Codes v. People: A Comparative Usability Study of Two Password Recovery Mechanisms

Vlasta Stavova, Vashek Matyas, Mike Just

Codes v. People: A Comparative Usability Study of Two Password Recovery Mechanisms

Vlasta Stavova[1], Vashek Matyas[1], and Mike Just[2]

[1] Faculty of Informatics, Masaryk University, CZ
[2] School of Mathematical & Computer Sciences, Heriot-Watt University, UK
{vlasta.stavova@mail.muni.cz,matyas@fi.muni.cz,m.just@hw.ac.uk}

Abstract. Password recovery is a critical, and often overlooked, requirement of account management. Currently popular solutions, such as security questions and out-of-band communications, have recognized security and usability issues. In this paper we evaluate two alternate recovery solutions considered by our industrial partner, using backup codes and trusted people, in order to determine their suitability as a viable password recovery solution. In this paper we focus on the usability evaluation of these two representative recovery methods, and not on the specifics of their design – while our evaluation results do indirectly point to general design enhancements. Our study determined that participants felt that backup codes (implemented as a QR-code in our solution) offer levels of usability and security that are acceptable to users for securing their "ordinary" accounts. For accounts perceived to require more security (e.g., online banking) more security was preferred by participants, resulting in a preference for trusted party recovery compared to backup codes. Our results also suggest that further research and deployment considerations should be given to options for other methods of password recovery, such as backup codes and trusted parties [3].

1 Introduction

Nearly every website that enables users to create an account also provides a process to recover the account, in case of a forgotten password, for example. This process is referred to by many names, such as account recovery, password recovery, password reset, secondary authentication and last-resort authentication [8, 16, 22]. The recovery process should be usable, and as secure as the access to the account via the primary authentication.

Researchers have shown that passwords, as a primary form of authentication, are indeed forgotten or lost, so that some form of recovery is required [12, 19]. Though current recovery solutions, such as the answers to *challenge questions*, are proven not to be reliable and secure enough [7]. Moreover, there are several examples of attackers gaining access to an account due to weak password recovery [10, 15, 23].

[3] Full details and paper supplementary materials can be found at http://crcs.cz/papers/wistp2016.

There are several ways in which password or account recovery can be performed, including the use of *challenge questions*, *out-of-band communications* (using email or SMS), calling a *help-desk operator*, using *password hints* or *backup codes*, or *using a trusted person*. Research in 2010 indicated that *out-of-band communications* and *challenge questions* were the most frequent methods used [8]. For the most part, current password recovery processes have maintained this trend. For example, Dropbox's password recovery process consists of an out-of-band email with a link to reset user's password [3]. Google services use a recovery email address or recovery phone number [6]. If a user has no access to his recovery email, phone or any other option, the user's identity can be verified by answering several questions about his account [4].

Three security questions must be answered by a user to recover his password for Apple services (iCloud, the App Store, the iTunes Store and more) [5]. All previously mentioned web services also support two-factor authentication. Since this option usually requires the combination of a computer and a mobile phone, there must be an approach to when the mobile phone is lost, stolen, or out-of-order. One common approach involves an emergency *backup (QR) code*. For example, after enabling two factor authentication in Dropbox[4], a user receives a special 16-digit backup code. The user must write this key down and store it somewhere safe. In case of losing his phone, this code may be used for an emergency access to the system [2]. Google users who use two factor authentication may download a backup code too or may add a backup phone in addition to the standard one [6]. Very similarly, Apple users get a recovery key for two factor authentication to be used when the trusted device is lost [5]. As an alternative to a *backup code*, researchers have also investigated using *trusted people* to support recovery [22], and at least Facebook has deployed such a solution, referred to as "trusted contacts"[5].

In this paper, we evaluate two password recovery methods based on the above-mentioned techniques: *backup codes* and cooperation of a *trusted person*. Both recovery methods were shortlisted by a company SODATSW. that offers secure data solutions. This company wanted to evaluate both solutions and compare them in terms of usability. The company agreed to use students as participants with the condition that both IT and non IT oriented students would be involved into study.

Thus, our task was to evaluate the usability of these two methods in order to determine their suitability as a viable option for password recovery and discuss possible further research and deployment consideration for other methods of password recovery.

---

[4] Dropbox has recently added an option to use Universal 2nd Factor (U2F) security keys to partially mitigate against mobile phone issues, though this too requires possession of a USB, which might become lost, stolen, or out-of-order. See `https://blogs.dropbox.com/dropbox/2015/08/u2f-security-keys/`

[5] `https://www.facebook.com/notes/facebook-security/introducing-trusted-contacts/10151362774980766`

To achieve our goal, we conducted a study with 186 student participants in order to compare the two password recovery methods.

