TPB	Reason for TPB predictors
1	Social bias	The app checks, whether friends set the public-search option	pbc	Knowledge how to change it
2	Optimism bias	It is expected that this will not happen to oneself	atb	If clickjacking happend, at-titude towards clicking on links may change
3	Social bias	It is perceived, what search engines know	sn	Users perceive, what can be found about friends via search engines
4	Optimism bias	Same as req. no. 2	atb	If double friends are found, attitudes towards accepting friend requests from strangers may change
5	Control bias	User perceive how much control exists over visibility of the entities	pbc	Knowledge rises
6	Control bias	Same as req. no. 5	pbc	Same as req. no. 5

Notes: atb – attitude toward the behavior; pbc – perceived behavioral control; sn – subjective norm

Table I.

The most important predictor of TPB and most important perception bias, deduced from questionnaire and interviews with users

- *No 3.* Most people do not know how much data is available about them. Common search engines shall be used to find out information about the user.
- *No 4.* Double names in the list of friends shall be checked, because they imply identity theft.
- *No 5.* “Social network squatting” is simplified, if the friend list is visible. This visibility shall be checked.
- *No 6.* The user shall be noticed which entities of his profile are visible, since most users do not know this is the case.

4.1 Design

The most difficult requirement was Nr.1, to check the public-search option, since Facebook’s API does not allow any access on this information. After a lot trial and error with screen scraping, it was concluded that the state of the public-search option can be checked via the redirection URL. The following code was used:

// Code:

```
If (uri.equals(https://www.facebook.com)
    return true; // case #1: public-search off
if (uri.contains("profile"))
    return true; // case #2: public-search off
else
    return false; // case #2: public-search on (default)
```

⇒ Req. No. 1 is feasible.

The following list covers requirements 2-6:

- “Likes” of a profile can be accessed via the Facebook API. Likes can be web sites and internal Facebook web sites; they are called “pages”. Mostly liked objects are Facebook pages. They start with <http://facebook.com> and “Like”-objects that are not starting with <http://facebook.com> are classified as external sites, thus may be potential clickjacking sites ⇒ No. 2 is feasible.
- Person search engines can be launched with the name of the user to make automatic research possible ⇒ No. 3 is feasible.
- List of friends can be accessed (for the user, but for the friends of the user) via the Facebook API ⇒ No. 4 is feasible.
- Screen scraping would make it possible to check visibility of entities. However, this is against the Facebook terms and conditions ⇒ No. 5 and No. 6 is not feasible.

4.2 Implementation

The application is written in Java and runs on “Google App Engine”. This “Platform as a Service” approach is used to build dynamic web applications and is less time-consuming than building the classical “LAMP”-Stack (Linux, Apache, MySQL, PHP). Applications on “Google App Engine” are highly scalable. “RestFB” (<http://restfb.com/>) is an interface written in Java in order to connect to Facebook’s graph API that enables the developer to access entities of a Facebook user via Java.

“Google custom search API” (<http://code.google.com/apis/customsearch/>) is used to access the Google search.

The application is loaded into the Facebook application directory with the following description (Table II):

- Facebook privacy: check public-search setting of you and your friends.
- Detect clickjacking: check whether you or your friends became victims of click-jacking.
- Use search engines: check what Google and “people search engines” know about you and your friends.
- Identity theft: check whether you have “double” friends in your friend list.
- Help your friends: post helpful tutorials on their wall.

4.3 Deployment

After tests with friends and family, the application was deployed. Figures 2-5 show screenshots of the application. (A) are links to search engines that are called with the name of the user. At (B) first hits of a Google search are listed. A smiley left to (A) is displayed, if the public-search is off and a question mark is displayed, if public-search is on (default setting is unchanged). (C) shows “Like” objects of the user. If a “Like” object is not pointing to a page it is marked as “spam?”. In (D) one can see that the list of friends is checked for double friends. When clicking on (E), the user can see his profile in the same way others see his profile.

In Figure 5 a screenshot is shown, where every friend is depicted within a box and one friend (see (F)) is victim of a clickjacking attack. Thomson and von Solms (1998, p. 1) inspired us to add a “praise” and “inform” button, because if a person’s behaviour is correct, then they should be praised and if their behaviour is not correct, then they are notified. This is realized through the either the possibility of posting a warning, a tutorial to fix the issue or praise directly posted to the wall of the user.

