Driving 2FA Adoption at Scale: Optimizing Two-Factor Authentication Notification Design Patterns

Maximilian Golla, *Max Planck Institute for Security and Privacy;* Grant Ho, *University of California San Diego;* Marika Lohmus, *Cleo AI;* Monica Pulluri, *Facebook;* Elissa M. Redmiles, *Max Planck Institute for Software Systems*

https://www.usenix.org/conference/usenixsecurity21/presentation/golla

This paper is included in the Proceedings of the 30th USENIX Security Symposium.

August 11–13, 2021

978-1-939133-24-3

Open access to the Proceedings of the 30th USENIX Security Symposium is sponsored by USENIX.

Driving 2FA Adoption at Scale: Optimizing Two-Factor Authentication Notification Design Patterns

Maximilian Golla, Grant Ho*, Marika Lohmus†,
Monica Pulluri⋆, and Elissa M. Redmiles§
Max Planck Institute for Security and Privacy, ∗ University of California San Diego, † Cleo AI,
⋆ Facebook, § Max Planck Institute for Software Systems

Abstract

Two-factor authentication (2FA) is one of the primary mechanisms for defending end-user accounts against phishing and password reuse attacks. Unfortunately, getting users to adopt 2FA remains a difficult challenge. While prior work at the intersection of measurement and usability has examined how to persuade people to avoid dangerous behavior (e. g., clicking through TLS warnings), relatively little work has conducted measurements at industry scale about how to persuade people to adopt protective behaviors.

In this work, we focus on improving end user security in the wild by examining whether (i) messaging that addresses users' motivations, mental models, and concerns about 2FA and (ii) UX design patterns found effective in other fields can effectively improve 2FA adoption. To do so, we conduct a series of large-scale in-the-wild, controlled messaging experiments on Facebook, with an average of 622,419 participants per experiment. Based on our results, we distill a set of best-practice design patterns for most effectively encouraging protective behavior, in the context of promoting 2FA adoption. Finally, we suggest concrete directions for future work on encouraging digital security behavior through security prompts.

1 Introduction

Two-factor authentication (2FA) has received increasing attention from industry [60, 61, 94, 95] and academic research [1, 17, 75, 76]. By augmenting the user authentication process with an additional security step, 2FA helps protect against account security threats such as phishing and password reuse attacks. Microsoft has recently claimed that using 2FA can prevent 99.9 % of account hacks [94]. Mirian et al. [60] studied the ability of professional hackers to infiltrate user accounts and found that 2FA created significant friction that hindered attackers. Yet despite its security benefits, fewer than 10 % of Google users have adopted 2FA and, as of 2016, fewer than 1 % of Dropbox users had done so [13].

To address this gap between the benefits of security best-practices, such as 2FA, and the decisions that users actually make, a significant amount of work has studied how to improve end user security behavior [9, 14, 20, 28, 66, 88]. For example, prior work has examined a variety of approaches to increase 2FA adoption, ranging from user education [5] to institutional policies that require users to adopt 2FA [13]. Unfortunately, despite this sizable and growing body of research, the problem of encouraging users to engage in protective behaviors remains an open and difficult problem.

In the context of improving user security behavior via prompts, prior work has extensively studied security warnings that *discourage* dangerous behaviors [4, 20, 28, 32, 74]. Although some studies do focus on promoting proactive security measures (such as better account hygiene), and have even evaluated their designs in the wild [4, 26, 86], no prior work has specifically studied the impact of prompts on improving 2FA adoption in the wild and at scale.

In this work, we conduct a series of large-scale measurement experiments (n=622,419 users per experiment on average) aimed at protecting end users by improving 2FA adoption in the wild. Specifically, we seek to answer the following research questions, with the ultimate goal of establishing a set of optimal design patterns for protecting end users by encouraging 2FA use:

- **RQ1**: Does messaging tailored to address users' motivations, mental models, and concerns about 2FA improve adoption?
- **RQ2**: Does applying UX design patterns from other domains (e. g., advertising and TLS warnings) in enrollment prompts encourage the adoption of 2FA?

Our work investigates these questions through a set of experiments using Facebook's native 2FA prompts. We use de-identified, aggregated log data to examine whether the strategies we apply in our experimental prompts lead to an increase in the volume of users who click-to-enable 2FA.

We find that tailoring messaging to increase users' sense of individual responsibility for digital security — in line with

protection motivation theory [78, 87] — increases the rate at which users click to enable 2FA by over 30 %.[1] Moreover, tailored messaging that provides users with an accurate mental model of 2FA, by explaining how 2FA works, also increases the rate at which users click to enable 2FA by nearly 30 %. Our analysis also indicates that users' demographics influence their receptiveness toward these different security messages, and their ultimate willingness to enable 2FA, regardless of how they are prompted to enroll in it.

Beyond tailoring the wording of messages displayed to users, we also find that three UX design strategies can effectively increase the proportion of users who protect their accounts by adopting 2FA. Personalizing prompts by including the user's name in the message — a strategy found effective in prior marketing and public policy work [40, 80] — increased the number of users who clicked to enable 2FA by 26.5 %. Interstitial prompts, or those that block the user's screen, also increased clicks to enable 2FA by over 20 %. Finally, we replicate and extend the results of prior work [26, 29], and find that using a combination of commitment devices (i. e., buttons that commit the user to a future action) and opinionated design (i. e., highlighting the safer choice visually) increased the proportion of users who sought to enable 2FA by over 10 %.

From both a practical and theoretical perspective, our results enhance our understanding of how to increase the adoption of 2FA and improve user security behaviors. First, we offer the first validation, to our knowledge, of the role of individual responsibility in the adoption of security behavior in a real world setting (rather than a lab). Second, we find that abstracting the details of how a security mechanism works may hinder adoption; instead, security messaging should clearly and simply explain the functionality and protections of a security mechanism. Third, we find that UX design patterns can significantly improve 2FA adoption, including simple patterns such as adding the user's name to the beginning of a prompt. In sum, we find that prompts can effectively improve the adoption of security behavior in the wild, although we note that prompts alone are not the only factor influencing security behavior adoption. To further protect users, future work should conduct additional research on the factors affecting security behavior more broadly, including the impact of feelings of individual responsibility and the role of user demographics; the latter appears to influence user response to security messages and the choice to adopt protective behavior, based on our study's results.

