Susceptibility to URL-based Internet Attacks: Facebook vs. Email

Zinaida Benenson, Anna Girard, Nadina Hintz and Andreas Luder*
Computer Science Department
University of Erlangen-Nuremberg, 91058 Erlangen, Germany
firstname.secondname@cs.fau.de

***Abstract*—The usage of social networking sites has been steadily increasing in the last decade. Communication via social networks has replaced email as the traditional means of electronic communication in many contexts. Accordingly, many types of Internet fraud also spread to social networks. In this work, we make the first to our knowledge direct comparison of users' susceptibility to attacks that involve clicking on dangerous links in Facebook messages versus in emails. We conducted a between-subjects quasi-experiment with 398 users where the users received links from strangers in a Facebook message or via email. We observed the respective clicking behavior and investigated users' attitudes to URL-based attacks by means of a post-experimental survey. Our results show that the communication medium (Facebook vs. email) leads to significant differences in attack susceptibility. Quite surprisingly, the success rate of email-based attacks is significantly higher.**

I. Introduction

The time people spend on Facebook and other social networking sites and the number of their online friends is increasing. As side effect, a new platform for criminal activity emerged. Almost all social networks have been attacked by some kind of malware [1], and news about recent attacks are not scarce [2], [3]. The most famous example of an attack within Facebook was the Koobface virus [4]. Koobface sent a link referring to a funny video that looked as if sent by a friend. If users clicked on the link, they were asked to update their Adobe Flash Player. In fact, instead of updating Adobe Flash Player the users downloaded a Trojan.

Most attacks involve clicking on a link that is sent via Facebook or via email in some Facebook context. As a result, the users can infect theirs computers with the "drive-by-download" malware that does not need user interaction, or be tricked into actively downloading malware as in Koobface case, or into giving important credentials to the attacker on a phishing website. The "human factor" plays an important role in computer security in general. Relating to this fact, Hong [5] writes: "It doesn't matter how many firewalls, encryption software, certificates or two-factor authentication mechanisms an organization has, if the person behind the keyboard falls for phish." Thus, susceptibility to attacks that require user's interaction is an important research topic [6], [5].

Contribution. We conduct the first to our knowledge direct comparison of users' susceptibility to attacks that involve clicking on dangerous links in Facebook messages versus in emails. We consider the following research questions:

- Do people react differently when they receive a link from an unknown sender via email versus via Facebook? Are there differences in clicking rate or in the number and content of reply messages?
- Do the gender of the sender and of the receiver influence clicking behavior?
- Does an accompanying friend request or the amount of information on sender's Facebook profile influence the clicking behavior of Facebook users?

We conducted a between-subjects quasi-experiment with 398 users where the users received links from strangers in a Facebook message or via email. We observed the respective clicking behavior and investigated users' attitudes to URL-based attacks by means of a post-experimental survey.

Results. We show that the communication medium (Facebook vs. email) leads to significant differences in attack susceptibility. Quite surprisingly, the success rate of email-based attacks is significantly higher. On the other hand, we did not find any gender differences in clicking behavior. Also the amount of information on the sender's Facebook profile does not influence the clicking rate. Although we hoped to find the reasons behind the clicking behavior by means of the post-survey, we discovered that only 17% of the users said that they clicked on the link. As in reality 39% of the users clicked, we could not extract reliable information about clicking behavior from the survey.

Roadmap. This paper is organized as follows. We firstly present related work in Section II. Then research hypotheses are stated (Section III) and study design is outlined (Section IV). We present our main results in Section V and some additional results in Section VI. We then discuss our findings (Section VII), limitations of the study (Section VIII) and conclude in Section IX.

II. Related Work

In 2005 Jagatic et al. [7] conducted an experiment to find out how people react to a phishing message that is sent in social context. They used information about social connections of the study participants out of an online social network and sent an email with the faked sender name of a friend from the social network to the study participants. More than 80% of the 1.731 receivers clicked on the link which directed to a (fake) phishing website. More than 70% entered their personal data on the website. Women more often became victims (77%) than men (65%). Phishing with information obtained from the

*Authors are given in the alphabetical order.

978-1-4799-2736-4/14/$31.00 ©2014 IEEE

social network turned out to be four times more effective than common phishing.

