FACEBOOK PRIVACY HARDENING USING VIRAL TECHNIQUES

Iwan Gulenko

Technical University of Munich, Munich, Germany, iwang@fastmail.net

Follow this and additional works at: http://aisel.aisnet.org/ecis2014
FACEBOOK PRIVACY HARDENING USING VIRAL TECHNIQUES

Research in Progress

Gulenko, Iwan, Technical University of Munich, Munich, Germany, gulenko@in.tum.de

Abstract

The 'Theory of Planned Behaviour' (TPB), a model from psychology to predict behaviour, is used as a theoretical foundation for an application that uses public available information of friends on Facebook to analyse their status of their privacy settings. Also one can check public-search settings of friends, check if friends became victims of clickjacking. Moreover, one can help Facebook friends by posting a short tutorials on their wall about how they can improve their privacy settings. The application propagated itself virally. Among over a hundred Facebook users, one tenth changed public-search option, if it wasn’t changed already. This research in progress suggests that scholars and practitioners make use of viral techniques to propagate security education.

Keywords: Security training, education, Facebook.
1 Introduction

According to Fossi (2011) social engineering is moving to Facebook. Due to this, it became interesting to information security of companies. 43% of 853 polled IT-experts stated, that they became at least once victims of social engineering. 33% of firms having more than 5000 employees were attacked 50 times or more using social engineering methods during the last two years. 30% of incidents costed more than 100.000 US Dollar. Social engineering via Web 2.0 is — after phishing — the most used method of criminals to attack businesses. Social networks are described as 'a dream come true for social engineers' (Hadnagy 2010).

The privacy setting “public-search” on Facebook can lead to an indexation of profiles in the Facebook directory and search engines if it is not disabled. It was activated in November 2009 for all profiles of adults. However, minors cannot activate this option – this is how Facebook tries to protect them. Security experts showed how users, who did not deactivate the ‘public search’ option, could be attacked: A torrent file has been made consisting of 171 million datasets of users from the Facebook directory (Bowe 2010). At that time Facebook had 500 million users. Thus 170/500 = 0.34 % of users could be extracted. Those data can be used by social engineers in various ways (e.g., cracking passwords through combining names and birthdays, harvesting personal information from the profiles). To mitigate these issues, we use the strength of social networks to prevent social engineering from happening. We use a viral approach to persuade users to change their Facebook privacy settings.

The remainder of the paper is organized as follows. First, we give a brief overview of the ‘Theory of Planned Behaviour’ (TPB) followed by the description of the viral Facebook application that implements one of the theories’ core concepts. Finally, we evaluate and conclude the results.

2 Theory of Planned Behaviour

The ‘Theory of Planned Behaviour’ (TPB) is a model from psychology to predict behaviour. We first describe the theory and then argue why we think it is the most suitable one.

As depicted in figure 1, the TPB consists of three main constructs: attitude, subjective / social norm and behavioural control. Attitude toward the behaviour describes all motivating factors, e.g., how much a person tries to perform a certain behaviour. 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 is about how much a person aligns his behaviour to the behaviour of the social circle. Perceived behavioural control predicts how much control a person thinks having.

The TPB fits to model why people on Facebook can be nudged to adjust their privacy settings when exposed to (bad or good) privacy settings of their friends because of the ‘social norm’ construct. Other theories in IS also have that component but are either solely focused on that (e.g., Social exchange theory, Social learning theory, Social network theory) or omit the social components (e.g., Diffusion of innovations theory, Technology acceptance model). We choose the TPB as the theory that is the simplest available and still having a social component.
3 Development of Facebook application

