I'm too Busy to Reset my LinkedIn Password: On the Effectiveness of Password Reset Emails

Jun Ho Huh
Honeywell ACS Labs
junho.huh@honeywell.com

Hyoungshick Kim
Sungkyunkwan University
hyoung@skku.edu

Swathi S.V.P. Rayala
Oregon State University
rayalas@oregonstate.edu

Rakesh B. Bobba
Oregon State University
rakesh.bobba@oregonstate.edu

Konstantin Beznosov
University of British Columbia
beznosov@ece.ubc.ca

ABSTRACT

A common security practice used to deal with a password breach is locking user accounts and sending out an email to tell users that they need to reset their password to unlock their account. This paper evaluates the effectiveness of this security practice based on the password reset email that LinkedIn sent out around May 2016, and through an online survey conducted on 249 LinkedIn users who received that email. Our evaluation shows that only about 46% of the participants reset their passwords. The mean time taken to reset password was 26.3 days, revealing that a significant proportion of the participants reset their password a few weeks, or even months after first receiving the email. Our findings suggest that more effective persuasive measures need to be added to convince users to reset their password in a timely manner, and further reduce the risks associated with delaying password resets.

ACM Classification Keywords

H.5.m. Information Interfaces and Presentation (e.g. HCI): Miscellaneous

Author Keywords

Password reset; password breach; reset email; LinkedIn.

INTRODUCTION

After the LinkedIn's data breach in 2012, it was reported that about 6.5 million user email addresses and passwords were leaked. Those passwords were stored as unsalted SHA-1 hashes, and were vulnerable to offline guessing attacks that use rainbow tables [9]. In May 2016, however, LinkedIn's chief information security officer, Cory Scott, published an official post [10] saying that,

> *".. we became aware of an additional set of data that had just been released that claims to be email and hashed password combinations of more than 100 million LinkedIn members from that same theft in 2012. We are taking immediate steps.. and we will contact those members to reset their passwords."*

LinkedIn sent out a password reset email to potentially affected users, asking them to reset their passwords the next time they sign in. LinkedIn "invalidated" those accounts, meaning that they were locked (unusable) until users reset their passwords. Each of the affected users was asked to visit LinkedIn, sign in with their current password, request a password reset, open a second email that contains a password reset link, and follow that link to create a new password. Dropbox also went through a data breach in 2012, and only recently realized that the breach may have affected 68 million users [7]. They also sent out an email to potentially affected users after locking their accounts. With this account locking practice in place, attackers would also have to compromise the email account of a victim to steal the password reset link, and take control of the account.

Nevertheless, this reliance on the security of an email account (a second channel) has well-known risks [4, 6]: people often use the same password across multiple sites, or make small changes to the current password in order to create a new password. If a user uses the same password for both LinkedIn and their email account, an attacker would be able to obtain the password reset link and reset the password, taking control of the user's account. Similarly, if the password of the user's email account is a small variation of the password used on LinkedIn, an attacker would be able to perform informed guessing of the email account password. Another possible attack involves an attacker signing into LinkedIn with a stolen email and password pair, and requesting a password reset. The attacker then immediately sends a phishing email to the user, requesting the user to copy and paste the password reset link they received on a malicious page (Karlof et. al. [8] showed that such a phishing attack has about 48% success rate). The attacker would then gain access to the password reset link without knowing the user's email password. This attack, however, will not work if the user has already reset his or her password.

To further mitigate such risks of account compromise, it is integral to persuade users to *quickly* reset their passwords. This paper studies the effectiveness of email-based password reset recommendation practices based on the recent real-world LinkedIn case study. We recruited 249 LinkedIn users who received a password reset email from LinkedIn in 2016, and

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
CHI 2017, May 6-11, 2017, Denver, CO, USA.
Copyright © 2017 ACM ISBN 978-1-4503-4655-9/17/05 ...$15.00.
http://dx.doi.org/10.1145/3025453.3025788

asked them about their experiences with this email. To the best of our knowledge, this is the first empirical analysis of the effectiveness and timeliness of email-based password reset practices used today by many IT companies. Surprisingly, only 46% of the participants reset their password after reading the email. The mean time taken to reset password was 26.3 days (standard deviation of 33.3), with some taking weeks or even months, indicating a significant delay. Only about 32% of those who reset their password (this is about 15% of all participants) did so on the same day they received the email. About 50% of the participants were using the same (LinkedIn) password on at least one other site, increasing the risk of password reset link and account compromise.