2 Background and Related Work

In this section, we begin by providing background and related work on two-factor authentication. Next, we review prior work on both (i) 2FA and its alternatives and (ii) security messaging to improve security behavior.

[1] While we find that increasing users' sense of individual responsibility is effective, we do not purport that users are solely, or even primarily, responsible for their security.

2.1 Two-Factor Authentication

To improve users' account security, large online services offer 2FA as an additional protection mechanism that reinforces password-based authentication; these services began offering 2FA around 2011 [22]. 2FA serves as an additional barrier that makes the security of an account less reliant on the secrecy and guessability of its password [65]. It is often advertised as protection against phishing and credential stuffing attacks, which exploit users' tendency to reuse passwords [15, 32].

Usability: The biggest usability challenges are problems with the level of effort or time required [18], the remembrance settings and session length (the number of times a user has to reauthenticate) [13, 76], the registration and handling of security keys [12], and in the case of time-based one-time passwords (TOTPs), tokens that change too frequently [75]. Despite these challenges, users generally perceive 2FA solutions as usable, as detailed in Section 2.2.

Adoption: The adoption of 2FA is generally very low. A measurement study from 2015 concluded that no more than 6.4 % of Google users enabled 2FA [65]. In 2018, Google [59] confirmed that less than 10 % of their users enabled 2FA. Statistics released by Dropbox in 2016 state that less than 1 % of their users had adopted 2FA at that time [13].

Types of 2FA: There are multiple ways in which companies implement 2FA. Commonly used solutions include:

- One-Time Passwords (OTP) sent to the user via SMS, app, email, or call, which the user must then enter to authenticate.
- "Tap to sign-in" (Push) notifications in an app that the user must approve to authenticate.
- Security keys (hardware tokens, caBLE [51, 62]) that the user must tap to authenticate.

Designed as a fallback solution, many platforms also provide a list of so-called one-time *backup codes* that users can print out and use in cases where the normal second factor is unavailable (i. e., new, lost, or broken authenticator). There are also less commonly used solutions that include smart cards [85] and/or other specialized hardware through which users can authenticate. These solutions are typically used in commercial settings or as part of online banking.

Attacks on 2FA: While 2FA is a powerful tool for increasing account security [60], there are attacks that try to bypass or compromise 2FA. A generic attack vector against 2FA solutions are *social engineering attacks* that, for example, involve tricking help desk employees to disable the 2FA [42].

All OTP-based 2FA solutions that ask users to enter a numeric code are susceptible to *phishing attacks*, regardless of

whether those solutions deliver a code via SMS, email, a 2FA app, or hardware token [53, 60].

Even though SMS-based 2FA is the most commonly used 2FA solution, delivering OTPs via SMS is often critiqued [61, 95] as an insecure mechanism when it comes to high-value accounts. Attacks such as *SIM swapping* [48] and *SS7 routing attacks* [33] can bypass SMS-based 2FA by exploiting vulnerabilities in the telephony signaling protocol stack. However, under many common threat models, SMS-based 2FA remains a good deterrent to compromise [60].

Push notification, or "Tap to sign-in", 2FA solutions provide a more phishing-resistant alternative to 2FA OTPs, but they require a smartphone with Internet connectivity and a service-specific app to receive the notifications. However, once users become habituated to approving such 2FA notifications, they might accidentally approve malicious requests [1]. One way to counter such reflex actions is to increase cognitive load by displaying three codes from which the user has to select the correct one [58].

Finally, due to their phishing resistance, FIDO Universal 2nd Factor (U2F) [12] and FIDO2 [50] security keys are of particular interest in security-sensitive environments and are a key component of Web Authentication (WebAuthn) and future password-less user authentication solutions. Since their deployment of U2F security keys in early 2017, Google reported in mid-2018 that they have not experienced any successful phishing attack against their more than 85,000 employees [45]. However, because a specialized key must be purchased for each user, they incur a higher cost than less secure 2FA mechanisms, making them best-suited for employees or security-keen end-users.

2.2 Related Work

Here, we review research on 2FA and security messaging.

2.2.1 Two-Factor Authentication

While a larger body of research about two-factor authentication in both enterprise settings [84, 85] and online banking [46, 96] exists, we primarily focus our review on non-enterprise and non-banking 2FA solutions for end-users.

Comparison Studies: Early work by De Cristofaro et al. [18] compared three 2FA OTP solutions (i. e., hardware token, SMS, and app) via an online survey with 219 participants. Their respondents perceived all OTP solutions as highly usable regardless of the motivation and context. The authors concluded by suggesting that 2FA usability is mostly driven by ease of use, trustworthiness, and required cognitive effort.

More recently, Reese et al. [75] compared five different 2FA mechanisms (i. e., OTP app, OTP SMS, push notification, security key, and pre-generated backup codes). To study 2FA usability, they conducted a between-subjects study with 72 participants. Participants were asked to log into a simulated banking website. As in previous work, participants perceived all methods as highly usable and expressed an interest in using 2FA for other sensitive accounts. The authors also examined the usability of setting up these methods of 2FA, in addition to using the 2FA methods. They found more usability issues with setup, especially with security keys and OTP solutions.

Deployment Studies: Weidman and Grossklags [93] studied the acceptance of a mandatory transition from hardware tokens to a Duo Mobile push notification-based 2FA solution running on employee-owned mobile devices (BYOD) at *Pennsylvania State University*. Their participants found the old token-based system easier to use than the new push notification solution and perceived the old token-based system as more "professional." The authors concluded by mentioning the need for better educational materials that focus on the benefits of the newly introduced system.

Colnago et al. [13] monitored the deployment of mandatory 2FA, using the Duo Mobile 2FA platform, at *Carnegie Mellon University*. They analyzed authentication log files and conducted two online surveys with over 2000 responses. While their participants found the new 2FA system annoying (e. g., some considered it a "significant hindrance to their daily routine"), the respondents also stated that it was relatively easy to use and believed it made their accounts more secure. The authors recommended focusing more on the implementation design (i. e., fixing "remember me" and push notification issues), refining and employing strategic messaging (i. e., emphasizing the added security), and ensuring that educational materials are easily accessible.

Dutson et al. [19] surveyed 4,275 participants from *Brigham Young University* one year after the university deployed mandatory, Duo Mobile-based 2FA. They found that half of their participants reported at least one instance of being locked out of their account. They also emphasized the need for 2FA methods that work without Wi-Fi, proposed UI changes to the 2FA authentication flow, and discussed issues with the remembrance parameters of existing systems.