We find that Facebook applications exist that help users to adjust their privacy settings (e.g., reclaimprivacy.org, safeweb.norton.com, defensio.com). However, none of them uses the profiles of the friends as a data source. We formulate requirements towards a Facebook application that scans profiles of friends for privacy issues. The application must check whether public-search is disabled on the users and the users’ friends profile; thus one can notice if the user changed default settings or not. Moreover, the likes of the user and the friends must be analysed for ‘clickjacking’. This is a malicious technique that uses invisible HTML elements that force the user to click on a ‘like’ button. One can filter such websites using a simple heuristic: if a website that is liked is not hosted on facebook.com, then there is chance that it is a clickjacking website. So the user is asked to double-check if he really ‘liked’ that website or if it is a clickjacking attack. Furthermore, the Google API can be queried to find out how much information is out there about the user using his first- and last-name. Beyond that – using the friendslist within Facebook – the app can check if duplicate names exist in the friends list. This can give hints regarding imposters. Finally visibility of friends list of the friends shall be checked.

The GUI of the app is depicted in figure 2 and figure 3. The data displayed comes from a profile that was registered for test purposes.

The application published as ‘Can you be Googled’ (Gulenko 2013) is written in Java and runs on ‘Google App Engine’. This ‘Platform as a Service’ approach is used to build a dynamic web application. This is less time consuming than building the classical 'LAMP'-Stack. Moreover, applications on ‘Google App Engine’ are highly scalable.

The application is uploaded into the Facebook application directory with the following description:

1. Facebook privacy: Check public-search setting of you and your friends.
2. Detect clickjacking: Check whether you or your friends became victims of clickjacking.
3. Use search engines: Check what Google and ‘people search engines’ know about you and your friends.
4. Identity theft: Check whether you have 'double' friends in your friend list (an attacker could set up a fake profile with the name of a friend).
5. Help your friends: Post short tutorials on their wall.

Figure 1. Theory of planned behaviour (Ajzen 1991).
Figure 2. Application running and checking user's profile (The testuser is German).
4 Evaluation

We tested the app by deploying it and mailing it to friends, relatives and posting it as a status update on Facebook. Gender and age of the sample could not be measured; we can only be sure that the sample were Facebook users. Among 117 users, 72 did not change the default settings of public-search (Gulenko 2013). As already stated by other sources (Error! Reference source not found.) only a minority changes privacy settings. One reason for this is that the privacy settings are considered to be inconsistent and people did not understood how to change them. Another reason may be that the
settings were not changed consciously, e.g., a user, who wants to be found through search engines should keep this option on. Twenty-six participants had the public-search already off. The most important metric is if public-search changed from on to off. We find that in our sample 15 users changed their public-search option because of our Facebook application. The act of changing public-search took on average 10.5 minutes. It was measured how long it took to start the app, do the changes and restart the app – this is what the user was supposed to do to check if the changes were successful. If a user did not do these steps, he was excluded from the study.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total users</td>
<td>117</td>
</tr>
<tr>
<td>Public search on (default)</td>
<td>72</td>
</tr>
<tr>
<td>Public search off (already changed before initial use of app)</td>
<td>26</td>
</tr>
<tr>
<td>Started application only once</td>
<td>56</td>
</tr>
<tr>
<td>Public search changed</td>
<td>15</td>
</tr>
</tbody>
</table>

Table 1. Results of the measurement of the Facebook application. Fifteen users changed the privacy setting “public search” due to our app.

5 Conclusion

Our research-in-progress study suffers from several limitations. Gender and age were not considered. However, these are possible confounding variables and have to be taken into account. Also previous knowledge of the users about privacy and IT-security must be measured. To get a bigger sample size, further studies could use Amazon’s Mechanical Turk or Microworkers.com. Moreover, the graphical user interface of the app should be refactored to become more user-friendly. Finally, the app could be made faster, because it takes about 10 seconds or more, if a user has more than 300 friends.

Despite the limitations, the Facebook application is a reusable solution to raise awareness for privacy among Facebook users. The treatment is cheap and highly scalable. The TPB predicted a significant change in privacy settings among the users and ten percent did exactly that. Therefore, we suggest further studies on viral techniques that nudge users to behave more securely online.
References