In 2007, Sophos, an IT security company, sent 200 friend-requests from a fake Facebook account to random people. The goal was to find out how many would respond. 41% of the respondents accepted the friend request from a stranger and thus gave the stranger access to pictures, information about family, hobbies, employment and many other sensitive information.

Bilge et al. [8] wanted to find out how people behave if they receive a friend request from fictitious people or from people they are already friends with. They cloned already existing social network profiles and additionally created totally new profiles. From both profiles they sent friend requests to the original friends of the cloned profile. Over 60% of the receivers accepted the request from the cloned profile and around 30% accepted the request from the totally new profile. Furthermore, they sent a message with an individualized link to the friends of the profile that has been cloned. Over 50% of the receivers clicked on the link sent from the cloned profiles and about 50% clicked on the link sent from the totally new profiles.

Stringhini et al. [9] tried to find out how spammers within social networks operate. To this end, they created a large amount of "honey-profiles" on three large social networks. They logged the kind of contacts and messages they received from spammers over one year period and tried to collect data about spamming activity. Out of 3.831 friend requests they received on Facebook during the observation 173 have been from spammers. They received 72.431 messages where 3.882 have been identified as spam. Based on the results, they developed techniques to automatically identify spammers in social networks.

Onarlioglu et al. [6] investigated in an experiment with 164 users how people react to some kinds of Internet attacks, including how well people can distinguish dangerous links from benign ones. They found out that the users mostly try to estimate link trustworthiness using size and complexity of the link as indicators.

As shown above, some research on clicking behavior in social networks and on the Internet have already taken place. Our study differs form the previous work in several important points. As far as we know, this is the first study that compares the clicking behavior of Facebook and email users. Additionally we compared the impact of six different sender profiles with different gender and privacy settings, as well as the clicking behavior of people who did and did not get a friend request.

III. Hypotheses

We derived the following six hypotheses from the research questions in Section I.

H1: People more often click on "suspicious" links in Facebook messages than on "suspicious" links in email messages.

We define a link as *suspicious* if this link could be a part of an attack, for example if the sender of the link is not known, or the link arrived in some suspicious context.

The rationale behind this hypothesis is that email as communication medium is much older than Facebook, and thus people should have more experience with attacks via email. Moreover, users generally trust Facebook [10], [11] and thus may develop a sense of security that leads them to paying less attention to the possibility of attacks.

H2: If a "suspicious" link was received via Facebook, receivers would more often contact the sender than if a "suspicious" link was received via email.

Getting and staying in contact with people is one of Facebook's primary goal (apart from self-presentation). Thus, we suppose that the social norms on Facebook make it easier to contact the sender.

We also formulated two hypotheses concerning specifically the clicking behavior of Facebook users.

H3: Facebook users that received a friend request from the sender of a "suspicious" link would more often click on the link than Facebook users that did not receive a friend request.

We suppose that sending a friend request makes the receiver perceive the unknown sender as more trustworthy, as the sender seems to act as a real person and behaves according to Facebook's social standards.

H4: Facebook users would more often click on the "suspicious" link that is sent from an open Facebook profile than on a link that is sent from a restricted or a closed profile.

The amount of information available on the sender's profile can influence the trust into the sender and thus lead to different clicking behavior. However, this could only be that case if people visit sender's profile *before* they click on the link.

The last two hypotheses are concerned with the connection of the gender of the sender or of the receiver with the clicking behavior. We think that here, the users will exhibit similar behavior on Facebook and via email.

H5: Female users will more often click on the "suspicious" links than male users.

Jagatic et al. [7] found evidence that women are more susceptible to social phishing than men. Although our type of attack is different (especially, it does not use a message from an existing friend), we hypothesize that women will also be more susceptible to our kind of attack.

H6: If a message is sent by a woman, respondents will more often click on the "suspicious" link, compared to a male or a neutral sender.

Neutral sender is a sender with unrecognizable gender. This can only be achieved via email, as on Facebook gender is a mandatory part of a profile. Phishing emails seem to be more successful when sent from female accounts [7], and fake female profiles receive more friend requests on Facebook [12]. Thus we hypothesize that women will have a higher success rate as senders than men.