Abbott and Patil [1] conducted an online survey with users at *Indiana University Bloomington* during their deployment of a mandatory two-factor authentication system. The authors recommended to only mandate 2FA for a few sensitive services to not degrade the user experience.

Reynolds et al. [76] analyzed millions of 2FA logs from the *University of Illinois at Urbana-Champaign* and the *University of California, Berkeley* to quantify the impact of mandatory 2FA deployments on employees. The authors estimated that the average user spends tens of minutes per year on 2FA. Thus, they concluded that 2FA systems are not a significant burden compared to other common risk-mitigation mechanisms and suggested that session timeouts and remembrance parameters should be tuned to further reduce this burden. The authors also noted that about one in twenty 2FA attempts

were unsuccessful, in most cases because users canceled or abandoned their interaction or entered an OTP incorrectly.

All of these prior in-the-wild studies address mandatory 2FA deployments. However, most commercial, non-university deployments of 2FA outside of industry settings are voluntary: users can choose whether to enable 2FA. Our work is the first, to our knowledge, to study how to promote *voluntary* adoption of 2FA at scale. Drawing upon suggestions from prior work, part of our study examines how strategic messaging and including educational content about the mechanism of 2FA — as suggested by Colnago et al. [13] and Reese et al. [75] — can increase voluntary adoption.

Security Keys: Many studies focus on specific issues related to the use of 2FA hardware tokens and security keys. Since prior work focuses on phone-based 2FA methods, we review this work only briefly. Reynolds et al. [77] studied the use of security keys in a non-enterprise setting over four weeks. They found issues with setup instructions but reported that most participants generally enjoyed using security keys. Das et al. [16] also studied security keys. Via a think-aloud protocol, they found participants did not understand the advantage of security keys compared to a more secure password and expressed fear of losing the device. In a follow up study, Das et al. [17] explored why *older adults* choose not to adopt 2FA. They found problems with handling the tiny form factors and the need to communicate the benefits of 2FA and risks of not using 2FA more clearly. Ciolino et al. [12] studied the usability of U2F security keys and compared them to SMS-based 2FA via a lab and diary study. They found the setup time for security keys was considerably longer, and participants perceived the keys as less usable than SMS-based 2FA.

Alternatives: Finally, 2FA is not the only approach to improving account security. Wiefling et al. [97] studied the usability of risk-based authentication – in which users are only asked for a second factor (an OTP received via email) if their login appeared risky based on several factors, such as whether the device was previously used and the login's current location – and compared it to traditional 2FA and a password-only solution. Further, Lyastani et al. [50] and Farke et al. [25] evaluated security key-based FIDO2 solutions in which the user only has to use a security key and no password.

2.2.2 Designing Security Messages

A large body of prior work has studied security messages, warnings, and notifications. Examples include warnings, messaging, and educational materials to help users detect phishing [20, 81], choose stronger passwords [21, 89, 90], avoid password reuse [32], change their password when it gets breached [86], and adopt 2FA [2, 5, 71].

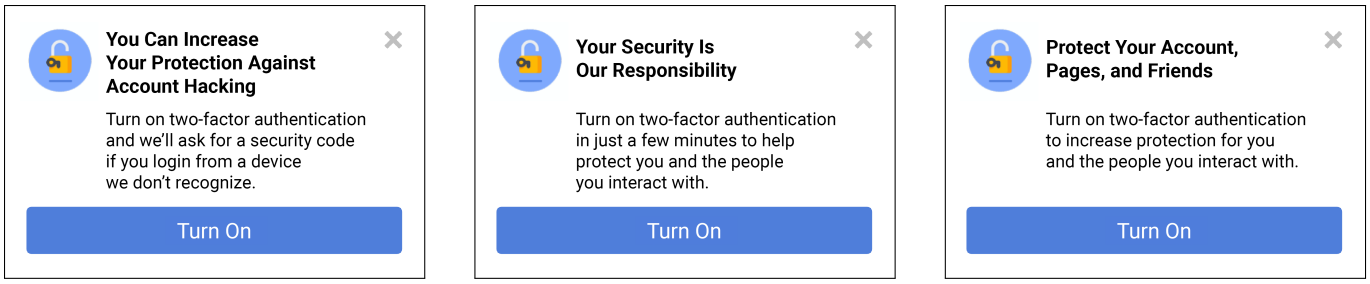
Browser Security: Akhawe et al. [4] found that user experience has a significant impact on behavior and that users often do look at warnings, contrary to other findings which claim that users often ignore web warnings [9, 10]. Felt et al. [26, 28] studied and compared click-through rates (CTRs) and designed new TLS warnings to help users make an informed decision and encourage them to act securely. Their work aimed to create a simple, brief, specific, and opinionated warning that included no technical jargon. Among other features, the study carefully considered how to communicate the threat and made use of opinionated design (for example, UX changes to promote the safe choice), which led to substantially improved adherence rates.

Account Security: Jenkins et al. [43] evaluated the efficacy of just-in-time fear appeals and found that such appeals resulted in a significant decrease in password reuse. Golla et al. [32] designed password reuse notifications that are usually delivered via email. They also evaluated a variant that suggested users to enable 2FA. Thomas et al. [86] designed password breach alerts that are shown when a user tries to reuse an already breached credential. They designed an in-page warning and tray icon warning message that included a clear action and the context for the danger. They minimized the technical jargon and linked to an explanation with more details. Markert et al. [52] evaluated enforcing and non-enforcing PIN blocklist warnings and their impact on the guessability of smartphone unlock PINs. Egelman et al. [21], Golla et al. [31], Ur et al. [88, 89], and Vance et al. [90] explored and tested various password strength meter designs to encourage users to choose more secure passwords. They explored various designs that included elements from fear appeals, peer-pressure, and gamification.

Most relevant to our work, Ackerman [2] and Albayram et al. [5] developed and evaluated informational videos about the security risk, self-efficacy, and ease-of-use to encourage 2FA adoption. They evaluated the impact of these videos in a lab setting and/or users' reported intent to adopt 2FA. Our experiments build on this prior work, evaluating the impact of messages that provide, for example, education about the mechanism of 2FA and the risks against which 2FA protects (e. g., hacking) on real-world 2FA adoption. Finally, Redmiles et al. [71] studied the design of 2FA messages. The authors conducted a small interview and participatory design study with 12 participants that evaluated existing 2FA messages and created a set of best practice guidelines for improved messages. Following recommendations from this work, we utilize messaging in our study that includes personalization and communicates the time costs of 2FA. In contrast to this prior work, we evaluate the impact of applying these strategies to improve 2FA adoption in the wild.

