Towards Building a Support System for User Security Awareness

Faqia Iqbal *LUMS*
Saad Jamal *LUMS*
Shaarif Sajid *LUMS*
Shoaib Asif Qazi *LUMS*
Mobin Javed *LUMS*

Users time and again take security risks in spite of warnings because they are either not aware of the possible repercussions of their actions, or think the utility is worth the risk. A fundamental problem that feeds this behavior is that users do not receive any feedback *at a later point in time* on how they are doing from a security point of view. A mistake once committed disappears into ether, and the user never learns from it.

While there are a number of tools and plugins to help protect users, our study of 19 such popular tools revealed a major gap: none of the existing tools gives users an option to review their activity at a later time and learn from their mistakes. Almost every tool displays an on-the-spot warning, but the absence of a delayed feedback makes it hard for users to track and improve their behavior.

We hypothesize that given the right support system, the users can, in fact, be trained to care about security and privacy decisions. We investigate the design of a support system that will enable users to monitor their security behavior over time. We aim to achieve this by monitoring and recording the users' actions and critical decisions (for example entering credentials) and presenting them with the picture of the right and wrong moves they make. A key difference from existing tools is a summary review and analysis of user actions, accessible at various time granularities (i.e, daily, weekly).

To elaborate on this further, Figure 1 shows an example interface of our feedback application. The app summarizes the information from a corresponding browser plugin installed on a user machine. The user can see a weekly review of her browsing behavior: she visited 127 websites during the week. The browser presented a malicious warning for three sites, for two of which the user proceeded to the site despite the warning. The user also created an account on one site and re-used one of her existing account's passwords. Finally, she did not lose any credentials to two of the phishing websites she visited.

However, presenting users with a review of their behavior is only useful if the users are interested in the first

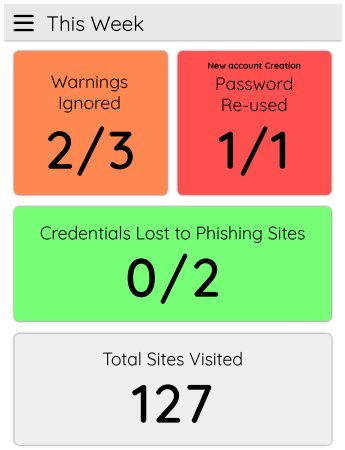

Figure 1: Example weekly review of user actions.

place, and if they understand the risks. To tackle the challenge of engaging the users, the framework will incorporate an incentive structure to help users stay committed to improving their security behavior. In this context, we aim to explore gamification techniques, such as avatars that give feedback in the form of encouragement and penalties. Similarly, we aim to explore the effectiveness of incorporating users' social network to introduce a point-scoring system and relative ranking with their friends.

The research questions that we aim to answer include:

(i) a pilot user study to understand: (a) how effective the proposed feedback will be in encouraging users to adopt security best practices, and (b) what are effective models for goal setting and sustained learning.

(ii) a framework for instrumenting critical online user decisions as well as models and meters for assessing the right and wrong moves for each action. Here we build upon previous research (for e.g., password strength meters) and existing tools (such as leveraging indicators of a site's maliciousness from Google Safe Browsing).

(iii) effectiveness of gamification techniques and time-shifted feedback in incentivizing users to take control of their security and privacy behaviors.