IV. Design of the Study

To measure the clicking behavior of the users, messages with an individualized link (a link with an unique hash tag at

the end) were sent to the participants. These messages came from different fake senders and had the following content:

> Hey *<receiver's first name>*,
> here are the pictures from the last week:
>
> http://*<IP address>*/photocloud/page.php?h=*<hash tag>*
>
> Please do not share them with people who have not been there :-)
>
> See you next time!
> *<firstname of the sender>*

The link led to a website that only showed "Access denied". With the individualized link we were able to distinguish clicks of different users.

A. Groups of Participants and the Course of the Study

We first consider two groups of participants, the Facebook and the email group, according to the medium through which they receive the message. In order to see the effects of receiver's gender on clicking behavior, the groups are further subdivided into gender groups, see Fig. 1.

For sending email messages we created three fake email accounts at one of the freemail providers: one male and one female with the address of the kind *firstname.secondname@providerdomain* and one and one neutral of the form xkl70@*providerdomain*. Thus, each email gender group is further subdivided into three groups according to the gender of the sender. This constitutes six distinct receiver groups for the email messages. The recruited number of email participants was 158, with 123 male and 35 female participants (see Fig. 2).

The Facebook group is also subdivided into two groups according to the receiver's gender. Furthermore, to measure how the profile of the Facebook sender influences the behavior of the receiver we created six Facebook profiles with different privacy settings and different gender:

1) Open profile (one male, one female): A totally open profile with no privacy restrictions.
2) Restricted profile (one male, one female): Only the profile picture and timeline pictures are visible for the public.
3) Closed profile (one male, one female): A profile with all restrictions set to "private". Only the name and a symbolic male or female profile picture are visible.

Half of the Facebook participants also received a friend request from the sender in order to measure the effect of a friend request on the clicking behavior.

In this way, we have 24 distinct groups of Facebook users. We were able to recruit 240 Facebook participants, 120 males and 120 females, thus each small group on Fig. 1 consisted of 20 users, 10 of them with friend request and the other 10 without friend request.

As shown in Fig. 2, we sent the messages as described above and then measured the reaction of the participants in three ways: the clicking behavior according to the link in our message, reaction via a reply message and the acceptance of the friend request.

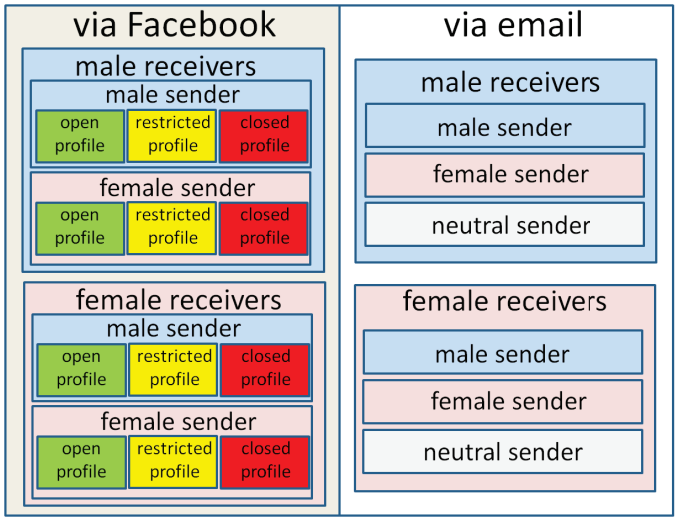

Figure 1. Groups of participants according to the communication medium (Facebook vs. email), gender of the sender and of the receivers, and also openness of the sender's Facebook profile. Each of the small Facebook groups is in addition subdivided into users who received the friend request and users who did not receive the friend request from the sender.

B. Post-Survey

Three weeks after the sending of the link we invited all study participants to take a survey with several questions about their handling of messages from strangers, their perception of Facebook's security and the reasons why they clicked or not clicked on the link in our message. We also asked the usual demographic questions (age, gender and education).

C. Ethical Considerations

Conducting real world fraud experiments always requires some ethical considerations [13], [14]. Our study was permitted by the department of privacy protection since there is no Institutional Review Board at the department of computer science at our university. Because of the permission procedure there is one restriction in study design: We were not allowed to track the users between two study parts, the clicking experiment and the final survey. Thus, although we sent individualized links to the users to click on, we were not allowed to use the same identifiers for distinguishing the survey participants. Thus, we cannot connect the real-world behavior and the survey answers back to an individual user.