3 Methodology

To systematically address our research questions and identify effective design patterns for improving 2FA adoption, we conducted a series of controlled experiments to improve the



(a) Prompt with a **user responsibility** headline and **mechanism** body text.

(b) Prompt with a **company responsibility** headline and **2FA cost** body text.

(c) **Control** prompt with a neutral headline and neutral body text.

Figure 1: Examples of prompts used in our RQ1 experiments.

messages used to prompt Facebook users to enable 2FA. We then analyzed aggregated, de-identified Facebook log data from these experiments to identify effective messaging strategies and design patterns.

3.1 Prompt Design Patterns

Motivated by a diverse body of prior literature from the security, public policy, and HCI communities [8, 13, 28, 34, 40, 41, 44, 71, 73, 80, 82, 91], we designed and compared the impact of nine different messaging strategies and three different UX design patterns on 2FA adoption.

RQ1: Messaging Strategies: To address RQ1, we used a 3×3 experimental design to craft a total of 9 prompts encouraging users to enable 2FA. Each prompt consisted of a headline message (3 variants), a body text (3 variants), and a blue "Turn On" button that a user could click to initiate the 2FA enrollment process.[2] Figure 1 shows three examples of our prompts. These examples illustrate the three different headlines and body texts that we evaluate in our experiments.

Each headline framed the *benefits* of 2FA through three different *responsibility* lenses. Protection motivation theory – an often cited theory for explaining users' motivations to take security precautions [38, 78, 87] – suggests that a sense of individual responsibility is a necessary prerequisite for users taking protective action. However, little work evaluating this theory has been conducted in a real-world setting. Separately, other prior work has suggested that users feel a loss of control with regard to digital security [83] and that users may be more responsive to requests to take security measures when they feel that the platform requesting those measures is taking responsibility for their security [69].

To evaluate these two contrasting hypotheses – that users must feel individual responsibility to take action vs. that users will be more likely to take action if they feel that action is part of a broader corporate approach to protecting them – we test the following headlines in our messages.

1. **User Responsibility:** This design framed 2FA's benefits as part of the user's responsibility ("You can increase your protection against account hacking").

2. **Company Responsibility:** This prompt emphasized 2FA's security benefits as part of the company's responsibility ("Your security is our responsibility").

3. **Control Message:** The final (control) prompt used a responsibility-neutral message that broadly spoke to 2FA's security benefits ("Protect your account, pages, and friends").

For our body text messages, we focused on addressing cognitive biases and concerns users might have about the operational mechanics and costs of 2FA. We designed one control message and two experimental messages designed to address common concerns found in prior work [13, 41, 71, 73].

1. **Time Costs of 2FA:** Prior studies have shown that user concerns about the time cost of a security process (such as 2FA) influence whether they engage in it [13, 41, 71, 73]. Our first experimental body text explicitly addressed the time cost of enrolling in 2FA ("Turn on two-factor authentication in just a few minutes to help protect you and the people you interact with").

2. **Mechanism:** Users' negative perceptions and/or lack of understanding of the mechanism and operational costs of 2FA (for example, when they will have to engage in extra operations and the potential burden of these extra steps) has contributed to the lack of 2FA adoption [13, 71]. To appropriately set users' mental models of 2FA, especially about its operational frequency and overhead, we crafted and tested a body text that explained the mechanics of 2FA and how this process protects the user ("Turn on two-factor authentication and we'll ask for a code if we see a login from a device we don't recognize").

[2] We conducted a post-test following this experiment (n=28,417) to validate the wording of this button. We evaluated the phrases: 'Try It,' 'Turn On,' and 'Get Started.' 'Turn On' resulted in a significantly higher CTE rate as compared to 'Try It' ($X^2 = 33.6$, $p < 0.001$) and 'Get Started' ($X^2 = 443.4$, $p < 0.001$).

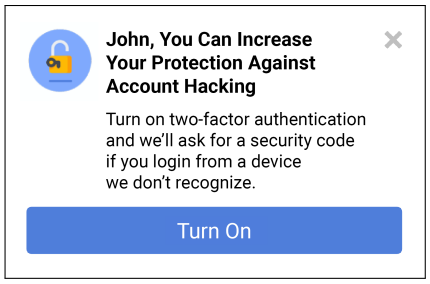


Figure 2: **Personalization** design.

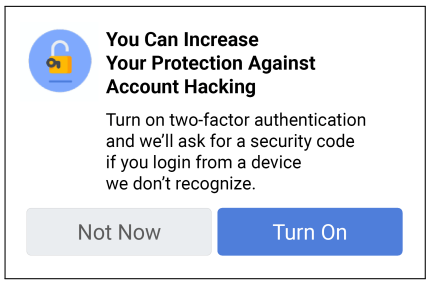


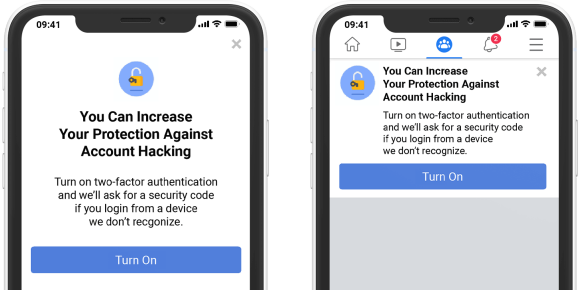
Figure 3: **Opinionated Reminder** design.

3. **Control Message:** For our third body text, we designed a neutral control message that omitted any discussion about the time or operational requirements of 2FA, and instead, simply re-framed the benefits of 2FA ("Turn on two-factor authentication to increase protection for you and the people you interact with").

RQ2: Applying UX Design Patterns: We explored the effect of three different UX design patterns on encouraging 2FA adoption, drawing upon prior work that illustrated the efficacy of these strategies in other notification and warning contexts [8, 28, 29, 34, 40, 44, 80, 82].