In Section 2 we describe the related work in the area of password recovery. Section 3 introduces our approach to the design of the two password recovery methods, while Section 4 specifies the experiment design. Section 5 explains the experiment analysis and we conclude in Section 6.

2 Related Research

In this section we highlight relevant research related to currently used techniques for the recovery (security questions, and out-of-band communications), as well as previous work on the two methods we investigate in this paper (backup codes and trusted people).

2.1 Current Recovery Techniques

A recent study by Google concluded that security questions are neither secure nor reliable enough to be used as a standalone account recovery mechanism [7]. As a major issue, security questions might get successfully guessed. High guessability may be caused by using publicly available answers (16% of answer can be found in social network profiles [20]), using answers available to user's family and close friends (they can guess 17% of answers correctly in less than five attempts [21]) or small answer spaces (more than 40% security questions have small answer spaces [16, 20]). The other disadvantage connected to security questions is that users tend to forget their own answers. Research [21] showed that participants forgot 20% of their own answers within six months. Considering the fact that password recovery is often a last-resort option to regain access to a system, this is a very serious drawback leading to user frustration and potentially to more expensive forms of recovery, such as through a help desk. As a solution to this issue, researchers have tested an approach where questions were chosen by users themselves [16]. The approach was based on the idea that users will choose questions familiar to them, and thus they will not have a problem to recall answers. Contrary to expectations, the approach did not bring the anticipated improvement.

Out-of-band communications for password recovery (also used for secondary authentication) have risen in popularity, for example Google strongly prefers out-of-band password recovery (via SMS or email) over security questions [7].

Despite their importance for secondary authentication, and the fact that smart phones aggregate many potentially sensitive functions, more than 60% of smart phone users do not lock their device [1]. This poses a threat for password recovery based on out-of-band communication (via email or SMS). Further, smart phone theft is a serious issue. About 3.1 million smart phones were stolen in USA in 2013. Moreover, 1.4 million smart phones were lost and never recovered in the same year [1]. When the smart phone is stolen, an attacker may initiate the password recovery based on the SMS or gain free access to an email

account which can be also be misused for password recovery. When a user does not react quickly and does not change all his secondary authentications connected with the smart phone, his accounts may become compromised. Recent research on two-factor authentication demonstrates that given one compromised device, either a PC or a mobile phone, an attacker is able to compromise another one by launching a cross-platform infection attack [11].

In terms of usability, Bonneau et al. [7] compared the main account recovery methods (SMS reset code, email and security questions) used in a Google environment. While they showed that out-of-band communication channels like SMS and email have a higher success rate (respectively 80% and 74%) than security questions (ranges from 44% to 60%), the highest success rate still leaves a 20% failure.

2.2 Existing Research on Codes and People

Recovery based on a *backup code* is used by several account providers, especially for the recovery process for two-factor authentication. However, it has received only limited attention in the research literature. The use of a backup code should reduce the instances of "being forgotten" or of a smart device becoming lost or not working properly, as the code is typically stored offline. The backup code may be provided to the user in a plain text or shown in a more sophisticated way, for example as a *QR code*.

Saving a code as a QR code instead of a written, alphanumeric code may have several benefits. For example, it might avoid errors when entering the code during recovery, as it may simply be more convenient to scan rather than type.

A QR code is a two-dimensional barcode that can include up to 4296 alphanumerical characters – a string long enough to store a strong password. All devices equipped with a camera and a QR code decoding application can serve as a QR code reader. Authentication using a QR code has been already presented in the literature [17, 18], but it was mainly designed for primary authentication. One step of these authentication schemes is to send a QR code with encoded information from a service provider to a user. The user decodes information stored in the QR code and generates a one-time password. The use of the QR code serves as an alternative to a security card in both cases. Unfortunately, the approach from [18] relies on the fact that user's smart phone must be well protected since the smart phone stores a user's long-term secret key. Similarly, another approach [17] also relies on information stored in a user's smart phone. Thus, smart phone theft poses a danger for both approaches.

A more recent approach for password recovery is to use a *trusted party*. This method relies on a user's trusted person or people to help him recover an account access.

This method seems to be a good match to use with social networks where trusted people are selected by the user from his trustworthy friends. For example, this method is used at Facebook and was studied in Microsoft Live ID [22]. The tested approach was based on requesting recovery codes by user's trusted friends

via specialized web interface. The user must collect from them at least three codes out of four to regain access to the system.