After the study, we informed the participants about our experiment and sent to them information about the dangers of clicking on suspicious links as well as a summary of study results.

D. Recruitment of the Participants

We recruited the participants via Facebook in several student groups and via an email to our university's student mailing list to participate in a study with the subject "Online behavior of Facebook users" in order not to prime them to

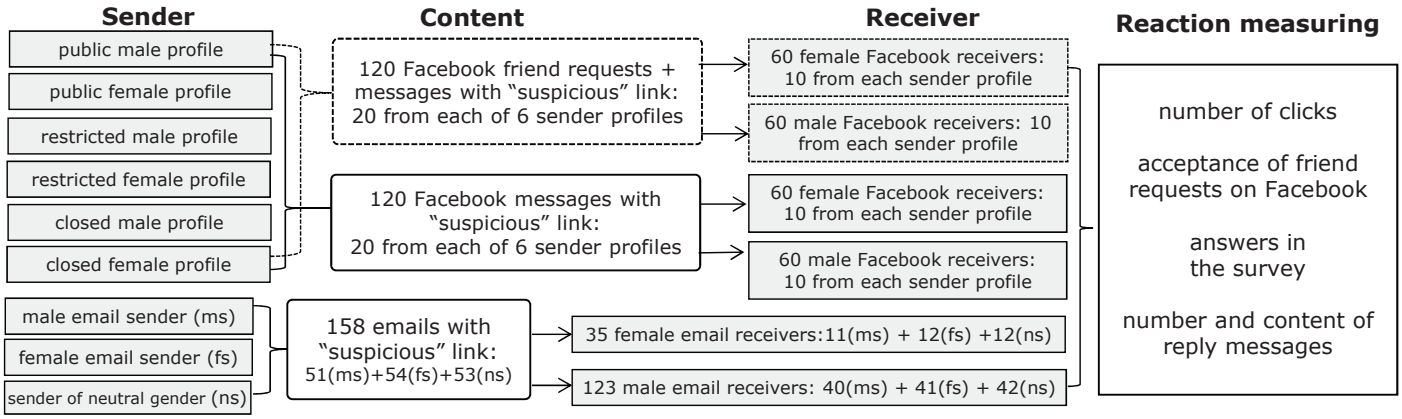

Figure 2. Methodical design of the study: ms, fs and ns mean male, female and neutral sender, respectively.

the real goal of our study. To offer an incentive, we drew ten Amazon vouchers with the value of 10 Euro each.

Participants who signed in via the mailing list received the message via email (158 people). Participants recruited via Facebook (240 people) received the message via Facebook, half of them also received Facebook friend request along with the message, as explained previously.

All Facebook users who wanted to participate in our study had to join our Facebook group named "Facebook user study" because of the following technical reason. Currently there are three different folders in Facebook accounts into which messages can be delivered: "Inbox", "Others" and "Spam". Users are only notified about new messages that are delivered into the Inbox. Furthermore, the users can choose between two settings called "Basic Filtering" which is the default setting and "Strict Filtering" for incoming messages. The allocating algorithm behind these two settings is not known in detail. We found out by experiment that users that chose strict filtering will receive Facebook message from strangers in the Others folder unless they accept our friend request previously. However, if people use basic filtering, a message will reach the Inbox if the receiver and the sender are members of the same Facebook group. In order to make our message as visible to the receivers as possible, we put our sender profiles into the participants group.

V. Hypotheses Testing

As we have categorical data (data classified into one or several distinct groups, e.g. email vs. Facebook), we use the Pearson chi-squared test for hypotheses testing. Minimum requirements are at least 5 observations per group and a total sample size of 107 participants (for df=2, and expected medium effect size of 0.30)[15]. We will report the significance of the tested differences and its importance (effect size). The effect size is reported by using Cramer's V, as the chi square coefficient is only appropriate for 2x2 crosstabs. As we have also 3x2 crosstabs for hypotheses H4 and H6 (see Table I), Cramer's V is the appropriate effect size measure [15], [16]. The analysis was conducted using SPSS [16].

