

1

Introduction

We have become accustomed to using multiple passwords every day: We enter a four-digit PIN to unlock our phone to check incoming messages even before breakfast. Paywalls shield the news of the day, so they force us to log into our favorite news website before we can read them during our commute. Once arrived at work, our fingers automatically type the password to unlock the computer. A colleague requests access to a client's platform, so we write down the credentials or share them via a password manager that itself is password protected. When we come home, we find the kids have used the family tablet to log into their social media accounts, so we need to re-authenticate if we want to check our own. Interacting with systems relying on password authentication has become ubiquitous, and we merely carry out the task. Passwords are the de facto standard when it comes to controlling access to resources on the Internet. While it may seem straightforward to deal with passwords because we are so acquainted with them, there is a wide range of problems they entail: The phone requests the PIN whenever we take it out of our pocket, so we spend considerable time per day authenticating [154]. The news website informs us that our password has expired, so we need to pick a new one that is not part of the ones we had used before. The work PC requires not only our credentials but also a one-time password that our phone generates for us every sixty seconds. At one point, the colleague leaves the company, so we have to request a new set of credentials from the client to maintain confidentiality. And the kids used the tablet at home to shop online because we had stored the password in the browser for convenience. So, we delete the stored password but fail to recall it a week later, because we had not typed it for a very long time. These and other situations lead to users feeling a considerable burden generated by password authentication.

1.1 The State of the World

In a wide sense, password authentication encompasses digit-only personal identification numbers (PINs), graphical schemes like the Android screen lock pattern (see Section 2.5.1),

and alphanumeric passwords consisting of letters and digits. Throughout this thesis, however, we focus on the latter because they still are the go-to method on the Internet: In 2007, users had around 25 accounts and roughly six distinct passwords on average [111], while more recent numbers suggest that users keep twelve unique passwords for different purposes [359]. With the growing number of accounts the issues around passwords amplify: users pick weak passwords, write them down in unprotected locations, reuse many of them, forget the exotic ones, and share credentials with other people [312]. These behaviors are referred to as *password coping strategies*.

Combating the risks entailed by these issues, researchers and practitioners have developed numerous approaches to support users in password authentication. Four central themes have emerged in their efforts: education, enforcement, assistance, and persuasion.

Education

Weak password practices were attributed to a lack of understanding of their consequences for the longest time [272]. Thus, first approaches to mitigate the situation leaned on educating users through trainings, and textual instructions [161]. Explaining all risks and defense strategies to users in lengthy prose is doomed to fail, because password security is a secondary goal that is dominated by a primary task, e.g., reading emails [367]. Nevertheless, carefully crafted advice and explanations may be a viable strategy for those who actively seek information [273, 337].

Enforcement

Since the inception of passwords in the 1960s, users have tried to create memorable passwords that are often based on simple dictionary words. To combat low complexity, enforcing password rules through policies is commonplace. Passwords must then meet length and complexity requirements, e.g., a certain number of uppercase letters, digits, or symbols. The choice of a specific policy is not trivial for service providers, and many organizations make poor tradeoffs [112, 291]. The plethora of policies even fosters insecure password practices, because users try to find easy ways to comply with the rules, which they do in very predictable ways [171, 198, 341].

Assistance

Users have to deal with a high number of passwords that also interfere with each other, so people reuse passwords and write them down on paper or digital files. To lower the risks entailed by these coping strategies, assistive tools like password managers (PWMs) and password generators automate certain interactions to boost both security and usability. However, they come at a price, e.g., lock-in effects to a particular vendor that make it difficult to move to a different tool in the future. Thus, many users rationally refrain from adopting them [64].

Persuasion

Finally, the youngest strategy to support users in password authentication is based on principles of *persuasive technology*. Fogg defined this paradigm as “any interactive computing system designed to change people’s attitudes and behaviors” [119, p. 1]. While assistive systems also often meet that particular goal, persuasive technology tries to create sustainable impact even when the assistive trigger is absent. Therefore, such interventions often come as *behavior-change support system* [123]. In the realm of authentication, password meters are the most representative form of persuasive interventions. Those user interface (UI) elements often appear on registration pages of web services, and give feedback on the strength of a user-selected password. They often implement various *nudges*, i.e. small, transparent attempts to change behaviors [328, p. 4], to convince the user to pick a more suitable password. The user stays in control and is free to *live on* without following the advice. Overcoming inertia is perhaps the biggest challenge in the design of persuasive password support. So far, the use of nudges has shown mixed results in empirical research [99, 263, 337], and the spectrum of persuasive interventions in the wild is fairly narrow.