METHODOLOGY

We recruited participants on Amazon Mechanical Turk (MTurk) between June and September 2016. We limited MTurk workers to those in the United States, and asked MTurk workers to participate only if (1) they had accounts on LinkedIn, and (2) have received a password reset email from LinkedIn in 2016. Before collecting responses, we conducted an in-person pilot study with 4 LinkedIn users (who received the email) to test our data collection instruments. Up to this point, most of the survey questions were designed as open-ended questions. We then conducted a second pilot study directly on MTurk with 51 participants to collect open-ended responses. Two researchers used *open coding* to code those responses separately, and discussed the identified codes until they reached consensus on all codes. Those codes were then used to create answer options for the final survey questions. The survey consisted of the following parts:

1. **Concerns:** We asked the participants about their concerns with LinkedIn account being hacked, and how many other sites that they use had the same password as their LinkedIn password.
2. **Password reset:** We asked the participants whether they reset their LinkedIn password.
3. **Reasons for (not) resetting password:** We asked the participants why they reset or did not reset their password after reading the password reset email from LinkedIn.
4. **Password reset behavior:** For those who did reset their password, we asked how they created their new password.

To validate whether a participant has received the password reset email, we asked the participants to submit two screenshots: (1) a screenshot of the initial password reset email received from LinkedIn, and (2) a screenshot of the reset confirmation email received after resetting password. The participants were asked to upload the second screenshot only if they reset their password. We paid $2.00 to all participants except for those who did not submit any screenshot. Hence, there was no reason for the participants to lie about whether they reset their password. We later used those screenshots to validate their eligibility to participate, and extract the *exact date* in which the reset email was first received and the password was reset.

We excluded responses from those who did not provide us with the screenshots, or who did not follow the screenshot instructions (attention checking). To rule out those who reset their password regardless of the content of the email (e.g., someone who tried to sign in without reading the email, and was asked to reset password to unlock their account), we excluded responses from those who answered *"not influential at all"* to the question *"How influential was the password reset email in deciding to reset your password?"* To minimize the effects of the participants habitually choosing options located in certain positions, we randomized option orders in all applicable questions. Our study was approved by a university Institutional Review Board (IRB).

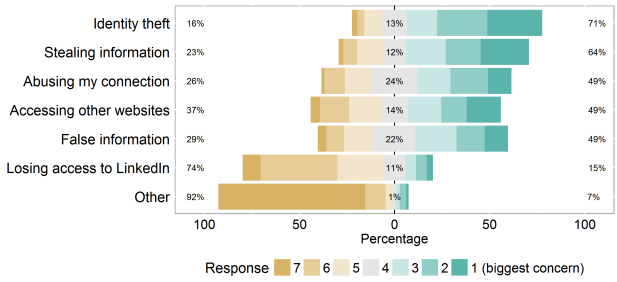

Figure 1. Concerns about LinkedIn account being hacked, sorted based on the overall distribution of the ranks between 1 and 7, where rank 1 is the biggest concern and 7 is the smallest concern.

RESULTS AND RECOMMENDATIONS

Demographics

In total, we recruited 943 LinkedIn users. From the 943 participants, we excluded 685 who failed at least one of the screenshot checks, and 9 who said that the email was "not influential at all." This left 249 (26.41%) responses for data analysis. Most of the participants were whites (72.87%), and the majority were in the age groups of 25–34 (58.63%), 35–44 (22.09%), and 19–24 (11.24%). 54.62% were female. 61.85% had a university degree, 22.89% had master's and doctoral degrees, and 14.06% had a high school diploma. 45 different occupations were reported with computer (15.26%), unemployed (10.44%), and business (9.24%) being the top ones.

Concerns about LinkedIn account being hacked

We asked the participants *"What would concern you the most if your LinkedIn account was hacked? Rank the options below in order of your level of concern, Rank 1 being your biggest concern. If a given option does not concern you at all, leave its ranking as blank. If there is no* `other` *concern, leave its ranking as blank"* We also asked the participants *"If you had* `other` *concern and ranked it, please specify what that reason is."* Figure 1 shows the concerns for LinkedIn account being hacked, sorted based on the overall ranking distributions.