A. Demographic Data

Apart from the gender of the participants that was presented in Section IV, all other data were determined via the post-experimental survey. Out of 398 participants, 339 (85%) completed the survey. The survey participants (163 male, 176 female) reported to be 22 years old on average with standard deviation 4.5. Most of them (96%) are university students. 54% study technical subjects or natural sciences, 14% study economic sciences or law, and the rest studies medicine (2,5%) or some other subject. 95% (323) of respondents have a Facebook account

B. Differences between Facebook and Email

H1: People more often click on "suspicious" links in Facebook messages than on "suspicious" links in email messages.

Hypothesis 1 is not supported because the links were, on the contrary, significantly more often clicked in email messages than in Facebook (56% compared to 38%, see Table I. The difference between the groups is highly significant, although the effect is rather small ($\chi^2(1) = 13.649, p < .01, V < 0.3$). We discuss possible reasons for this behavior in Section VII.

H2: If a "suspicious" link was received via Facebook, receivers would more often contact the sender than if a "suspicious" link was received via email.

This hypothesis is supported ($\chi^2(1) = 20.981, p < .01$), although the effect size is rather small (V¡0.3). Only 18 out of 158 email users sent a reply, whereas 75 out of 240 Facebook users answered to the message.

C. Clicking Behavior on Facebook

H3: Facebook users that received a friend request from the sender of a "suspicious" link would more often click on the link than Facebook users that did not receive a friend request.

The number of clicks between the group with friend request and the one without friend request is almost the same (46 compared to 44). Not surprisingly, there is no statistically significant difference between the two groups ($\chi^2(1) = 0.071, p > .10$). Hence, H3 is not supported.

Table I. RESULTS OF THE HYPOTHESES TESTING.

Hypothesis	Independent variable	Dependent variable	Results: absolute frequency	χ^2	df	p	Cramer's V
H1	communication channel	clicked on link	email: 89/158; FB: 90/240	13.649	1	**.000**	.185
H2	communication channel	contacted sender	email: 18/158; FB: 75/240	20.981	1	**.000**	.230
H3	friend request on FB	clicked on link	no: 44/120; yes: 46/120	.071	1	.790	.017
H4	profile information of the sender on FB	clicked on link	public: 31/80; restricted: 28/80; closed: 31/80	.32	2	.852	.037
H5 email	receiver's gender	clicked on link	female: 19/35; male: 70/123	.076	1	.782	.022
H5 FB	receiver's gender	clicked on link	female: 44/120; male: 46/120	.071	1	.790	.017
H6 email	sender's gender	clicked on link	female: 37/54; male: 25/51; neutral: 27/53	4.994	2	.082	.178
H6 FB	sender's gender	clicked on link	female: 41/120; male: 49/120	1.138	1	.286	.069

"FB" means Facebook. p for significant results is written in **bold**. The interpretation of the row describing H1 is as follows: Hypothesis H1 relates communication channel (Facebook vs. email) to the number of people that clicked on the link. In the email group 89 of 158 users clicked, in the Facebook group 90 of 240 users clicked. The difference between the groups is highly significant with small effect size .185. All other rows can be interpreted analogously.

H4: Facebook users would more often click on the "suspicious" link that is sent from an open Facebook profile than on a link that is sent from a restricted or a closed profile.

H4 is not supported, because there is no significant difference in clicking between the three groups ($\chi^2(2) = 0.320, p > .10$). Thus, 31 Facebook users clicked on the link sent from the public profile, and just as much people clicked in the link sent from the closed sender profile; 28 people clicked on the link from the protected profile. This behavior could indicate that users first clicked on the link and only afterwards viewed the sender's profile.

D. Gender-related Hypotheses

H5: Female users will more often click on the "suspicious" links than male users.

The clicking behavior is independent of receiver's gender. We found no difference between sexes neither in the group of Facebook ($\chi^2(1) = 0.071, p > .10$) nor in the group of email receivers ($\chi^2(1) = 0.076, p > .10$). Therefore, H5 is not supported.

H6: If a message is sent by a woman, respondents will more often click on the "suspicious" link, compared to a male or a neutral sender.

There is no significant difference for email users ($\chi^2(1) = 4.994, p > .05$) as well as for Facebook users ($\chi^2(1) = 1.138, p > .10$). Thus, the hypothesis is not supported.