1.2 Problem Statement and Research Objectives

Password-related challenges and risks for the users are at the heart of this dissertation. The balance between usability and security, especially for passwords, has been under investigation for several decades. This allows us to observe tectonic shifts in the hassles that users have to bear. The notion of the inconsiderate user, who is the “weakest link” in the authentication chain and notoriously refuses security measures, has started to crumble: There is considerable evidence that many users want more control over their security and that they are willing to sacrifice usability for it [190]. This might not even be necessary, or lie in their best interest, which I illustrate below.

1.2.1 Balancing the Costs

Changing the status quo of the authentication world can be seen as a game-theoretic problem [35]. It involves risks and opportunities that need to be balanced in terms of their costs for different “players”.

Maintaining Usable Password Practices

Fortunately, the costs of being attacked remain hypothetical for many users [163]. However, there is a growing number of people who have experienced an attack with all its consequences to resolve and recover the damage [45]. First, usable but risky password practices, like excessive reuse and obvious password choices, can cause financial losses for end-users. For instance, an attacker who manages to impersonate a user might be able to withdraw

money from bank accounts. At the moment, attacks on digital wallets containing cryptocurrency are highly lucrative, so protecting these assets with strong passwords is vital¹. Herley et al. noted that “*money is the most obvious loss, but time, frustration and reputation are also at stake*” [164], let alone the emotional distress [292]. Accounts that have a weak password are more likely to be hijacked [354], and it often takes victims painful effort to recover from identity theft². Although social engineering, where an attacker lures people into forfeiting their credentials, is a central threat for companies, the employees’ overall password practices still generate considerable financial losses³.

Striving for Stronger Password Practices

Solving the problems raised by passwords, we also need to consider the other end of the security-usability spectrum. Moving to strong password practices often inflates usability challenges for users that are largely neglected by security experts. For instance, typing an overly complex password takes long and is error prone [295]. Such passwords are especially tedious to enter on mobile phones or devices that were not originally designed for text input, e.g., smart TV sets [229]. Moreover, most people are incapable of creating and memorizing a strong, unique password for every single account on their own. So, it is unrealistic to expect that they will do so without the use of external aids like handwritten notes or password managers. The cost of using such methods is a dependency on the tools that users did not ask for in the first place. In any case, strong passwords are no panacea in boosting online security. They do not stand a chance in fending off social engineering attacks where the victim unwillingly surrenders the password in plain text. In an effort to alleviate the risks of unknowingly forfeited credentials, service providers often require users to reset passwords after a given period. Such expiration policies are rather ineffective [53] and responsible for many support desk calls, whose resolutions are costly [3, 273].

1.2.2 The Challenge: Improving an Innately Annoying Interaction

Passwords are annoying for users, and as we can see above, there is no easy solution to alleviate this situation. It is impossible to remove all usability pain points [34]. Yet, no alternative can fully replace passwords, either (see Section 2.5). Thus, Herley and Van Oorschot point out that “*supporting passwords better is a vast opportunity for improvement*” [164], because making even a small change can have an impact on **so** many users.

¹ <https://blog.dashlane.com/cryptocurrency-exchange-password-power-rankings-2018/> (last accessed 24.03.2018)

² <https://www.businesswire.com/news/home/20151006006149/en/Latest-Data-Breach-Spotlights-Identity-Restoration> (last accessed 11.01.2018)

³ <https://www.helpnetsecurity.com/2017/09/19/infosec-weakest-links/> (last accessed 09.04.2018)

So far, persuasive strategies have produced mixed results regarding their efficacy in supporting users with passwords. This could be due to several issues: Mental models and coping strategies evolve over time [312, 348], which has seen little attention in the design of persuasive interventions. Much of the past research dealt with one-shot triggers in isolation, but many context factors and costs for different stakeholders were left out. In an analogy to the design principle “form follows function”, a better understanding of the functions of user support can help design assistive and persuasive solutions (the form). Moreover, many highly effective nudges from other domains have not been adapted for password support, so we simply may not have discovered the best intervention, yet. However, since nudging strategies are nuanced, we need a structured exploration of how we can bring them to password authentication to remove its most important pain points.

