ReSecure+ Your Passwords: Designing a Chrome Extension for Context-Aware, Real-Time Interventions to Combat Password Reuse and Improve Security

Lukas Mecke
LMU Munich

David Neubauer
LMU Munich

Oliver Hein
University of the Bundeswehr Munich

Florian Alt
LMU Munich

Abstract

ReSecure+ is a browser-based prototype that explores how context-aware security interventions can address password reuse and weak passwords during everyday web use. Rather than focusing on password management in isolation, the extension delivers in-context warnings when users interact with vulnerable accounts, translating insights from prior usable security research and expert interviews into a concrete design. We present ReSecure+ as a work in progress and boundary object for discussion, highlighting open design questions and trade-offs around trust, habituation, and effective intervention strategies. We look forward to discussing with the community how context-aware password security systems should be designed and evaluated in realistic browsing environments.

1 Introduction

Password reuse and the use of weak passwords present a critical security vulnerability affecting individuals and organizations worldwide. Weak passwords can be compromised through dictionary attacks or brute-force guessing, while credentials exposed in a breach of a single service may subsequently be reused in so-called credential stuffing attacks against other accounts. Despite this risk, weak and reused passwords are still widespread due to users' limited knowledge of where passwords are reused and the difficulty of managing unique passwords for many services. Password managers can store credentials and alert users when passwords have been compromised. However, notifications often arrive too late to prevent damage, and research shows that users rarely change passwords without external prompts or situational motivation [5]. This highlights the need for proactive interventions that encourage users to update passwords before breaches occur.

More broadly, prior work on security warnings demonstrates that effectiveness is strongly influenced by timing, framing, and presentation [7]. Users often misunderstand the risks of password reuse and cross-site compromise propagation [2], while poorly timed or overly technical warnings can contribute to habituation and dismissal. In contrast, persuasive and clearly framed messages, combined with actionable guidance and progressive disclosure, can improve user engagement with security interventions [2–4] if they are aligned with users' context and cognitive state [1].

Based on this prior work and expert interviews, we introduce *ReSecure+* (see Fig.1), a Chrome-based prototype that explores how context-aware security warnings can be integrated into everyday browsing. Rather than replacing existing password managers, ReSecure+ builds on them by showing contextual information about password reuse and weakness when users interact with affected accounts. Existing research has demonstrated the technical feasibility of detecting password reuse and compromised credentials in context [6, 8]. Our work extends this direction by focusing more strongly on how such information should be presented to end users in real browsing workflows. By building a functional prototype, we make design trade-offs tangible and invite discussion around in-context password security intervention design.

2 Expert Interviews

We recruited two senior usable security and HCI researchers for semi-structured interviews. They reviewed five mockup designs based on the literature (see Apendix A) and were asked to reflect on notification timing, visibility, usability, and behavioral impact. We transcribed the interviews and two researchers independently applied open coding. Disagreements were resolved through discussion, resulting in three themes.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2024.
August 11–13, 2024, Philadelphia, PA, United States.

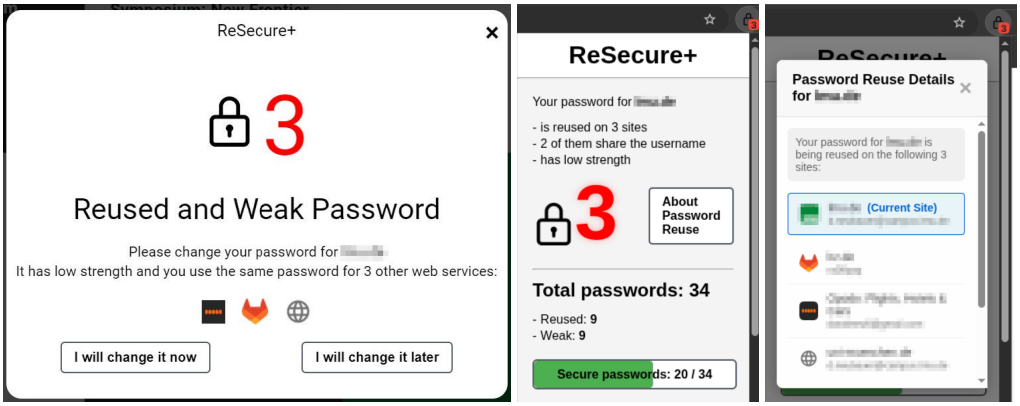


Figure 1: We propose *ReSecure+*, a browser extension that can display blocking warnings upon visiting a webpage with a weak or reused password (left). It offers a dashboard on overall security status (center) and provides details on demand (right).