Personalization: Our first UX strategy examined the impact of personalizing a prompt's text. Research from marketing and public policy studies have shown that personalizing notifications can lead to significant increases in response rates [40,80]. Motivated by these results, we explored whether adopting the simple personalization techniques from this prior literature would lead to similar improvements in 2FA adoption. Specifically, we crafted an experimental prompt that addressed the user by their first name in the beginning of the headline (e. g., "John, You Can Increase Your Protection Against Account Hacking"). See Figure 2 for an example.

Opinionated Reminders: For our final UX strategy, we studied whether using reminder messaging — which was found effective in prior work [29] on encouraging self-reported adoption of 2FA — combined with opinionated design — which was found effective in prior work [26] measuring the efficacy of different warnings on discouraging bypassing of SSL warnings in the wild — could increase 2FA adoption. Prior work has shown that adding a deferral or



(a) Interstitial design. (b) Non-blocking design.

Figure 4: Figures showing the **interstitial** (blocking) and non-interstitial (non-blocking) designs we evaluated in our third RQ2 UX experiment.

reminder option to security prompts can reduce the likelihood that a user ignores or dismisses the notification [29]. Researchers hypothesize that adding these options helps reduce the effect of "present bias," or the tendency for users to undervalue future risks and rewards (a bias that can lead users to make less secure decisions). However, while adding these choices decreases the proportion of users who outright dismiss a prompt, this decrease is often the result of more users selecting the reminder (deferral) option, and not an increase in users who choose to follow the prompt and immediately perform the secure behavior.

For our design, we explored whether augmenting this "reminder" option with opinionated design could not only decrease the number of users who dismissed the 2FA enrollment prompt, but actively increase the users who engaged with our prompts to enable 2FA. In particular, research from the security and marketing literature reveals that employing forms of opinionated design, such as coloring, pre-selected defaults, and specific wording can encourage users to make particular decisions [11, 26, 34]; in cases where companies employ this design to emphasize potentially unwanted options, the community considers this a dark pattern (termed "nagging"). Because our goal is to improve user security, we explored whether we could combine techniques from this literature with reminder messaging to improve 2FA adoption.

In our experiments, we crafted two prompts. The first design combined reminder messaging with opinionated UX coloring to encourage 2FA adoption: this prompt included both the blue "Turn On" button that would initiate 2FA enrollment, as well as a grayed out "Not Now" (reminder) button that a user could click to close the 2FA prompt; this prompt design also included the standard "×" window closure button. See Figure 3 for an example. Our control prompt excluded this "Not Now" button, allowing users to either click-to-enable 2FA via the "Turn On" button or click on the window closure button to close the prompt (as seen in Figure 1).

Interstitial (Blocking) Prompts: Although prior work has shown that users do not prefer interstitial ("blocking")

prompts [8, 82], other related work has shown that this style of prompt does improve the message's efficacy and user compliance [28, 44]. Examining the impact of this design pattern, we developed an interstitial prompt that covered the user's full Facebook News Feed. We then compared the efficacy of this interstitial design versus the default prompt style used in RQ1, where the prompt hovered at the top of a user's News Feed, but did not block them from interacting with Facebook if they did not first interact with the prompt. Figure 4 shows a side-by-side comparison of the prompts.

3.2 Procedure

We conducted two series of experiments to answer each of our research questions.

In each experiment, participants were selected following standard procedures for Facebook product experiments. Our samples consisted of a subset of US Facebook users who did not already have 2FA enabled and whose demographics (age, gender, friend count, tenure, activity level) were not statistically significantly different from the demographics of all US Facebook users (see Section 3.4 below for sample demographics). Selected users were shown the prompt at the top of their Facebook News Feed. If users clicked to enable 2FA on the prompt, they were taken through Facebook's 2FA enrollment flow, which offers OTP 2FA via SMS or a third-party authenticator app (cf. [24]). On the other hand, if they clicked away from their News Feed, the prompt disappeared.

To evaluate the efficacy of our design patterns, we measured the click-to-enable (CTE) rate of our messages. The CTE corresponds to the fraction of users that initiated the 2FA enrollment process in response to our prompt (i.e., clicking on the "Turn On" button to start the 2FA enablement process). We focus on measuring CTE rates, since none of our experiments influenced subsequent parts of the 2FA enrollment flow; i.e., the different designs we implemented center around this first step of the 2FA enrollment (clicking on our prompt to start the enablement process). Additionally, all of the designs with a statistically significant increase in CTE rate also had a statistically significant increase in 2FA enablement.

RQ1 Experiments: Across the nine messaging strategies explored in our RQ1 experiments, a total of 697,212 users each received only one style of prompt, where each prompt varied in headline (3 variants) and body text (3 variants), resulting in an average of 71,700 distinct users per prompt (SD=275.29). To compute the CTE rate for each prompt, we recorded the number of users who clicked on the "Turn On" button for each message and divided this count by the total number of users who received the prompt.[3] After we identified the most effective message among these nine strategies, all users in our study who had received one of the less effective messages and who had not enabled 2FA were shown the most effective message to maximize participant safety; this step was separate from our study's measurements.

RQ2 Experiments: To address RQ2, we conducted three experiments, each addressing one UX design principle that prior work found effective in other notification contexts (see Section 3.1); each experiment compared an experimental prompt against a control prompt. In these experiments, we used the most effective message from the RQ1 experiments.

In the first experiment ($n = 609,327$), we tested the effect of personalization by comparing a prompt that addressed the user by their first name in the beginning of the prompt's headline (e.g., "John, You Can Increase Your Protection Against Account Hacking") to a version that did not ("You Can Increase Your Protection Against Account Hacking"). 304,633 users saw the personalized prompt and a separate set of 304,694 users saw the control prompt.

In the second experiment ($n = 562,459$), we tested the effect of using interstitial (blocking) prompts, instead of the less intrusive prompts used in the RQ1 experiments. 273,322 users received an interstitial prompt and a separate set of 274,571 users received a non-interstitial prompt.

Finally, we tested the effect of reminder messaging and opinionated design on improving 2FA adoption ($n = 620,678$). Half our sample received a control prompt that only presented the blue "Turn On" button ($n = 310,220$) and the $\times$ window closure button, as seen in Figure 1). The other half of the users in this experiment ($n = 310,458$) received a prompt that had both a "Turn On" button in blue and also offered a "Not Now" button in gray (in addition to the standard $\times$ window closure button in the top right corner).