"Someone pretending to be me through identity theft" (`identity theft`) and *"Stealing my personal information from LinkedIn"* (`stealing information`) were the top two concerns. `Identity theft` showed statistically significant difference in the overall ranking distribution against all other reasons (all $p < 0.05$, Bonferroni-corrected Mann-Whitney U test) except for `stealing information`. `Stealing information` showed statistically significant difference against all other reasons (all $p < 0.05$, Bonferroni-corrected MW U test) except for `identity theft` and *"Exploiting and abusing my LinkedIn contacts"* (`abusing my connections`). The participants were least concerned about

Table 1. Percentage of the participants who reset, or did not reset their passwords after receiving the email.

Options	Count	
`Yes (I reset)`	114	(45.78%)
`No (I did not reset)`	119	(47.79%)
`I have no idea`	16	(6.43%)

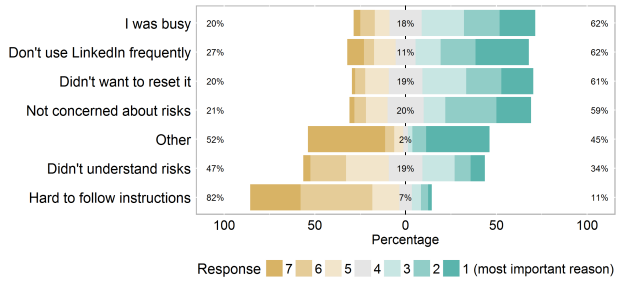

Figure 2. Reasons for *not resetting* password, sorted based on the overall distribution of the ranks between 1 and 7.

"Losing access to my LinkedIn account" (`losing access to LinkedIn`), which showed statistically significant inferiority in ranking distribution against all other reasons (all $p < 0.0001$, Bonferroni-corrected MW U test) except for `other`.

Did you reset your password?

To gauge the number of participants who reset their password, we asked *"In response to receiving the password reset email from LinkedIn, did you reset your password?"* Surprisingly, only 45.78% of the participants reset their passwords as shown in Table 1. 47.79% said they did not reset passwords, implying that their accounts are still at risk of being compromised.

Reasons for not resetting password

To those who did not reset their password, we asked *"If you did not reset your password after reading the email, why did you not reset it? Rank the options below in the order of your level of importance, Rank 1 being the most important reason. If a given reason is not important at all, leave its ranking as blank."* Figure 2 shows the reasons for not resetting password, sorted based on the overall ranking distributions.

Top three reasons for not resetting password were *"I was busy"* (`I was busy`), *"I do not use LinkedIn frequently"* (`don't use LinkedIn frequently`), and *"I did not want to reset my password"* (`didn't want to reset it`), indicating that those who did not reset password tend to be infrequent users, and/or did not feel it was necessary to make time to reset their password. `I was busy` showed statistically significant difference in the overall ranking distribution against *"I did not understand potential security risks to my LinkedIn account"* (`did not understand risks`), *"Instructions for resetting my password were hard to follow"* (`hard to follow instructions`), and `other` (all $p < 0.005$, Bonferroni-corrected MW U test). *"I was not concerned about potential security risks to my LinkedIn account"* (`not concerned about risks`) also ranked high, and did not show any statistically significant inferiority in the ranking distribution against the top three reasons.

These results indicate that the email design needs to be improved to communicate more effectively the importance of resetting password in a timely manner (for instance, using visual design cues such as opinionated design [3]), and clearly convey the `identity theft` and `stealing information` risks associated with delaying password reset.

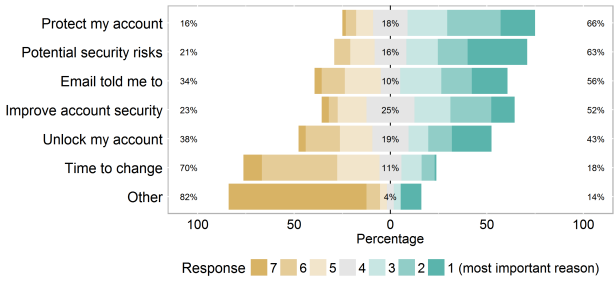

Figure 3. Reasons for *resetting* password.

Reasons for resetting password

To those who did reset their password, we asked *"Why did you reset your password after reading the email?"* We used the same option-ranking format as the previous ("reasons for not resetting") question. Figure 3 shows the reasons for resetting password, sorted based on the overall ranking distributions.