Trust and Credibility. The experts emphasized that notifications could not risk revealing sensitive information and the importance of consistency to establish legitimacy and trust.

Engagement and Usability. We observed a key tension between intrusive warnings that force engagement and subtle cues that risk being ignored. The experts favored contextually timed notifications, optional deferral, and minimal animations to attract attention without being disruptive.

Motivation and Behavioral Change. Experts agreed that users needed actionable feedback and positive reinforcement. Password generators, progress indicators, and affirmative feedback were seen as effective, while overly ambitious goals and frequent interruptions would risk notification fatigue.

3 Prototype: ReSecure+ Browser Extension

Based on related work and the findings of our exploratory interviews, we implemented *ReSecure+* as a Chrome extension that delivers in-context password security guidance.

The core component is a dashboard that summarizes password security for the currently visited site at a glance. The popup uses a small set of visual indicators (e.g., severity colors and counters, see Fig. 1 center) and reveals details on demand (e.g., affected accounts, see Fig. 1 right), mirroring layered warning recommendations from related work [4].

ReSecure+ combines three warning modalities, each triggered under specific conditions. *Small bar warnings* appear with a sliding animation at the top of visited pages when a site is associated with a weak or reused password. They use color-coded severity cues and serve as the default, low-intrusion reminder. *Large modal warnings* are designed to force attention, but only appear after repeated exposure to small warnings and no more than once a day and domain. The warning presents a full-screen overlay with detailed explanations, affected account counts, and explicit options for action (see Fig. 1 left). Finally, *password creation warnings* appear directly adjacent to password input fields during account registration or password changes, offering just-in-time guidance on password strength. These warnings are complemented by persistent toolbar badges that signal risk without interruption.

Password metadata (reuse groups and weakness flags) is obtained through a user-initiated import from Google Password Manager's password checkup page, thus the extension has at no point access to actual passwords.

4 Discussion

We present *ReSecure+* as an ongoing design exploration informed by literature and expert interviews rather than a finalized system to share early insights and invite discussion around key design tensions and evaluation challenges.

Prior work highlights the value of contextual security interventions, but few systems demonstrate how such warnings can be integrated into everyday browsing. We explore this design space by embedding password reuse and strength warnings directly into account interactions. We addressed tensions between visibility and disruption through a progressive notification strategy, while addressing trust and privacy concerns through restrained messaging and careful design choices. Finally, we incorporate lightweight motivational and guidance elements to support users at the moment of decision.

5 Conclusion

We presented ReSecure+, a prototype exploring context-aware password security interventions for everyday browsing. Grounded in prior research and expert interviews, we propose a concrete approach to balancing timing, intrusiveness, and user motivation when addressing password reuse. While user evaluation remains future work, we hope this work provides a basis for discussing design trade-offs and future directions for in-context security interventions.

References

[1] Piotr D. Adamczyk and Brian P. Bailey. If not now, when? the effects of interruption at different moments within task execution. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '04, page 271–278, New York, NY, USA, 2004. Association for Computing Machinery.

[2] Maximilian Golla, Miranda Wei, Juliette Hainline, Lydia Filipe, Markus Dürmuth, Elissa Redmiles, and Blase Ur. "what was that site doing with my facebook password?": Designing password-reuse notifications. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, page 1549–1566, New York, NY, USA, 2018. Association for Computing Machinery.

[3] Marian Harbach, Sascha Fahl, Polina Yakovleva, and Matthew Smith. Sorry, i don't get it: An analysis of warning message texts. In Andrew A. Adams, Michael Brenner, and Matthew Smith, editors, *Financial Cryptography and Data Security*, pages 94–111, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[4] Yue Huang, Borke Obada-Obieh, and Konstantin Beznosov. Users' perceptions of chrome compromised credential notification. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 155–174, Boston, MA, August 2022. USENIX Association.