4.4 Evaluation

Among 117 users, 72 have not changed the default settings of public-search. The results of Gross and Acquisti (2005) are verified: only a minority changed their privacy settings. One reason for this is that the privacy settings are considered to be inconsistent and people did not understand how to change them. Another reason may

Description	User checks, whether his profile has any problems, he did not know about
Actor	Facebook user
Pre-condition	Installation of “Can You Be Googled?” Facebook-application
Post-condition	Facebook profile free from unwanted external “Likes”, Facebook profile free from unwanted external “Likes”, public-search is set consciously. Search engine results were checked. There are no doubles in the list of friends
Process	Friends are warned, where necessary
Alternative process	Google custom API Key is used to get results from Google about friends and show it within the application
Quality requirements	Only “Likes” that are not hosted on the facebook.com domain can be classified as spam. The request of the application should not take more than 15 seconds. Due to the asynchronous API calls it is possible that not every request is successful

Table II.
Use-case for Facebook application <https://apps.facebook.com/can-you-be-googled/>




Check Account(s) About



 Max MustermannEins

Google, Google faces, 123people.de, yasni.de, wink.com, isearch.com

Google Hits:
Uncaught TypeError (JsonStore)
▶ more Hits...

▶ Profile with 7 Likes

 No double friends found in your friendlist (Identity theft).
This is how your profile looks to most people on Facebook. Show

1. Deactivate "public Search" in Facebook: A -smile next to your name means, that you have opted-out of facebook's search engines feature. If there is a -smile next to your name your profile can be found through search engines. Unless you need to be found in Google you should **disable this option:**



(Due to the forced activation of public search in Nov. 2009 it was possible to collect 170 Million Facebook Accounts. This was NOT a technical error by facebook, it's a change in thinking about privacy. This application wants to make you aware of this.)

2. Help your friends:

1. If there is a "inform" button next to their name, they did not adjusted "public search" in Facebook.

Get Permissions to post on Wall and inform your friends

2. Check whether they became a clickjacking victim. Clickjacking is a malicious technique of tricking Web users into revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. A vulnerability across a variety of browsers and platforms, a clickjacking takes the form of embedded code or script that can execute without the user's knowledge, such as clicking on a button that appears to perform another function.

Get Permissions to check Likes (regarding malicious Clickjacking links) of your friends.

3. If there is embarrassing or funny information in person search engines, which does not belong there.

Social against
social
engineering

97

Figure 2.
User profile, first Google hits and likes of the user

Figure 3.
Get permissions from the Facebook platform in order to post on walls

be that the settings were not changed consciously, e.g. a user, who wants to be found through search engines should would let public-search unchanged.

56 users started the application only once, thus it remains unknown, whether they changed any privacy-settings. 26 had the public-search already off, which means that they must have changed it before launching the application. The most important metric is the row named "public-search changed" in Table III. It measures, if the application had been started, the settings were changed and the application was restarted again to check the smile. The "chain of action" of these 15 successfully treated users is depicted in Table IV.

It is possible that more than 15 people changed their privacy-settings, since changes except for the public-search option changes cannot be observed: it is technically impossible to check Facebook privacy settings via the Graph API. The users, who did not change their settings, saw at least how it can be done, if they need it in the future. Awareness is, according to Schneier (2008, p. 4), an important milestone: "We are more afraid of risks that we are more aware of and less afraid of risks that we are less aware of". If people are aware of the risk, if they are more afraid, they are more likely to act.

The Facebook application is a reusable solution to raise awareness among users. The treatment is cheap and highly scalable. It can help Facebook users to set their privacy settings correctly. The second research question can be answered:

The use of the Facebook application to raise risk and security awareness regarding social engineering, which includes the social circle, induced 15 of 72 users (21%) to change the public-search option. It took on average 10.5 minutes.

5. Outlook

A holistic treatment in order to raise risk and security awareness in general must take place. The developed application can be seen as a web-based training. Offensive awareness campaigns like phishing mails based on data from Facebook, as implemented by Jagatic *et al.* (2007), may be such a holistic treatment.

Besides the latent danger of social engineering through third-parties, the misuse through Facebook itself should not be underestimated. No one knows, to what it leads, when so much personal data is in the hands of one enterprise. On the one hand governments, companies and mass media have to make some effort to educate people about proper behaviour, on the other hand people have to understand that they are the ones, who have to act:

However, many words you read, however many you speak, what good will they do you if you do not act on upon them? (Siddhartha Gautama, 563-483 BC).