When a Facebook user forgets his password, he must contact his trusted friends to send a recovery request to the provider and obtain the security code. The user must collect at least three codes from three to five selected trusted friends [13]. The trusted party based method is prone to Forest fire attack [13], which misuses the fact that the user and his trusted friends are all members of one single system. If a small subset of users are compromised, all friends who trust them can be compromised too. As the number of compromised accounts rises, even more users may be compromised. In other words, it spreads like a forest fire.

3 Our Password Recovery Approaches

When designing password recovery processes, we discussed all of our approaches with SODATSW company designing a new secure data storage solution. The company insisted on a balance between usability, security and resistance to a smart phone theft. Based on SODATSW requirements, a Master thesis [14] reviewing possible approaches to password recovery was written, also suggesting some new ones. After a final round of discussions with the company, we agreed to test the approach based on a QR code and the other based on a trusted person.

3.1 Password Recovery via One-Time Password Stored in a QR Code

We designed a simple password recovery process using the backup code in the form of the QR code. The steps of this process are as follows:

1. A user receives a QR code via a registered letter (or any other service that guaranteed delivery to the receiver) and hides it in a secret place. The QR code contains a backup code.
2. If the user forgets his password, the recovery process can be initiated.
3. To start the recovery, the user scans the QR code.
4. The user inserts his user name into a system and retypes the code from the QR code reader into the system. When the user has a smart phone with the QR code reader and Internet access, he may open the system in the smart phone and copy and paste the code directly.
5. The system requires setting a new password.
6. After setting a new password, the user gains access to the system.

The QR code is not bound to a specific device, so when a user's own smart phone is stolen, the user can utilize any other QR code reader. It is also a disadvantage, because any QR code reader can read the QR code with the backup code. This increases requirements for the secret distribution and storage of the QR code. The user is instructed to securely store the QR code together with his important contracts. It is also strictly forbidden for the user to scan the QR code

in an advance and store it in the smart phone (though this might be difficult to enforce).

Unlike a one-time password stored as text on a piece of paper, a one-time password stored as a QR code enables a user to copy a decoded password directly from a smart phone application to the system which can be opened in the smart phone. Of course, when the user has only a QR reader without an access to the Internet, password retyping is unavoidable. A possible drawback is when the recovery password from a QR code is used, a new QR code must be securely distributed to the user. Company SODATSW is aware of it and plans to use this solution only in countries that have necessary infrastructure. As far as costs are concerned, QR codes are not expensive to produce, but the price of secure distribution must be taken into account.

3.2 Trusted Party Based Password Recovery

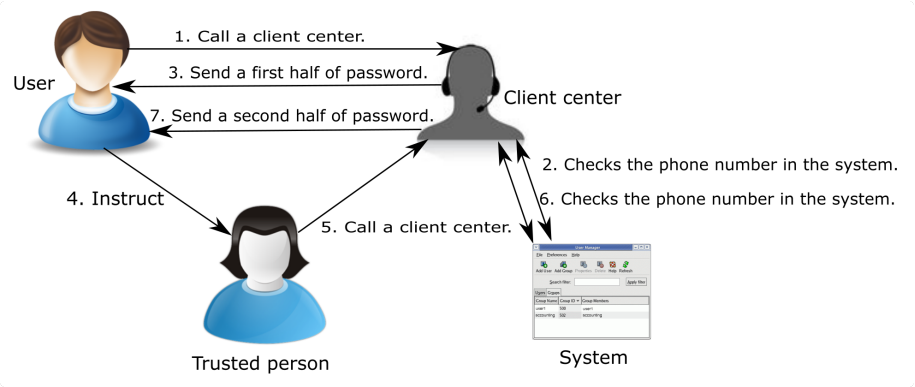
Unlike the use of a QR backup code, the use of a trusted party is based on shared inter-personal trust. To balance usability and also take into account a potential problem with low willingness to provide a phone number of a user's friends, we decided to require only one trusted person for each user (and the user himself also actively participates in the recovery). The trusted person may or may not be another system user. The user is expected to set family members or co-workers as a trusted person to decrease the probability of a Forest fire attack [13].

A step-by-step password recovery process (see also Figure 1) was designed as follows:

1. During the registration process, a user registers his phone number and also the phone number of the person he trusts.
2. When a password is lost or forgotten, the user will call the client center.
3. If the phone number he used for a call matches with the phone number registered in the system, a client center operator sends him a first half of a backup code via SMS.
4. The user must instruct his trusted person to call the client center and ask for a second half of the password.
5. The trusted person who recognizes the user's voice or appearance will do the task. If the trusted person's phone number matches with the phone number registered in the system, the operator sends the other half of the code to the user.
6. The user inserts his user name and both codes into the system.
7. The system requires setting a new password.
8. After setting a new password, the user gains an access to the system.