[5] Sanam Ghorbani Lyastani, Michael Schilling, Sascha Fahl, Michael Backes, and Sven Bugiel. Better managed than memorized? studying the impact of managers on password strength and reuse. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 203–220, Baltimore, MD, August 2018. USENIX Association.

[6] Kurt Thomas, Jennifer Pullman, Kevin Yeo, Ananth Raghunathan, Patrick Gage Kelley, Luca Invernizzi, Borbala Benko, Tadek Pietraszek, Sarvar Patel, Dan Boneh, and Elie Bursztein. Protecting accounts from credential stuffing with password breach alerting. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 1556–1571, Santa Clara, CA, August 2019. USENIX Association.

[7] Anthony Vance, Jeffrey L. Jenkins, Bonnie Brinton Anderson, Daniel K. Bjornn, and C. Brock Kirwan. Tuning out security warnings: A longitudinal examination of habituation through fmri, eye tracking, and field experiments1. *Management Information Systems Quarterly*, 42(2):355–380, 06 2018.

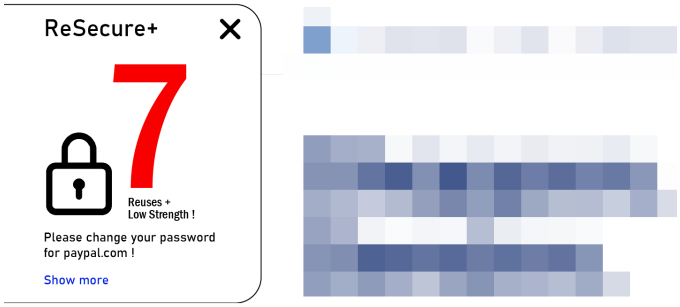
[8] Ke Coby Wang and Michael K. Reiter. How to end password reuse on the web. In *Proceedings 2019 Network and Distributed System Security Symposium*, NDSS 2019. Internet Society, 2019.

A Design Prototypes

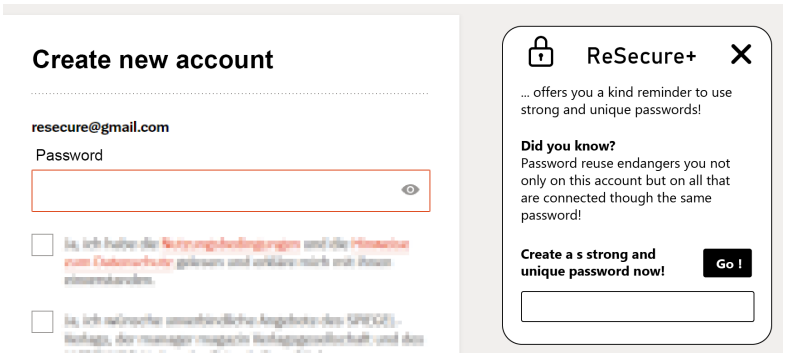
Overview of the design prototypes presented in the expert interviews to gather feedback: (a) A persistent notification bar at the top of the page, (b) a semi-transparent overlay that blocks interaction and presents a detailed warning dialog with optional educational links, (c) a compact, non-blocking notification near the page content, displaying a visual indicator of password risk with an option to expand for details, (d) a context-sensitive prompt directly next to password fields, reminding users to choose strong and unique passwords and (e) a compact extension popup that presents page-specific password security feedback alongside a high-level overview of the user's overall password health.

(a) Bar notification

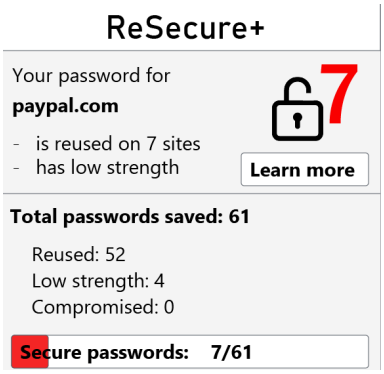
(b) Fullscreen Overlay



(c) Contextual Icon



(d) Password Entry



(e) Security Status Overview