1.2.3 Research Questions

In this thesis, I take a holistic approach to address the problem of providing users with the right support in their password practices. To accomplish this, the research presented here tries to answer the following questions:

- RQ1** What is the role of psychological factors and mental models for password selection and coping strategies?
- RQ2** How can password authentication be simplified for users?
- RQ3** How can we design persuasive strategies to support users in any password-related tasks?

1.3 Main Contributions

As highlighted above, several aspects of password support have been left out in the literature, although there are many reasons to consider their importance. First and foremost, a broader understanding of contextual factors that contribute to the formation of specific coping strategies is necessary to improve password support. The primary goal of this thesis is to provide this understanding on a fundamental level by exploring existing factors and addressing them with persuasive designs. The solutions include new paradigms for the design of persuasive interventions.

Insights into Context Factors of Password Practices

Researchers seem to have reached consensus that the context in which a password goes through its life-cycle [312] is an exploratory variable for users’ practices. However, contextual factors have merely been addressed in the discussions of empirical findings. Only a few studies specifically correlated users’ backgrounds to their password practices (e.g.

[190, 224]) and they mostly focused on demographic factors. We contribute several insights that enrich the understanding of a wide range of context factors. Specifically, we address how users' mental models are associated with their password practices. We do this through a novel method to study mental models in-the wild with the aid of a game. Moreover, we are the first to thoroughly investigate the interconnection between personality traits and password authentication. The insights gathered through three online studies revealed interesting associations between personality, attitudes, and behaviors regarding passwords. Lastly, we performed an extensive audit of the real-world constraints that form the context for password reuse. All these insights shape our understanding of the problem space as the foundation for persuasive interventions.

Investigation of Persuasive Strategies

With the context factors in mind, we extended the range of persuasive design strategies. As a starting point, we investigated users' explicit and implicit needs in password feedback. From this exploration, we contribute the “*show-explain-help-empower*” paradigm that serves as a heuristic for persuasive password assistance. We followed this up with two studies that were carried out both in the lab and in the field: The first study was the first of its kind to evaluate the Decoy effect for choice architectures in password authentication. Here we learned important lessons about the interplay between feedback and feedforward, and about the role of simplification in persuasion. The second study was focused on empowerment. We evaluated different dimensions of usability of emojis inside text-based passwords. The study delivers timely insights, because an increasing number of web-services enable users to pick such emoji-passwords and there are some issues that need attention from the very start.

A Structured Process for the Design of Persuasive Password Support

Finally, the exploration of the context factors, and the design studies on persuasive assistance in password authentication are melted into a framework for structuring future design processes in this domain. I contribute the Persuasive Design for Password Support (P4P) framework. It respects the dynamism of the status quo, aids in finding the right interventions, and implementing them successfully. At that end, we present a design exercise that demonstrates how the P4P framework can be used.

1.4 Thesis Structure

This dissertation encompasses four major parts that unravel the different aspects of persuasive password support. I chose to structure the content in fourteen self-contained chapters. Although they do follow a narrative, it is possible to read them in any order by following the provided cross-references for the necessary background information. Part I is an exhaustive overview over the related work that serves as the basis for all the discussions in later parts. In Part II, I report on empirical research exploring the various context factors of password

selection and coping strategies. Part III then shows how these factors helped to craft novel persuasive design strategies. Lastly, Part IV establishes a research and design framework, and concludes with a reflection on the gained insights and future work. In the following, I highlight the contents of the individual chapters with the questions they try to answer.

Part I: Foundations of Usable Authentication

Chapter 2: Foundations This chapter provides an overview of password-based authentication from a system-perspective. Questions answered:

- How has password authentication evolved over time?
- What benefits, drawbacks, and threats do passwords entail?
- What is a strong, what is a weak password?
- Why do we still need passwords when there are more advanced schemes?