If an attacker steals a user's mobile phone, he does not know which of his friends is the trusted person. Even if the attacker knows this information, he must convince the trusted person to call the client center. To increase overall security and to decrease the probability of impersonating the user by an attacker, users are encouraged to instruct their trusted party to proceed with a call to the client

Fig. 1. Trusted party based recovery.



center only after proper identification. For example, the user should instruct the trusted party to call a client center only during a face-to-face meeting or a phone call.

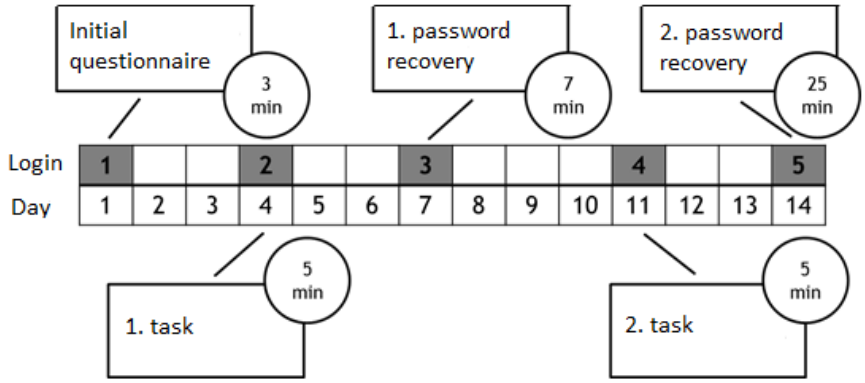
One disadvantage of this process is that during registration users may not fully think about the prospect of a password recovery and might be less likely to submit the phone number of an appropriately reliable and trusted person. Further, this person may change during a user's life and it would be important to keep this information up-to-date. Also, it is not the most efficient recovery process due to the fact that the trusted person may be away (for example on business trip, on holiday) when his call is necessary. This recovery method is also based on the user's phone number being registered into the system. If a user loses his number and in the same time forgets his password, this password recovery can not be successfully processed. The other issue may be that people might forget which person they designated. But similarly, they can forget the response for a security question (as we mentioned in the previous section). Recovery costs are higher, because the client center must be available, but the interaction may be automated.

4 Experiment Design

To compare both approaches, an experiment in cooperation of Faculty of Social Studies and Faculty of Informatics was designed. The experiment design was undertaken in accordance with experimental and ethical regulations of our university.

The experiment ran in May and June 2015 and the main aim of the experiment was to compare both approaches. There were 186 participants in total (of the original 203 who underwent full registration), half of them from the Faculty of Informatics, the other half together from other faculties (mainly from Faculty of Social Studies, Faculty of Law and Faculty of Arts). We used a within-subject experiment design – all participants went through both recovery approaches,

Fig. 2. Experiment process.



and we alternated the order of their encounter so that half started with backup codes, and half with the trusted person approach. We collected quantitative data (but not qualitative) from this experiment.

To support our recruitment, we made a short presentation to students from several faculties at the start of one of their lectures. After an initial experiment presentation, participants obtained an envelope with a letter describing the process of the entire experiment, with a login and password to the system and a QR code (14 characters, charset size is 62) to be used for one password recovery. Each participant went through a two-week process. We prepared two online tasks for participants and two password recoveries (see also Figure 2). We also separated participants into halves. Half of them went through the QR code recovery on the seventh day and the trusted person recovery on the day 15. The other half of participants used a an opposite recovery order. The experiment length was two weeks for each participant. We estimated that the time spent in the experiment would be 45 minutes for each participant.

- When participants first logged into the system, they filled an initial questionnaire, provided their demographics and information necessary for both recoveries (their phone number, their trusted person's phone number). We only mentioned that it should be a person of trust, for example, a good friend or a family member.
- On the fourth day after the first login, participants were encouraged to log into the system and to execute a short task of computing a number of characters in an attached PDF file. The purpose of this step was to attempt to maintain an active, realistic environment for participants.
- On the seventh day of the experiment, participants were asked to process a first recovery. Half of the participants went through a recovery using their QR code, and the other half used the trusted party based recovery. After completing the recovery, participants filled a questionnaire to evaluate it.

Table 1. Experiment participants overview.

Faculty	Males	Females	Participants in total
Faculty of Informatics	75	17	98
Faculty of Social Studies	23	41	67
Faculty of Law	8	9	17
Faculty of Arts	1	5	10
Other faculties	2	5	9

- On the eleventh day participants were asked to complete a second task. The task was to find a concrete paper, read through it, find one particular piece of information and insert it into the system.
- Fifteen days after the experiment started, participants completed their second password recovery and filled in a final, longer questionnaire where they evaluated and compared both recovery processes.