3.3 Analysis

To answer RQ1, we first constructed a logistic regression model comparing the elements of the different prompts. The dependent variable is whether a user clicked and the independent variables are the headline of the prompt they were shown, the body text of the prompt they were shown, and an interaction term between the headline and the body text that they were shown. Next, to ensure our results were robust to demographic variance, we added demographic features and interactions between those features and message characteristics to our model. Specifically, we added the independent variables: gender (a binary factor for whether the user self-reported in their Facebook profile as Female, or not), age (a numeric value self-reported by the user), Facebook tenure in years (how many years the user had been on Facebook), friend count in hundreds of friends (how many hundreds of friends the user had on Facebook), and days active on Facebook (the number of days out of the last 30 days where the user engaged in any activity on Facebook). We additionally included interaction factors between each of these demographic variables and the headline and body message variables.

[3] Once a user clicks on the 'Turn On' button, they are taken to the 2FA onboarding flow in which they need to either enter their phone number or set up app-based 2FA [24].

For both models, we report the odds ratio (i. e., the exponentiated regression coefficient which, for significant variables, represents the likelihood of a click given this variable), 95 % confidence interval for the odds ratio, and the p-value.

For RQ2, we compared the CTE rate for experimental conditions in each of the three RQ2 experiments using χ^2 proportion tests. Section 4 presents the results of these models and tests, as well as the relative differences in CTR rates.

3.4 Sample Demographics

The Facebook users in our experiments were all based in the U.S. and had their locale (language) set to English. Given that many of our experiments focus on improving the *language* of 2FA prompts, we chose to focus on a single country and language for this work to avoid introducing locale-related confounding effects. These users had a median self-reported age of 42 and a mean self-reported age of 43.8 (Std. Dev.: 15.2 years). 54.3 % of our sample self-reported as Female, 43.7 % self-reported as Male, and 2.0 % either chose not to self-report their gender or self-reported as non-binary.

In the 30 days prior to the experiment, participants had a median of 30 / 30 days with some online activity, and a mean of 25.5 / 30 days with prior activity (Std. Dev: 9.00 days). The median account age across our sample was 11 years, and the mean was 10.76 years (Std. Dev: 3.69 years). The sample had a median Facebook friend count of 607 friends and an average of 950.7 friends (Std. Dev.: 1070.2 friends).

3.5 Ethics and Use of Facebook Data

In this work, we analyzed de-identified, aggregated Facebook log data records. Apart from displaying the 2FA enablement prompts there was no manipulation of any Facebook user's experience, and no personal identifying information was used in this work. All users in this work were offered the opportunity to enable 2FA authentication, and experiments were ordered such that the best-performing message from the first set of experiments were used in the second set of experiments to ensure the most benefit to user security.

3.6 Limitations

Our work has multiple limitations. First, we conducted our experiments only on Facebook. While Facebook is the largest social media platform and among the largest platforms on the internet, with 2.85 billion monthly active users as of March 2021 [23], user behavior on Facebook may not be representative. Moreover, our results most accurately reflect 2FA in the context of individual (personal) use, and may not generalize to, for example, 2FA adoption in enterprises.

Additionally, we conducted our experiments only with U.S. Facebook users. We do so because our experiments focus on language, and thus to avoid the introduction of language-related-variables we focus on a single locale. However, prior work studying security behavior on Facebook [69, 70] and security behavior in general (cf. [7, 36, 39]) has found significant differences between users based on geography. Thus, our results cannot be presumed to generalize beyond the U.S. Finally, we focus on SMS-based 2FA, and do not explicitly examine 2FA adoption for more elaborate mechanisms (e.g., security keys, app-based 2FA).

4 Results

In this section, we examine the results of our experiments using the analysis procedure described in Section 3.3. For simplicity, we report our results in terms of click-to-enable (CTE) rates. Across our experiments, CTE is significantly and strongly correlated with actual adoption ($r = 0.744$, $p < 0.001$), and every design pattern that exhibited significant CTE results also exhibited a significant change in 2FA enablement. Our analysis indicates that two messaging strategies and all three of the UX design patterns we studied lead to statistically significant improvements in user click-to-enable rates (an increase in the relative volume of users who initiate the 2FA enrollment process via our notification prompts). Additionally, our results illuminate interesting dynamics between user demographics and the effect of different strategies we explored, which we highlight as a direction for future work.

4.1 Impact of Messaging Strategies

Table 1 shows the results of our logistic regression model of the relationship between clicking-to-enable 2FA and the different messaging strategies we explored. Two designs, one headline and one body variation, showed statistically significant relationships to increased 2FA adoption.

We found that a headline that framed 2FA as the user's responsibility led to an increase in CTE. Relative to a control headline that generically stated the security benefits of 2FA, this user-responsibility headline led to a 33 % increase in users who clicked to enable 2FA. We hypothesize that this message is effective for two reasons. First, it underscores individual responsibility as a factor that protection motivation theory, and prior digital security work conducted in the context of behavioral intent, has suggested is an important prerequisite to users taking protective digital security action [38, 78, 87]. Second, it effectively communicates risk [2, 5, 47, 71] by bringing up hackers, whom research shows are one of the main threat models of western users for computer security [92], and particularly account security [69].

With respect to addressing users' cognitive biases about the burden of 2FA, via variations in the prompt's body text, a message that explained the mechanics of how 2FA would work significantly increased CTE rates. Users who received

Variable	O.R.	CI	p-value
Intercept	0.01	[0.01, 0.01]	< 0.01
Headline: Company Responsibility	1.05	[0.96, 1.16]	0.25
Headline: User Responsibility	**1.33**	**[1.22, 1.45]**	$<$ **0.01**
Body: Mechanism of 2FA	**1.28**	**[1.17, 1.39]**	$<$ **0.01**
Body: Cost of 2FA	1.00	[0.92, 1.1]	0.92
Headline: Company Responsibility * Body: Mechanism of 2FA	1.04	[0.92, 1.18]	0.5
Headline: User Responsibility * Body: Mechanism of 2FA	1.00	[0.89, 1.12]	0.98
Headline: Company Responsibility * Body: Cost of 2FA	1.02	[0.9, 1.16]	0.74
Headline: User Responsibility * Body: Cost of 2FA	1.10	[0.98, 1.24]	0.12

Table 1: Logistic regression model of the relationship between user likelihood of clicking to enable 2FA and the headline and body text of the 2FA prompt they were shown. The table reports odds ratio (O.R.), 95 % confidence intervals for the odds ratios (shown in brackets), and p-values.