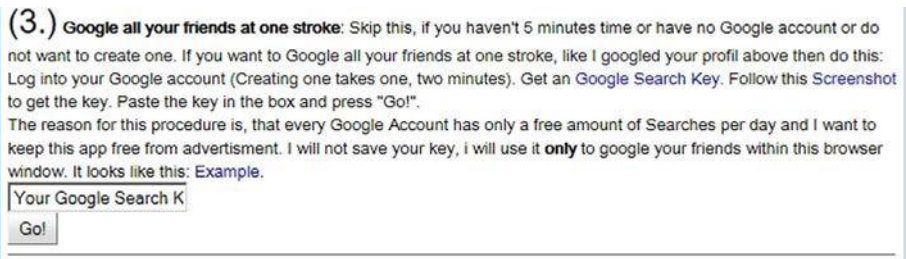


Figure 4.
Google Custom API Key
can be used to get search
results about friends

The call may take 5 minutes, sine 4 things must be checked for every friend: 1. public disabled? 2. Get all likes 3. Is there spam? and if applicable 4. google search.

Expand/fold all Likes

Use ctrl+f to search for delicate words.

7 / 10 (70%) of my friends have a ? -smile. So they can be found on Google. They did not adjusted their facebook profile properly. With <https://can-you-be-googeld.appspot.com>, developed by TU Munich, you can check wheather you can find your facebook profile / the facebook profile of your friends in search engines. Just Google your name and see it for yourself what the web knows about you.

Post on my Wall

The screenshot displays a Facebook interface with several friend profile cards. Each card shows a name, a profile picture (or a placeholder), a status, and search results from various engines. Some profiles have 'inform' buttons, while others have 'praise' buttons. One profile, 'Nie Denechtenamen', has a dropdown menu showing 'Profile with 13 Likes, 1 x Spam?' and a list of search results for 'Barack Obama' and 'Verrückter LKW Fahrer'.

Note: One friend is a clickjacking victim

Figure 5.
Information about friends
is displayed

Metrics	Numbers
Total users	117
Public-search on (default)	72
Public-search off (already changed it)	26
Started application only once	56
Public-search changed	15

Note: Most important metric is the last row

Table III.
Results of the
measurement of the
"Can You Be Googled?"
Facebook application

IMCS
21,2

100

No	Process of starting application	Instant change	Sum of mins
1	False, true, 1.9 days, true, 5.03 days, true, 2,62 minutes		
2	False, true, 7.6 minutes, true, 19.56 days	✓	7.6
3	False, true, 19.37 minutes, true, 4.02 hours	✓	19.37
4	False, true, 29.42 minutes	✓	29.42
5	False, true, 11.6 minutes	✓	11.6
6	False, false, 58.0 seconds, true, 8.84 days		
7	False, false, 2.13 minutes, true, 10.85 minutes, true, 1.35 minutes	✓	12.98
8	False, true, 5.77 minutes	✓	5.77
9	False, true, 13.12 minutes	✓	13.12
10	False, false, 19.0 seconds, true, 7.57 minutes	✓	7.886..7
11	False, true, 1.67 minutes, true, 1.95 minutes, true, 3.1 minutes, true, 14.07 minutes, true, 46.0 seconds, true, 6.57 minutes, true, 44.0 seconds, true, 2.7 minutes, true, 1.17 hours, true, 1.4 minutes	✓	1.67
12	False, true, 51.0 seconds	✓	0.85
13	False, true, 2,94 days		
14	False, false, 2,05 minutes, true, 6.72 minutes, true, 0.0 seconds	✓	8.77
15	False, false, 18.0 seconds, false, 6.05 minutes, true, 1.18 minutes, true, 72.94 days, true, 0.0 seconds, true, 5.75 days, true, 0.0 seconds, true, 0.0 seconds	✓	7.53
	Mean		10.54
	Standard deviation		7.48

Table IV.
Users, who changed public-search option and thus performed a security aware action

Notes: False – “public-search off”; true – “public-search on” the time indicates the duration between two consecutive executions of the application

References

- Acquisti, R. and Gross, R. (2006), “Imagined communities: awareness, information sharing, and privacy on the facebook”, *6th Workshop on Privacy Enhancing Technologies*, pp. 36-58.
- Ajzen, I. (1991), “The theory of planned behavior”, *Organizational Behavior and Human Decision Processes*, available at: <http://econpapers.repec.org/RePEc:eee:jobhdp:v:50:y:1991:i:2:p:179-211>
- Anonymous (2011), *Facebook.com – Statistics*, available at: www.facebook.com/press/info.php?statistics (accessed 13 May 2011).
- Bowe, R. (2010), “Return of the Facebook snatchers”, available at: www.skullsecurity.org/blog/2010/return-of-the-facebook-snatchers (accessed 8 June 2011).
- Dimensional-Research (2011), “The risk of social engineering on information security: a survey of it professionals”, Technical Report, Dimensional-Research, Long Beach, CA.
- Gilbert, D. (2006), “If only gay sex caused global warming”, available at: www.commondreams.org/views06/0702-26.htm (accessed 10 October 2011).
- Gross, R. and Acquisti, A. (2005), “Information revelation and privacy in online social networks (the Facebook case)”, *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, available at: www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf

