Where You're Logged In: Analyzing the Usability of Device Activity Pages (Work-in-Progress)

Angel N. Fernandes
University of Denver

Philipp Markert
Ruhr University Bochum

Sanchari Das
University of Denver

1 INTRODUCTION

Account Remediation is a systematic process to re-secure a compromised account or provide security to the account from a proactive defensive mechanism perspective. This remediation process consists of five phases [1]: (1) discover the compromise by noticing suspicious activity, (2) recover access to the account if it was lost or compromised, (3) limit access to the account to prevent unauthorized access, (4) restore the service of the account to its pre-compromised state, and (5) secure the security of the account to prevent future compromises. Web services provide users with advice for account remediation through help pages. However, account remediation is a technically complex process and advice differs drastically among web services in terms of completeness [1, 2]. Incomplete account remediation advice does not fully help re-secure a compromised account. Therefore, investigating the quality of the 'Security and Privacy' part of any web page is critically important and serves as our main research agenda.

2 MOTIVATION

This research focuses on the first account remediation phase, which requires users to discover the compromise. We do this by focusing on the device activity pages. These pages display all devices on which the user is logged in and are one of the primary ways to detect potentially malicious sessions in case of a compromise. As an entry point to this research, we analyzed the device activity pages of 10 popular websites: Adobe, Facebook, GitHub, Google, LinkedIn, Microsoft, Netflix, Pinterest, Twitter, and Yahoo. We did this to find commonalities and differences between the websites' device activity pages. Table 1 gives an overview of the analysis regarding the available information. As can be seen, there are no two pages with the same amount of information. This raises the question of what type of information actually needs to be present to enable users to make informed decisions when asked to tell legit and malicious sessions apart.

3 OUTLOOK

To answer the depicted question, we prepared an in-lab user study to analyze the interaction with the device activity pages. The study consists of two phases, the interaction with the device activity page and a subsequent survey. For the interaction, we first instruct participants to download the source code of one of their real-world device activity pages. We then use the source code to duplicate the page, which enables us also to include new sessions in the original list. We have investigated users' login sessions, blocked other functionalities the page had, and cloned the websites. As a first step for the websites, we focused only on the "Security and Privacy" page, which displayed the user activity sessions. After completing this initial step, we duplicated the HTML pages of the other six websites (Microsoft, GitHub, Adobe, Yahoo, Pinterest, and Netflix) to create a simulation. We insert different types of sessions, ranging from potentially easy-to-detect ones by deviating substantially from all previous sessions to others harder to detect by only changing the browser or the operating system. Afterward, participants are asked to interact with the duplicated page and also challenged to identify any unrecognized activities. In the subsequent survey, we will further ask participants about their interaction with the page, their approach to detecting malicious logins, and their overall impression. By combining survey results and the data from the interaction with the device activity page, we intend to understand better how users interact with these pages, which information helps them to tell legit and malicious logins apart, and ultimately improve the design of device activity pages.

REFERENCES

[1] Lorenzo Neil, Elijah Bouma-Sims, Evan Lafontaine, Yasemin Acar, and Bradley Reaves. 2021. Investigating Web Service Account Remediation Advice. In *Symposium on Usable Privacy and Security (SOUPS '21)*. USENIX, Virtual Conference, 359–376.

[2] Kathryn Walsh, Faiza Tazi, Philipp Markert, and Sanchari Das. 2021. My Account Is Compromised – What Do I Do? Towards an Intercultural Analysis of Account Remediation for Websites. In *Workshop on Inclusive Privacy and Security (WIPS '21)*. USENIX, Virtual Conference, 1–6.

Table 1: Information contained on the 10 analyzed device activity pages.

	Adobe	Facebook	GitHub	Google	LinkedIn	Microsoft	Netflix	Pinterest	Twitter	Yahoo
Browser	●	●	●	●	●	●	○	○	○	○
Country	●	●	●	●	●	○	●	●	○	○
State	○	●	●	●	●	○	○	○	●	○
City	●	●	●	●	●	○	●	●	●	○
Date	●	●	●	●	●	●	●	●	●	●
Time	○	●	○	○	○	○	●	●	●	○
Device	○	●	●	●	○	○	●	●	●	○
Graphics	○	●	●	●	○	●	○	○	●	○
Hidden Sessions	○	○	○	○	○	●	○	○	○	○
IP Address	○	●	●	○	●	●	●	●	○	●
Network Owner	○	○	○	○	●	●	○	○	○	●
Operating System	●	●	●	●	●	●	○	●	●	●