We sent email reminders to participants to remind them to perform the above tasks. As a motivation to join the experiment, we offered $400 and 25 32GB MicroSD cards to 26 randomly chosen participants who went through all experiment steps.

5 Experiment Results and Analyses

5.1 Participants

There were 186 participants in total (of the 203 undergoing full registration). All participants were students of our university (for a detailed breakdown see Table 1). All of them have at least secondary education.

The experiment had 5 phases, and participants went through the initial questionnaire, two tasks and two password recoveries. 132 participants out of 186 finished all phases. Half of the 132 participants went through the QR code recovery first followed by the trusted party. The other half (also 66) went through the process in an alternate order.

The majority (117) of participants were aged 19-22 years, while 69 participants were between 23 and 26 years. For a detailed view of when participants decided to leave the experiment, see Table 2. The fact that all participants were students is a limitation, though participants were recruited from both IT and non IT related programs. Since all participants are young people, we expect that they are more technically skilled than older generation.

Table 2. Experiment phases and dropped out participants. The table shows the number of participants who dropped before proceeding with each experiment phase. Group 1 has the QR code as 1^{st} recovery and trusted party based recovery as 2^{nd} recovery. Group 2 has alternate order of recoveries.

Group	Initial questionnaire	1^{st} task	1^{st} recovery	2^{nd} task	2^{nd} recovery
Group 1	5	4	3	15	–
Group 2	4	21	0	2	–

5.2 Recovery Method Evaluation

Participants went through two password recoveries in the experiment. After each recovery, participants evaluated the recovery in four categories. There were 132 participants who performed these evaluations (we involved only those who went through both recoveries). We did not observe any significant difference in answers between participants who had started with one recovery method versus the other.

- **Difficulty:** How difficult was it for you to use the recovery? The Likert scale was used for responses from 1 (totally easy) to 6 (totally difficult). We conducted a paired t-test analysis and it proved that the QR code password recovery is considered by participants to be less difficult (mean=1.72, SD=1.1) than the trusted party based recovery (mean=2.79, SD=1.56) ($t(132)=7.37$, $p<0.001$).
  We did not observe any significant difference between men (mean=2.57, SD=1.49) and women (mean=3.067, SD=1.60) in evaluating difficulty of the trusted party recovery ($t(133)=-1.92$, $p=0.057$) and also no significant difference between men (mean=1.71, SD=0.12) and women (mean=1.72, SD=0.14) in evaluating difficulty of the QR code recovery ($t(148)=-0.054$, $p=0.957$).
  We observed significant difference between IT (trusted party, mean= 2.32, SD=1.40), (QR code recovery, mean=1.48, SD=0.931) and non IT participants (trusted party, mean=3.25, SD=1.56), (QR code recovery, mean=1.98, SD= 1.22) in both the trusted party ($t(133)=3.59$, $p<0.001$) and the QR code recovery ($t(148)=2.85$, $p=0.005$). IT participants considered both recoveries as less difficult than non IT participants.
  Correlation of age and the trusted party recovery difficulty is significant ($r=0.22$, $p=0.011$), similarly correlation of age and the QR code recovery difficulty ($r=0.21$, $p=0.007$). The older user is, the more difficult recovery is.
- **Security:** How secure do you consider the recovery? The Likert scale was used for responses from 1 (totally secure) to 6 (totally insecure). The paired t-test proved that participants in this scale consider the QR code based recovery less secure (mean=3, SD=1.15) than the trusted party based recovery (mean=2.38, SD=1.17) ($t(129)=-5.25$, $p<0.001$).

Men (mean=3.2, SD=1.22) and women (mean=2.7, SD=0.96) had significant difference in evaluating security of the QR code based password recovery ($t(144)=2.94$, $p<0.004$). Men considered the QR code based recovery significantly less secure than women. On the other hand, there is no significant difference observed in security of the trusted party based recovery ($t(121)=0.24$, $p=0.8$) between men (mean=2.41, SD=1.27) and women (mean=2.36, SD=1.07).
Very similar results are obtained when comparing IT and non IT participants. Non IT participants (mean=2.74, SD=1.00) considered the QR code based recovery significantly more secure ($t(144)=-2.94$, $p=0.004$) than IT participants (mean=3.29, SD=1.22). There is no difference in IT (mean=2.53, SD=1.18) and non IT participants (mean=2.25, SD=1.18) in evaluating security of the trusted party based recovery ($t(131)=-1.34$, $p=0.18$).
Correlation of age and the trusted party recovery security is not significant ($r=0.14$, $p=0.1$), similarly correlation of age and the QR code recovery security ($r=0.128$, $p=0.123$).