-
- Hadnagy, C. (2010), *Social Engineering: The Art of Human Hacking*, 1 Auflage, Wiley, Hoboken, NJ.
- Herkanaidu, R. (2011), "The rise of targeted attacks", available at: [www.securelist.com/en/blog/514/The rise of targeted attacks](http://www.securelist.com/en/blog/514/The_rise_of_targeted_attacks) (accessed 14 June 2011).
- Irani, D., Balduzzi, M., Balzarotti, D., Kirida, E. and Pu, C. (2011), "Reverse social engineering attacks in online social networks", *Proceedings of the 8th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, Springer, Berlin, DIMVA'11, available at: <http://dl.acm.org/citation.cfm?id=2026647.2026653>
- Jagatic, T.N., Johnson, N.A., Jakobsson, M. and Menczer, F. (2007), "Social phishing", *Communications of the ACM*, available at: <http://portal.acm.org/citation.cfm?doid=1290958.1290968>
- Mattarelli, M. (2007), Überprüfung der "Theory of planned behavior", von Ajzen and Fishbein (1977) und deren Erweiterung durch "Rechtfertigungsprozesse" am Beispiel Littering, Ref.: Roland W. Scholz., available at: <http://books.google.com/books?id=ZzAccgAACAAJ>
- Meredith, L. (2010), "Facebook replaces email, instant messaging online", available at: www.livescience.com/6822-facebook-replaces-email-instant-messaging-online.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Livesciencecom+%28LiveScience.com+Science+Headline+Feed%29 (accessed 30 August 2011).
- Mitnick, K.W.L.S. (2003), *The Art of Deception: Controlling the Human Element of Security*, 1 Auflage, Wiley, Hoboken, NJ.
- Schermann, M., Gehlert, A., Pohl, K. and Krcmar, H. (2009), "Justifying design decisions with theory-based design principles", *17th European Conference on Information Systems Information Systems in a Globalized World: Challenges, Ethics and Practices, Verona*, pp. S. 2870-S. 2881.
- Schneier, B. (2008), "The psychology of security", available at: www.schneier.com/essay-155.pdf
- Thomson, M.E. and von Solms, R. (1998), "Information security awareness: educating your users effectively", *Inf. Manag. Comput. Security*, Vol. 6 No. 4, pp. 167-173.

Further reading

- Angwin, J., Raice, S. and Ante, S.E. (2011), "Facebook retreats on privacy", available at: <http://online.wsj.com/articleemail/SB10001424052970204224604577030383745515166-1MyQjAxMTAxMDEwMDExNDYw.html> (accessed 11 December 2011).
- Boshmaf, Y., Muslukhov, I., Beznosov, K. and Ripeanu, M. (2011), *The Socialbot Network: When Bots Socialize for Fame and Money*, ACSAC, Orlando, FL.
- McKeon, M. (2011), "The evolution of privacy on facebook", available at: www.mattmckeeon.com/facebook-privacy/ (accessed 13 May 2011).
- O'Neill, N. (2009), "10 privacy settings every Facebook user should know", available at: www.allfacebook.com/facebook-privacy-2009-02

About the author

Iwan Gulenko holds a Bsc in Information Systems from Technische Universität München and is now studying for an Msc in Computer Science with focus on IT Security. With his Bachelor's thesis he won the second prize in the "IT security conference for the next generation" from Kaspersky Labs. Iwan Gulenko can be contacted at: gulenko@in.tum.de

This article has been cited by:

1. Ryan Heartfield, George Loukas. 2015. A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks. *ACM Computing Surveys* **48**:3, 1-39. [[CrossRef](#)]
2. Rute Abreu, Fatima David, Mena Legcevic, Liliane Segura, Henrique Formigoni, Flavio Mantovani Ethics and fraud in E-banking services 1-6. [[CrossRef](#)]
3. Mr Veniamin Ginodman, Ms. Natalya Obelets, Mr Ram Herkanaidu Iwan Gulenko Department of Information Systems, University of Technology Munich, Munich, Germany . 2014. Improving passwords: influence of emotions on security behaviour. *Information Management & Computer Security* **22**:2, 167-178. [[Abstract](#)] [[Full Text](#)] [[PDF](#)]