"To protect my LinkedIn account from being accessed by others" (`protect my account`) and *"I became aware of potential security risks associated with my LinkedIn account"* (`potential security risks`) were the top two reasons, showing that security was the top concern. `Protect my account` showed statistically significant superiority in the ranking distribution against *"To unlock my account and continue using LinkedIn"* (`unlock my account`), *"It was about time for me to change my password anyway"* (`time to change`), and `other` (all $p < 0.0005$, Bonferroni-corrected MW U test). `Potential security risks` showed statistically significant difference against `time to change` and `other` (all $p < 0.0001$, Bonferroni-corrected MW U test).

Password reset behaviors

To analyze the time it took for the participants to reset their password, we manually extracted the email received date from the two screenshots that the participants (those who reset password) uploaded. We subtracted the two dates to compute the elapsed time between when a participant first received the password reset email and when they signed into LinkedIn and reset password. Figure 4 shows the elapsed time, and the median and average values, which were 11.5 and 26.3 days (standard deviation of 33.3), respectively. The high variations indicate that some participants reset their passwords quickly – about 32% reset on the same day they received the email (this is only about 15% of all participants though) – whereas some participants took several days, weeks, or even months to reset their passwords. What is concerning is that 50% of those participants took 11.5 (median) or more days to reset their password. This demonstrates the timeliness issues of the password reset email as it has failed to convince those participants to quickly reset their password. To address this gap, we suggest sending another password reset reminder (e.g., after about 11 days) to those who have not yet reset their password.

We also asked *"How many other sites that you use have the same password as your LinkedIn password?"* and *"Among those sites that had the same password as your old LinkedIn*

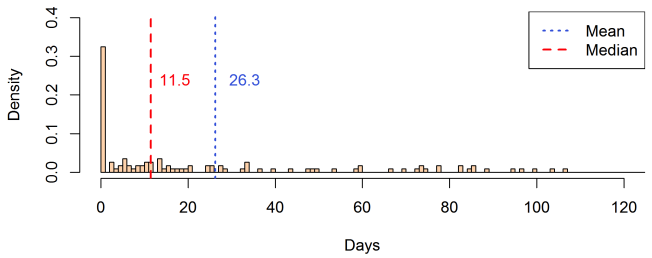

Figure 4. The number of days taken to reset password.

password, how many of those passwords did you also change after receiving the password reset email from LinkedIn?" Overall, about 46% of the participants said they use the same password on other 1-6 sites. About 4% responded that they use the same password on 7 or more sites. Considering that about half of the participants reused the same password, we argue that the risk of account compromise due to an attacker obtaining the password reset link (from a user's inbox) is real, and merely locking user account may not be sufficient. This further emphasizes the importance of persuading affected users to reset their password as soon as they check the email. Among those who reset their LinkedIn password, about 51% said they use the same password on 1-6 sites. But 67% (of that 51%) said they did not change their passwords on any of those 1-6 sites. Since any other account that uses the same password is also at risk (*and its account would not have been locked!*), the password reset email should inform users about such risks, and strongly recommend that users should also change passwords from other sites that use the same password.

We also asked those who reset password about how they created their new password. The proportion of each technique used are shown in Table 2. 46.02% indicated that they used their own method or process for generating new passwords, and 32.74% responded that they followed guidelines for creating strong passwords (e.g., using numbers or uppercase letters). What is worrying is that a significant proportion, 22.12%, indicated that they made small changes to their old, potentially compromised LinkedIn password. Adversaries could easily exploit this behavior, and try permutation guessing attacks based on the old LinkedIn passwords [11]. Another worrying observation is that the 17.70% answered that they simply reused a password from another site. Password reset mechanisms need to be designed to help users avoid making small changes to their old passwords and reusing passwords from other sites.

The results presented in Figure 4 measure the number of days taken to reset password from the date emails were first receieved, and not from the date they were first checked by the participants. Further, all of our MTurk workers were recruited from the United States. Hence, any generalization of the results presented in this paper needs to be performed with caution.