VI. ADDITIONAL RESULTS

A. Received Reply Messages

Altogether we received 18 reply messages from email receivers, 11 of them complaining that the web site does not work. Interestingly, out of 75 reply messages from Facebook receivers, only 13 people mentioned that they cannot see the pictures. The users asked whether they received the message by mistake, or confessed that they do not exactly remember where they know the sender from.

B. Clicks per Receiver and Response Time

On average, email as well as Facebook users clicked on the link three times. There was a main difference in the response time between email and Facebook users. While 38% of all email recipients clicked on the link within 12 hours after the message has been sent, only 12% of all Facebook participants did this in the same time. Interestingly, Bilge et al. [8] report that about 36% of social network users clicked on the link sent by an unknown sender during this period of time. However, their experiments were not conducted on Facebook.

C. Survey Results

Out of 398 participants, 339 (85%) completed the survey. In the survey, 169 people could remember that they received the message, and from these, 68 people (20% of 339 survey participants) said that they clicked on the link (31 via email and 37 on Facebook). However, in the experiment 179 users (39%) clicked on the link (89 people via email and 90 on Facebook). Thus, only 17% of all 398 users said that they clicked on the link, and the answers of other 15% are not known because they did not take part in the survey. Therefore, we could not extract reliable information about clicking behavior from the survey.

Due to data protection restrictions (see Section IV-C) we were not able to compare actual and reported behavior of concrete individuals. Nevertheless, the study results still give some insight into users' perception of Facebook's security and their reported clicking behavior.

For example, 61% of Facebook users think that spam messages can be sent via Facebook, 31% are not sure about it, and the remaining 8% think it impossible. Only 6% of the users think that Facebook messages are scanned for malware, whereas 35% think that it is not the case, and the rest is unsure. These answers show a high percentage of uncertainty among Facebook users about the security of Facebook messages.

Only 15% of Facebook users reported that they use "Strict Filtering" for receiving their messages, and 13% said that their settings allow friend requests only from friends of friends. We note that we cannot compare the reported settings with the actual ones, and previous research shows that people usually overestimate the privacy of their settings [17], [18].

65% of all survey respondents (220) said that they do not click on Facebook links in messages from unknown senders. Moreover, 67% (228) of all respondents said that they do not click on links in the emails from unknown senders. In the experimental setting, 62% of all Facebook recipients did not click, and 44% of all email receivers did not click on the link.

VII. DISCUSSION

Contrary to our intuition, people seem to exhibit risky link clicking behavior significantly more frequently when using email than on Facebook. Probably the Facebook message with the suspicious link was filtered out at some accounts. On the other hand, as the receivers were addressed by the first

name, the email users probably perceived the message as more trustworthy, because spam and phishing emails usually do not use names. Moreover, the Facebook users had more possibilities to verify that they actually don't know the sender.

Although people contacted the link sender more often on Facebook than via email, we do not know how these contacts influenced the clicking behavior. The fact that there is no difference in clicking behavior for open, restricted and closed profiles may supply some evidence that people actually clicked on the link *before* viewing the sender's profile. The absence of gender differences contradicts some previous findings [7], [6] and needs further investigation.

Small effect size (Cramer's $V < 0.3$) that we found for both our significant results (see Table I) implies that there are also some other factors that influence clicking behavior, for example personality traits or simply the fact that a user went to a party the week before the message with the link came.

VIII. Limitations

The user population in our study is not representative for the Internet or Facebook users. An average German Facebook user was 38.7 years old in 2013 [19]. Most of our participants are university students with average age of 22.

We did not conduct a randomized experiment, but a quasi-experiment with Facebook participants recruited via Facebook and email participants recruited via email. If we wanted to recruit participants only via Facebook, we would need their email addresses. However, according to our prior experience, people are reluctant to give their email addresses on Facebook. Similar problems arise when recruiting solely via email.

We note that our results do not give any insight into more context-aware attacks that simulate, for example, messages coming from a real friend. However, our work gives a lower bound for success probability of URL-based attacks.

IX. Conclusion

In this work we investigated the difference in reaction of Facebook versus email users when they receive a message from a stranger with a possibly dangerous link. We found out that email users click on such a link significantly more often than Facebook users. We also looked into some other factors that may influence clicking behavior, such as the gender of the sender and of the receiver, friend requests and the amount of information available about the sender on Facebook.