– **Advanced security:** How secure do you consider to use this recovery for online banking? The Likert scale was used for responses from 1 (totally secure) to 6 (totally insecure). When considering a password recovery for a system with sensitive data, based on the paired t-test, the QR code based recovery is considered as less sufficient for online banking (mean=3.92, SD=1.34) than the trusted party based recovery (mean=2.89, SD=1.38) ($t(132)=-7.62$, $p<0.001$). However, the trusted party based recovery still only received a mean score between 2 and 3, and hence was not viewed as "totally secure".
Men (mean=4.17, SD=1.38) and women (mean=3.62, SD=1.24) evaluated differently advanced security of the QR code based password recovery ($t(147)=2.46$, $p=0.015$), but saw no difference in advanced security of the trusted party based recovery ($t(133)=0.53$, $p=0.594$, men:(mean=2.97, SD=1.39), women:(mean=2.84, SD=1.38)).
IT and non IT participants had no difference in evaluating advanced security of both the QR code based recovery ($t(147)=-1.61$, $p=0.108$) and the trusted party based recovery ($t(133)=-1.17$, $p=0.24$).
There is no significant correlation for age and advanced security of the QR code based recovery ($r=-0.007$, $p=0.929$) and the trusted party based recovery ($r=0.125$, $p=0.14$).

– **User friendliness:** How user friendly do you consider the recovery? The Likert scale was from 1 (totally user friendly) to 6 (totally user unfriendly). The paired t-test proved that the QR based password recovery is considered to be more user friendly (mean=2, SD=1.2) than the trusted party based recovery (mean=3.58, SD=1.57), ($t(132)=9.83$, $p<0.001$).
There is no significant difference in user friendliness of both recoveries for men and women (QR code recovery: ($t(148)=0.00$, $p=1$), trusted party based recovery ($t(133)=0.44$, $p=0.65$)). We observed significant difference in evaluating user friendliness of IT and non IT respondents in the QR code based recovery ($t(148)=2.41$, $p=0.017$), but no difference in the trusted party based recovery ($t(133)=-0.628$, $p=0.531$). IT participants (mean=1.77, SD=1.107)

evaluated the QR code based recovery more user friendly than non IT participants (mean=2.25, SD=1.35).
There is also a significant but weak correlation between age and user friendliness for the trusted party based recovery (r=0.176, p=0.041) and the QR code based recovery (r=0.16, p=0.42).

5.3 Overall Views

At the end of the experiment, participants were asked about their opinion of the two recovery methods using categories similar to those above. We also asked for their overall recovery method preference. The questions they were asked were "Which recovery do you consider more easy to use/secure/user friendly?" and "Which recovery do you overall prefer more?" The possible responses were "QR code recovery", "Trusted party based recovery" and "Both similarly". We used answers only from those 132 participants who went through both recoveries.

- **Ease to use:** 113 (86%) participants considered the QR code recovery easier to use than the trusted party based recovery. Only 6 (4%) participants thought the opposite and 13 (10%) participants considered both methods similarly easy.
- **Security:** 90 (68%) participants considered the trusted party based recovery more secure than the QR code based recovery. Only 14 (10%) participants had an opposite opinion and 28 (21%) did not see a difference between both methods.
- **User friendly:** 100 (76%) participants considered the QR code based recovery more user friendly over the trusted party based recovery. Only 6 (5%) participants thought the opposite and 26 (20%) considered both recoveries to be equally user friendly.
- **Overall recovery preferences:** When participants were ask to choose one recovery that they prefer, 76 (58%) participants preferred the QR based recovery whereas 35 (25%) participants preferred the trusted party based recovery. 21 (16%) participants preferred both recoveries equally.

We also conducted a χ^2 [9] test and Fisher's exact test (when some crosstab cells remained empty) and we did not find (at the significance level α=0.05) any statistically significant differences in perceptions of security, user friendliness and overall preferences of these recovery methods between men and women or IT and non IT participants. The only statistically significant difference (p=0.03) is in easiness to use recoveries between IT and non IT participants. IT participants had higher tendency to choose "Both options were similarly easy to use" over "Trusted party based recovery was easiest to use" in comparison with non IT participants.

5.4 Other Observations

In terms of the *effectiveness of both recovery methods*, we can report that we observed some unsuccessful trials. 79% participants succeeded with a QR code

based recovery at the first try. Moreover, 89% participants did a QR code based recovery with zero or one unsuccessful trial. Recovery with a trusted party had similar results. 75% of participants succeeded on their first attempt. In addition, 88% of the users processed a trusted party based recovery with zero or one unsuccessful trial. In comparison to earlier studies on currently used recovery techniques such as challenge questions where 20% of participants forget their answers after 6 months [21], our studied recovery methods show an improvement. We observed no significant difference in number of trials of men and women or IT and non IT participants.