STEALING RESET LINKS WITH PHISHING ATTACKS

Recommending password reset or recovery through an email [6] is a commonly used security practice. Bonneau and Preibusch [1] reported that about 92% of 150 popular websites use an email-based solution, with 44% sending a reset link, 32% sending a new randomly-generated password, and 24% sending the original password. Furnell [5] explored password reset practices used in 10 popular websites (likes of Facebook and Google), and found that unique practice and policy was being used at each website. A user study conducted by Karlof et al. [8] showed that a phishing attack that tricks users into copying and pasting a password reset link has about 48% success rate – implying that the phishing attack we presented in "Introduction" can be highly successful against users who do not reset their passwords in a timely manner. Zhang et al. [11] showed that a changed (new) password can be effectively guessed from knowing the old password. 17% of the 7,700 new passwords were cracked within 5 guesses in an online attack. Chiasson et al. [2] formally quantified security advantages of a password expiration policy that forces users to change password within a fixed interval. Our results were consistent with the findings from [8], showing that the "passive warnings" provided in the reset email from LinkedIn were not sufficiently persuasive.

Table 2. Percentage of the techniques used upon resetting password. We allowed selection of multiple techniques.

Technique	Count	
I have my own method	52	(46.02%)
I followed the guidelines for creating strong passwords	37	(32.74%)
I made small changes to my old LinkedIn password	25	(22.12%)
I reused a password from another site	20	(17.70%)
I used a combination of words that are memorable	12	(10.62%)
I used memorable phrases or sentences	11	(9.73%)
I reused one of my old passwords	8	(7.08%)
I used a randomly generated password	8	(7.08%)
I used a password manager to automatically generate a password	6	(5.31%)
Other	1	(0.88%)

CONCLUSIONS AND FUTURE DIRECTIONS

Upon receiving a password reset email from LinkedIn, 47.79% of our study participants did not reset their passwords, indicating that they were simply "too busy." As for those who did reset their passwords, the mean time taken was 26.3 days. A significant proportion of the participants took several weeks or even months to reset their passwords. Those results suggest that the security practice of locking accounts and forcing password reset through emails, in the case of LinkedIn at least, failed to convince users to reset passwords in a timely manner. Password reset emails need to be improved to (i) better explain associated security risks, and (ii) better convey a sense of urgency and persuade users to immediately reset their passwords. We also recommend sending another reset reminder to those who have not yet reset their passwords. While creating a new password, users need to be provided with more security guidance so that they do not just make small changes to their old, potentially compromised passwords.

Acknowledgment

This work was supported by the ITRC (IITP-2016-R0992-16-1006), and the School of EECS at Oregon State University.

REFERENCES

1. Joseph Bonneau and Sören Preibusch. 2010. The Password Thicket: Technical and Market Failures in Human Authentication on the Web. In *Proceedings of the 9th Annual Workshop on the Economics of Information Security*.
2. Sonia Chiasson and P. C. van Oorschot. 2015. Quantifying the security advantage of password expiration policies. *Designs, Codes and Cryptography* 77, 2 (2015), 401–408.
3. Adrienne Porter Felt, Alex Ainslie, Robert W. Reeder, Sunny Consolvo, Somas Thyagaraja, Alan Bettes, Helen Harris, and Jeff Grimes. 2015. Improving SSL Warnings: Comprehension and Adherence. In *Proceedings of the 33rd Conference on Human Factors and Computing Systems*.
4. Dinei Florencio and Cormac Herley. 2007. A Large-scale Study of Web Password Habits. In *Proceedings of the 16th International Conference on World Wide Web*.
5. Steven Furnell. 2007. An assessment of website password practices. *Computers & Security* 26, 7–8 (2007), 445–451.
6. Simson L. Garfinkel. 2003. Email-Based Identification and Authentication: An Alternative to PKI? *IEEE Security and Privacy* 1, 6 (Nov. 2003), 20–26.
7. Patrick Heim. 2016. Resetting passwords to keep your files safe. https://blogs.dropbox.com/dropbox/2016/08/resetting-passwords-to-keep-your-files-safe/. (August 2016).
8. Chris Karlof, J. D. Tygar, and David Wagner. 2009. Conditioned-safe Ceremonies and a User Study of an Application to Web Authentication. In *Proceedings of the 16th Network and Distributed System Security Symposium*.
9. Simon Marechal. 2008. Advances in password cracking. *Journal in Computer Virology* 4, 1 (2008), 73–81.
10. Cory Scott. 2016. Protecting Our Members. https://blog.linkedin.com/2016/05/18/protecting-our-members. (May 2016).
11. Yinqian Zhang, Fabian Monrose, and Michael K. Reiter. 2010. The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis. In *Proceedings of the 17th ACM Conference on Computer and Communications Security*.