Chapter 3: Human Factors I describe the method space to study passwords, before discussing findings about users' password practices. The chapter also highlights the central approaches that have been implemented to mitigate security risks on the user side. Questions answered:

- How do we conduct valid research on passwords with humans and ethics in mind?
- How do users cope with passwords? What makes their practices particularly risky?
- What can we do to steer people away from risky behavior?

Chapter 4: Related Work Summary This chapter describes the status quo of password authentication and highlights ill-defined aspects that warrant further research.

Part II: Exploring the Context Factors

Chapter 5: Mental Models of Password Strength We present a novel approach to study the perception of password strength: PASDJO, the password game. A longitudinal field study aimed to quantify common misconceptions about the benefits of password complexity, which are an underlying context factor for password practices. Questions answered:

- How well can users gauge password strength?
- Do we have to update our views on users' capabilities?
- Is a game suitable to collect the necessary data?
- How effective is the game to educate users?

Chapter 6: Policies and Reuse This chapter reports on a thorough audit of the password policies of the most-visited websites in Germany. It explains external context factors that shape password reuse in the real world. Questions answered:

- How consistent are password policies in the wild?
- Is it possible to find a password that meets all requirements at once?

Chapter 7: Personality in Password Practices This chapter presents three empirical studies about the role of personality traits in password practices. In particular, we shed light on the psychometric context factors for the usability of policies, mental models of password strength, and password selection behavior. Questions answered:

- Is personality associated with password practices, attitudes, and behaviors?
- How well can we model such associations?
- What are the specific implications on the design of personalized password support?

Chapter 8: Mental Models of Password Managers We present a qualitative user study eliciting the users' motivations to either adopt or dismiss password managers. A fine-grained mental model is established to depict biases as context factors. Questions answered:

- Why are people (not) using password managers?
- How do they make sense of their functionality?

Part III: Persuasive Design Strategies

Chapter 9: Feedback Requirements This chapter presents two studies on users' explicit and implicit expectations around password feedback. We derive a paradigm for persuasive password support. Questions answered:

- What are users' needs in persuasive feedback?
- How would they design a feedback system?

Chapter 10: The Decoy Effect We carefully craft a choice-architecture for password support and explore a marketing phenomenon as nudging strategy. The chapter reports on an online study and highlights the interconnection between feedback and feedforward. Questions answered:

- Does the decoy effect work to make stronger passwords more attractive?
- How effective is feed-forward in combination with feedback?

Chapter 11: Emoji-passwords This chapter presents emoji-passwords as an approach to simplify memorization in persuasive ways. We investigate different facets of usability and report on a mixed-methods study. Questions answered:


- How usable are emoji-passwords?
- What are the risks and potentials of emoji-passwords?
- How do platform-dependent differences affect memorability?


Part IV: Synthesis

Chapter 12: P4P Framework This chapter synthesizes the insights from the first three parts to establish a new framework for the design of persuasive password support. Through a design exercise, I show how it can be applied to develop a novel password manager. Questions answered:

- How can we design persuasive password support in a structured way?
- How do we practically apply the framework?

Chapter 13: Summary In this chapter, I reflect on the presented research and draw conclusions. The contributions are summarized, and contrasted by the limitations of the methodology. I provide eight meta recommendations for future design work. Questions answered:

- What have we learned?
- What are the implications and limitations?
-  Where do we need to consider in the future?

Chapter 14: The End In the final chapter of this thesis I present open research topics and show their potentials. The dissertation concludes with a reflection  the role of password-authentication in the present and the future. Questions answered:

- What research topics have been opened up by this thesis?
- What needs to change still to make users' authentication practices easier?

1.5 Style Choices

Singular They: Throughout this dissertation pronouns are used in the plural although speaking about an individual, e.g. “the user” is mostly referred to as “they” instead of “he” or “she”, to avoid discrimination of certain demographic groups.

Plurals: As is common in HCI literature, the author utilizes “We” instead of “I” to acknowledge the work of collaborators. In later more opinionated parts, the explicit usage of “I” intends to communicate the subjective nature of thoughts and interpretations.

Footnotes: Throughout the thesis, footnotes are excessively used to link to web content. Publications in scientific archives appear in the list of references at the end of the thesis.