The success rate (ratio between the number of successful attempts and the total number of attempts) of a trusted party based recovery is approximately 48%. The success rate for QR code based recovery is approximately 49%. This shows that both methods seem to be similarly prone to error. We had no limits in attempts to insert a code in the recovery. The ratios are particularly low due to few outliers who tried to insert a recovery code 10, 11, 12 or 13 times before they succeeded.

The time between system request to start recovery and finishing the recovery was on average nearly 53 minutes for the trusted party based recovery, and 9 minutes for the QR code based recovery. From the user's point of view *trusted party based recovery is slower than the other recovery method.*

We also included a couple of additional questions related to the difficulty of carrying out the recovery processes. The first was related to the difficulty of finding a QR code reader. We used the Likert scale from 1 (totally easy) to 6 (totally difficult) for responses. In general, participants found it very easy to locate their QR code reader (mean=1.64, SD=1.17). We conducted a t-test and observed statistical significant differences (at the statistical significance level α=0.05, t(130)=2.86, p<0.05) between participants from the Faculty of Informatics (mean=1.36, SD=0.92) and participants from other faculties (mean=1.92, SD=1.33). Statistically significant differences (α=0.05, t(130)=-2.21, p<0.05) in this question were also observed between men (mean=1.49, SD=0.99) and women (mean=1.89, SD=1.33). To sum up, even with these relative differences, all participants found it easy (with mean scores less than 2).

The second question related to the difficulty of QR code scanning. We used the Likert scale from 1 (totally easy) to 6 (totally difficult) for responses. Generally speaking, participants considered this process easy (mean=1.35, SD=0.95), but we observed a significant difference (at the statistical significance level α=0.05, t(130)=3.72, p<0.001) between participants from the Faculty of Informatics (mean=1.06 SD=0.24) and participants from other faculties (mean=1.65, SD=1.27). Participants from the Faculty of Informatics considered the QR code scanning even easier than their colleagues from different faculties. Very similarly, participants considered it to be very easy to call a client center (mean=1.84, SD=1.19), and we did not observe any statistically significant difference between IT and non IT students or men and women. On the other hand, we must take into account that if a participant had a serious problem to find the QR

code reader or had a problem to call the client center, he may have stopped the experiment without completing the questionnaire.

Related to the use of the client center, there were several issues connected with password recoveries. The major flaw connected with the QR code recovery was that several QR code reading applications do not distinguish characters "l" and "I", "O" and "0". One participant also reported that his QR reading application showed the whole text in lower case. One solution may be to recommend a particular QR code reading application that would work correctly to avoid above mentioned issues. Another solution may be also to remove problematic characters out of the backup code. Of course, it could mean that codes would be lengthened.

The client center similarly observed issues connected with the trusted party based recovery. We have observed several difficulties in retyping SMS codes from a phone to the system. For participants was hard to recognize several problematic characters. For example "0" instead "O". The solution can be same as in the previous case.

6 Conclusion

We evaluated two alternate recovery solutions, using backup codes and trusted people. Despite the fact that both methods have expectable drawbacks, our research set out to confirm these issues to support our goal of promoting a discussion on other types of recovery processes. Despite the fact that the *trusted party based recovery was considered by 90 (68%) participants to be more secure than the QR code based recovery* (14 participants (11%)), the majority of participants gave their *overall preferences to the solution that they consider easier to use and more user friendly: the QR code based recovery.* 100 participants out of 132 considered the QR code based recovery more user friendly and 113 participants considered it easier to use than the trusted party based recovery. We observed that for the trusted party based recovery participants spent more time to perform the recovery (53 minutes for trusted party and 9 minutes for QR code) whereas the number of unsuccessful trials were nearly equal – 89% participants processed the QR code recovery with one or zero unsuccessful trial and 88% did the same with the trusted party based recovery. We observed several interesting points such as that IT participants considered both recoveries as less difficult than non IT participants. Men (and IT participants) considered the QR code based recovery significantly less secure than women (and non IT participants).

We also observed that participants perceived a strong difference between an "ordinary" website level of security and the security good enough to be used for their online banking. When comparing both recovery methods, results for the "standard security" were nearly the same, but for security good enough for online banking there were significant differences in answers so that the trusted party based recovery was considered to be more secure. Our participants, who

are university students, seemed to be well aware of possible secure drawbacks of our solutions.

As for the perception of password recovery difficulty, both recoveries scored similarly. *We did not find (at the statistical significance level α=0.05) that there would be any difference in recovery preferences (security, user friendliness or in overall recovery preference) between men and women or the IT and non IT participants.* The only significant difference was between IT and non IT participants in ease of use. IT participants tended to choose "Both recovery methods are similarly easy to use" more than non IT participants who slightly more preferred the trusted party recovery as easier to use.