Variable	Odds Ratio	CI	p-value
Intercept	0.00	[0, 0]	< 0.001
Headline: Company Responsibility	1.02	[0.37, 1.08]	0.09
Headline: User Responsibility	**2.28**	**[1.29, 4.08]**	$<$ **0.001**
Body: Mechanism of 2FA	**2.06**	**[1.16, 3.71]**	**0.01**
Body: Cost of 2FA	0.70	[0.4, 1.23]	0.22
Age	**1.02**	**[1.02, 1.02]**	$<$ **0.01**
Gender: Female	**0.90**	**[0.82, 0.99]**	**0.03**
FB Friend Count (100s)	**1.02**	**[1.02, 1.02]**	$<$ **0.001**
FB Tenure (yrs)	**0.92**	**[0.91, 0.93]**	$<$ **0.001**
Days Active (out of 30)	**1.05**	**[1.03, 1.07]**	$<$ **0.001**
Headline: Company Responsibility * Body: Mechanism of 2FA	1.04	[0.92, 1.17]	0.55
Headline: User Responsibility * Body: Mechanism of 2FA	1.00	[0.89, 1.12]	1
Headline: Company Responsibility * Body: Cost of 2FA	1.00	[0.89, 1.14]	0.97
Headline: User Responsibility * Body: Cost of 2FA	1.08	[0.96, 1.21]	0.22
Headline: Company Responsibility * Age	1.00	[1, 1]	0.81
Headline: User Responsibility * Age	**0.995**	**[0.99, 1]**	$<$ **0.001**
Body: Mechanism of 2FA * Age	1.00	[1, 1]	0.49
Body: Cost of 2FA * Age	1.00	[1, 1]	0.8
Headline: Company Responsibility * Gender: Female	1.04	[0.94, 1.15]	0.4
Headline: User Responsibility * Gender: Female	1.00	[0.91, 1.1]	0.92
Body: Mechanism of 2FA * Gender: Female	0.99	[0.9, 1.08]	0.77
Body: Cost of 2FA * Gender: Female	0.97	[0.88, 1.07]	0.5
Headline: Company Responsibility * FB Friend Count (100s)	1.00	[0.99, 1]	0.12
Headline: User Responsibility * FB Friend Count (100s)	1.00	[0.99, 1]	0.13
Body: Mechanism of 2FA * FB Friend Count (100s)	**0.99**	**[0.99, 1]**	$<$ **0.001**
Body: Cost of 2FA * FB Friend Count (100s)	1.00	[1, 1]	0.69
Headline: Company Responsibility * FB Tenure (yrs)	1.00	[0.99, 1.02]	0.77
Headline: User Responsibility * FB Tenure (yrs)	1.00	[0.98, 1.01]	0.58
Body: Mechanism of 2FA * FB Tenure (yrs)	**1.03**	**[1.02, 1.04]**	$<$ **0.001**
Body: Cost of 2FA * FB Tenure (yrs)	1.01	[0.99, 1.02]	0.44
Headline: Company Responsibility * Days Active (out of 30)	0.98	[0.96, 1]	0.21
Headline: User Responsibility * Days Active (out of 30)	0.99	[0.97, 1.01]	0.39
Body: Mechanism of 2FA *Days Active (out of 30)	1.02	[1, 1.04]	0.06
Body: Cost of 2FA * Days Active (out of 30)	1.01	[0.99, 1.03]	0.2

Table 2: Logistic regression model of the relationship between user likelihood of clicking to enable 2FA, the Headline and body text of the 2FA prompt they were shown, and the user's demographics. See Table 1 for column details.

prompts with this messaging strategy were 28 % more likely to enable 2FA protection, as compared to users who received a generic prompt that simply re-iterated the security benefits of 2FA. We hypothesize that this may be the case because users do not know, or are suspicious, about why they need to turn on 2FA. Prior work suggests that users want to understand *why* they need to provide information, like their phone number, to gain security benefit [72].

Demographics and Messaging Strategies: Next, we expanded the model presented in Table 1 to include user demographics (see Table 2). We find that even when controlling for user demographics, our results remain the same. However, our analysis suggests that (i) some user demographics are more or less likely to enable 2FA regardless of the message they were shown, and (ii) certain messaging is particularly effective, or ineffective, for different demographics.

Specifically, we find that older users, more active users, and those with more Facebook friends were all more likely to enable 2FA. However, women — in line with prior work showing that women may focus more on content-level safety controls, while men focus on system-level controls [35,55,68] — and those who have been on Facebook longer, perhaps because this group has been prompted regarding enabling 2FA in the past, are less likely to enable. While our work does not focus on explaining these findings – future work on the relationship between 2FA use and socio-demographics is needed – they do suggest that (i) prompts are not the sole determiners of 2FA use and (ii) prompts alone cannot bring equity to differential use of security behaviors, but may offer a step in the right direction.

Related, we find that different messages may be more, or less, effective for different user groups. Those who are older and who were presented with the headline focusing on user responsibility were less likely to enable. This suggests that older users may have different perceptions of their role in the security protection relationship with platforms, and that further work is needed to customize security messaging to older adults. Indeed, a growing – yet still small – body of work has recently emerged focusing specifically on older adults [30,49,56,57,67], and suggests that the needs of this population may differ from those of other users.

Those who have more friends on Facebook were less likely to click to enable 2FA if they were presented with the message focusing on the mechanism through which 2FA works. We hypothesize this may be the case because our control body text mentioned "increasing protection for you and **the people you interact with**." In other words, those with more friends may value protecting others more than those with fewer friends, making the control message more salient.

On the other hand, those who had been on Facebook longer (those with longer tenure) were even more likely to enable when shown the message describing the mechanism through which 2FA works than those who had been on the platform for less time. We hypothesize that because these users may understand Facebook better, they might be able to more clearly reason about the information provided in the mechanism body text. That said, the mechanism body text remains significant in this model: users of any demographic who saw this were more than twice as likely as those shown the control text to click to enable 2FA. This finding simply suggests that messaging around the operational mechanics of 2FA is even more effective among those with longer tenure on Facebook.

4.2 Impact of UX Design Patterns

With respect to the different UX design patterns we explored (RQ2: §3.1), all three designs led to significant increases in user CTE rates. Figure 5 summarizes the increases in CTE rates of prompts that used each design pattern, relative to a control prompt that did not employ the design.

