**“What was that site doing with my Facebook password?”   
Designing Password-Reuse Notifications**

|  |  |  |
| --- | --- | --- |
| Maximilian Golla  Ruhr University Bochum  maximilian.golla@rub.de  Miranda Wei  University of Chicago  weim@uchicago.edu | Lydia Filipe  University of Chicago  lydiafilipe@uchicago.edu  Markus Dürmuth  Ruhr University Bochum  markus.duermuth@rub.de  Juliette Hainline  University of Chicago  juliettehainline@uchicago.edu | Elissa Redmiles  University of Maryland  eredmiles@cs.umd.edu  Blase Ur  University of Chicago  blase@uchicago.edu |

A S M Nazrul Islam  
1018312016  
Institute of Information and Communication Technology (IICT), BUET

The titled paper focused on the content and effectiveness of the prevailing **password reuse notifications** and discussed best practices for password-reuse notifications and necessity of other ways in password reuse.

According to the paper, they are the first one to conduct this type of study on password reuse notifications and paved way for further research in this area.

With the advancement of technology and necessity, people maintain multiple of online accounts in multiple platforms. But, in most of the cases, these completely different multiple accounts have same or almost same login credentials, especially passwords. Due to low adoption of password managers and single sign-on systems, password reuse is a common strategy to attain ease of access.

In this paper, the authors at first tried to comprehend the vulnerabilities of password reuse. How attackers can exploit a compromised password and endanger other online accounts having the same or more or less same password. Then the authors conducted two studies to check the users’ response and efficacy of the password reuse notifications.

In study one, the authors studied the content of the prevailed password-reuse notifications provided by the active account providers and monitored the response of the users on those notifications. With the help of a fictitious company named Aceme Co., they used one of the six representative notifications on 180 users. Surprisingly, the outcome was- only less than a third of respondents reported intentions to change any passwords. The authors characterized the structure of the notifications as the cause of this low rate of success.

And in study two, they developed **five notification goals** for password-reuse scenario, by synthesizing results from study one. 588 participants were watched one of 15 variations on a model notification. Though **90%** of them intended to change the passwords, but only **2%** of them actually willed to set a new password. While 13% of them reused the previous password and 68% of them modified the previous password.

Based on the studies, the authors suggested some best practices for password reuse notification, like, to send the notification via email or via more conveniently immediate channel, to name password reuse as the root cause in the sent notification, to force password reset, to encourage 2FA and password managers and to suggest unique passwords in the notification. They also directed to find ecosystem-level solutions regarding this matter.

**Comments**

As a novel work, the authors of this paper did an incredible job by introducing this concept in research area. The introduction and background sections of the paper give well description of the concept and provide a reader an appreciation of the necessity to look on this matter.

To get into the depth of the problem, the authors have studied the prevailing notification systems rigorously. They have conducted studies to comprehend the users’ perception on password-reuse notifications.

Based on the findings of the first study, they identified the factors that could play important roles to ameliorate the prevailing condition. Keeping in mind those factors, they modulated a standard form of notification to send to the users.

They studied the real life persons to check their reactions and actions on getting password-reuse notifications. However, they only considered persons of a specific profession. If, their test subjects were comprised of persons from multitude of profession, then the findings might become more empirical.

They also proposed some ways on how to construct and send notifications to the users more promptly, conveniently with efficacy. And, they hinted directions for future research by mentioning to find ecosystem-level solutions.

Overall, this paper has enriched the field of cyber-security by introducing a concept that has been agitating many of us and by pointing out why and how it should be given much attention.