We recommended to the company to offer the QR code solution as a default for all users. The trusted party based recovery should be suggested only to users who demand a higher level of security. The trusted party based recovery can be then used either instead or even in combination with the QR code based recovery.

Acknowledgements. The authors acknowledge the support of the Masaryk University (MUNI/M/1052/ 2013). Authors would like to thank Department of social studies for a help with a data analysis.

References

1. Smart phone thefts rose to 3.1 million in 2013. `http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-million-last-year` (2014), [Online; Accessed 15-June-2016]
2. How do I enable two-step verification on my account? `https://www.dropbox.com/en/help/363` (2015), [Online; Accessed 15-June-2016]
3. I forgot my password. How do I reset it? `https://www.dropbox.com/help/168` (2015), [Online; Accessed 15-June-2016]
4. I'm having trouble resetting my password. `https://support.google.com/accounts/answer/1723426?hl=en` (2015), [Online; Accessed 15-June-2016]
5. Security and your Apple ID. `https://support.apple.com/en-us/HT201303` (2015), [Online; Accessed 15-June-2016]
6. Set up a recovery phone number or email address. `https://support.google.com/accounts/answer/183723?hl=en` (2015), [Online; Accessed 15-June-2016]
7. Bonneau, J., Bursztein, E., Caron, I., Jackson, R., Williamson, M.: Secrets, lies, and account recovery: Lessons from the use of personal knowledge questions at google. In: Proceedings of the 24th International Conference on World Wide Web. pp. 141–150. International World Wide Web Conferences Steering Committee (2015)
8. Bonneau, J., Preibusch, S.: The Password Thicket: Technical and Market Failures in Human Authentication on the Web. In: WEIS (2010)
9. Corder, G., Foreman, D.: Nonparametric Statistics: A Step-by-Step Approach. Wiley (2014)
10. Cubrilovic, N.: The Anatomy Of The Twitter Attack. `http://techcrunch.com/2009/07/19/the-anatomy-of-the-twitter-attack/` (2009), [Online; Accessed 15-June-2016]

11. Dmitrienko, A., Liebchen, C., Rossow, C., Sadeghi, A.R.: On the (in) security of mobile two-factor authentication. In: Financial Cryptography and Data Security, pp. 365–383. Springer (2014)
12. Florencio, D., Herley, C.: A large-scale study of web password habits. In: Proceedings of the 16th International Conference on World Wide Web. pp. 657–666. ACM (2007)
13. Gong, N.Z., Wang, D.: On the security of trustee-based social authentications. Information Forensics and Security, IEEE Transactions on 9(8), 1251–1263 (2014)
14. Hamerník, J.: Autentizační metody používané k obnově přihlašovacího hesla, Master thesis (in Czech), Masaryk University (2014), [Online; Accessed 15-June-2016]
15. Honan, M.: How Apple and Amazon Security Flaws Led to My Epic Hacking. `http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/all/` (2012), [Online; Accessed 15-June-2016]
16. Just, M., Aspinall, D.: Personal choice and challenge questions: a security and usability assessment. In: Proceedings of the 5th Symposium on Usable Privacy and Security. p. 8. ACM (2009)
17. Lee, Y.S., Kim, N.H., Lim, H., Jo, H., Lee, H.J.: Online banking authentication system using mobile-OTP with QR-code. In: Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference on. pp. 644–648. IEEE (2010)
18. Liao, K.C., Lee, W.H.: A novel user authentication scheme based on QR-code. Journal of Networks 5(8), 937–941 (2010)
19. Moallem, A.: Did You Forget Your Password? In: Design, User Experience, and Usability. Theory, Methods, Tools and Practice, pp. 29–39. Springer (2011)
20. Rabkin, A.: Personal knowledge questions for fallback authentication: Security questions in the era of facebook. In: Proceedings of the 4th symposium on Usable privacy and security. pp. 13–23. ACM (2008)
21. Schechter, S., Brush, A.B., Egelman, S.: It's no secret. measuring the security and reliability of authentication via secret questions. In: Security and Privacy, 2009 30th IEEE Symposium on. pp. 375–390. IEEE (2009)
22. Schechter, S., Egelman, S., Reeder, R.W.: It's not what you know, but who you know: a social approach to last-resort authentication. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 1983–1992. ACM (2009)
23. Wikipedia: Sarah Palin email hack — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Sarah_Palin_email_hack& direction=next&oldid=667446959 (2015), [Online; Accessed 15-June-2016]