We conclude that the long existence of the threat from dangerous links in the emails have not led the users to better awareness. On the other hand, Facebook users seem to be either more aware of the threats, or better protected from attacks by technical means. Also richer social context of Facebook may contribute to better attack detection by Facebook users.

Our study showed that trying to learn the reasons behind users' risky behavior by means of a post-survey questionnaire seems to be very difficult, because the people do not remember that they received the experimental message, and the reported number of clicks is much smaller than the real number of clicks. Improving the reliability of the survey remains an interesting question. On the whole, further investigation of the factors that influence clicking behavior is needed in order to understand how the users can be protected from URL-based attacks.

Acknowledgments. This work was supported by the Bavarian State Ministry of Education, Science and the Arts within the scope of research association ForSEC (www.bayforsec.de).

References

[1] H. Gao, J. Hu, T. Huang, J. Wang, and Y. Chen, "Security issues in online social networks," *Internet Computing, IEEE*, vol. 15, no. 4, pp. 56–63, 2011.

[2] N. Perlroth, *Malware That Drains Your Bank Account Thriving on Facebook*. NY Times: http://bits.blogs.nytimes.com/2013/06/03/malware-that-drains-your-bank-account-thriving-on-facebook, Jun. 2013.

[3] V. Goel, *Malicious Software Poses as Video From a Facebook Friend*. NY Times: http://bits.blogs.nytimes.com/2013/08/26/malicious-software-poses-as-video-from-a-facebook-friend/, Aug. 2013.

[4] Kasperski, *Kaspersky Lab Detects New Worms Attacking MySpace and Facebook*. www.kaspersky.com/news?id=207575670, 2008.

[5] J. Hong, *The State of Phishing Attacks*. Commun. ACM, 55(1):74-81, 2012.

[6] K. Onarlioglu, U. O. Yilmaz, D. Balzarotti, and E. Kirda, "Insights into user behavior in dealing with internet attacks," in *NDSS, 19th Annual Network and Distributed System Security Symposium*, 2012.

[7] T. Jagatic, N. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," in *Commun ACM, 50 (10):94-100*, 2005.

[8] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All your contacts are belong to us: Automated identity theft attacks on social networks," in *18th international conference on World wide web*, 2009.

[9] G. Stringhini, C. Kruegel, and G. Vigna, "Detecting spammers on social networks," in *26th Annual Computer Security Applications Conference*, 2010.

[10] C. Dwyer, S. R. Hiltz, and K. Passerini, "Trust and privacy concern within social networking sites: A comparison of facebook and MySpace," *Americas Conference on Information Systems*, 2007.

[11] J. Fogel and E. Nehmad, "Internet social network communities: Risk taking, trust, and privacy concerns," *Computers in Human Behavior*, vol. 25, no. 1, pp. 153–160, 2009.

[12] D. Irani, M. Balsuzzi, D. Balzarotti, E. Kirda, and C. Pu, "Reverse social engineering attacks in online social networks," in *Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA)*, 2011.

[13] M. Jakobsson and J. Ratkiewicz, *Designing Ethical Phishing Experiments: A study of (ROT13) rOnl query features*. 15th international conference on World Wide Web, 2006.

[14] M. Jakobsson, N. Johnson, and P. Finn, *Why and How to Perform Fraud Experiments*. IEEE, 2008.

[15] J. Bortz and C. Schuster, *Statistik für Human- und Sozialwissenschaftler.* Berlin, Heidelberg: Springer, 2010.

[16] J. Janssen and W. Laatz, *Statistische Datenanalyse mit SPSS. Eine anwendungsorientierte Einfhrung in das Basissystem und das Modul Exakte Tests*. Berlin, Heidelberg: Springer, 2010.

[17] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove, "Analyzing Facebook privacy settings: User expectations vs. reality," in *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*. ACM, 2011, pp. 61–70.

[18] M. Madejski, M. Johnson, and S. M. Bellovin, "A study of privacy settings errors in an online social network," in *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on*. IEEE, 2012, pp. 340–345.

[19] "Soziale Netzwerke vergreisen." http://heise.de/-1828958 (in German), 2013.