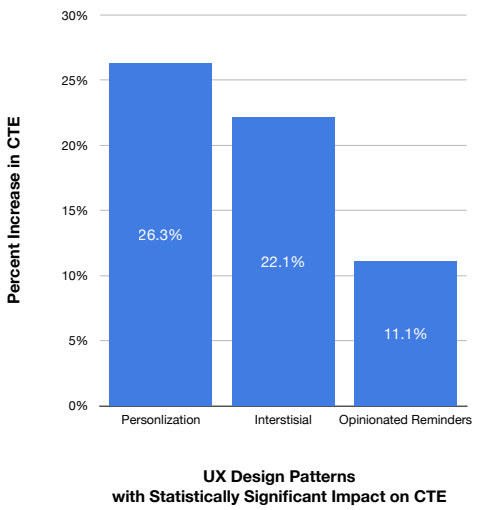


Figure 5: The percent increase in user click-to-enable (CTE) rates for the UX design patterns we tested (cf. Section 4.2).

Personalization led to higher 2FA CTE rates: Prior work studying public policy messaging strategies suggests that addressing users by name leads to increased responsiveness [40,80]. Testing this approach, we found that this strategy of personalizing 2FA prompts did lead to a significant, 26.3 % improvement in CTE rates ($\chi^2 = 103.4$, $p < 0.001$).

Opinionated Reminder Messaging increased 2FA CTE rates: In this experiment, we explored whether combining reminder messaging with opinionated design could increase 2FA click-to-enable rates. Our results revealed that this design pattern, adding an option to dismiss the prompt for the time being (reminder messaging) and using coloring to highlight the click-to-enable option, led to a significant improvement in adoption: click-to-enable rates to begin the enrollment process increased by 11.1 % ($\chi^2 = 30.814$, $p < 0.001$), relative to a prompt that completely omitted the "Not Now" button. Although prior work has shown that reminder messaging leads to a decrease in users who explicitly exit a prompt [29], this design pattern did not improve the users that affirmatively engaged with the prompt (i. e., who chose to perform a security action like enabling 2FA or updating their software). Rather, reminder messaging led a significant fraction of users to select the reminder option, in lieu of clicking to immediately dismiss the prompt. Our results suggest that *opinionated reminders* that combine reminder messaging with opinionated design, in the form of selective coloring to highlight the 2FA enablement option, can effectively increase the number of users who choose to protect their accounts with 2FA.

Interstitial prompts increased 2FA CTE rates: The second UX modification tested the effect of a blocking prompt [8,28,44,82,91], instead of the less intrusive prompts used in the RQ1 experiments. In our experiments, we observed that the

interstitial prompts did lead to a significant increase in 2FA adoption: interstitial prompts resulted in a 22.1 % higher CTE rate ($\chi^2 = 14768.0$, $p < 0.001$).

4.3 Does 2FA Remain Enabled?

While not directly tied to our experimental stimuli, we also sought to investigate whether those who enabled 2FA kept it enabled. We find that 95.2 % of participants in our experiments still had 2FA enabled 90 days following their initial enablement period. Notably, this is 8.06 % higher ($\chi^2 = 19761$, $p < 0.001$) than the 2FA retention rate for non-experiment participants who turned on 2FA without having been prompted, during the same time period. This suggests that prompting users to enable 2FA – when appropriate – may be effective not only for increasing the number of users who enable 2FA but also the number of users who keep it enabled.

5 Discussion

Overall, our experiments show that adjusting the messages used in 2FA prompts, as well as implementing UX design patterns found effective in other applications, can significantly increase the number of users who enable 2FA. We found that messages emphasizing the user's responsibility for protecting their account and messages explaining specifically how 2FA works increased the proportion of users who clicked to enable 2FA by approximately 30 %.

Individual responsibility as a driver of digital security behavior. Our work first evaluates the impact of prompt messages that focus on user vs. company responsibility in order to compare two contrasting bodies of literature. Protection motivation theory [78] suggests that individual responsibility is a prerequisite to protective behavior and prior work on security behavior supports this theory [87]. On the other hand, a separate set of prior work on digital security behavior suggests that users may be more receptive to engaging in secure behavior when they believe the platform promoting such behavior is in control of their security [83] and/or looking out for their interests [69]. Our work — which is the first, to our knowledge, to test the individual responsibility criterion of protection motivation theory in the wild — supports the validity of protection motivation theory in digital security behavior. Specifically, our results indicate that increasing individual feelings of responsibility through explicit messaging leads to an increase in users' willingness to enable 2FA. We do not find support for messaging that emphasizes the platform or company's responsibility. This may be because 2FA is a proactive behavior, rather than a reactive behavior (e. g., changing password after a breach) studied in past work [32, 69, 83].

That said, we do find that emphasizing user responsibility is less effective among older adults, perhaps because these adults feel less confident and in control over their technology use and ability to stay safe online [6,54]. While we do not find that older adults are receptive to the idea of the platform being responsible for their security either, future work may seek to further investigate the role of responsibility in security. In particular, it should seek to examine the role of responsibility and feelings of confidence across users of different ages.

We note that while emphasizing individual responsibility for security is an effective strategy to increase a user's likelihood of enabling 2FA, we do not purport that security *is* solely, or even primarily, the user's responsibility. Rather, platforms should make all possible efforts to secure user accounts, and only when it is necessary to partner with the user should their individual responsibility be emphasized. Finally, an alternative to these individual approaches are policy solutions, such as the EU payment services directive (PSD2), which mandate the use of 2FA. However, such solutions may burden users who are less concerned about account security or who have lower digital skills [73].

Don't hide the mechanism of protective behavior from users. We also find that explaining the mechanics of how 2FA works — including what threat (e.g., an unrecognized login) it protects against and how it does so (e.g., by blocking the login until a code is entered) — led to an increase in the number of users who sought to enable 2FA. This effect is even more pronounced among those who have more experience on the platform; i. e., users who have used Facebook for longer were even more likely to enable 2FA when provided with these additional details. This result supports prior work that suggests cognitive biases around the difficulty of enabling 2FA may prevent users from adopting it [13, 71]. Adding to our understanding from prior work, our analysis shows that (a) the perceived difficulty of enabling 2FA can be reduced and that (b) reducing the perceived difficulty of enabling 2FA can increase enablement rates. Furthermore, this finding suggests that abstracting away all detail about a security behavior from the user is not necessarily helpful, which is in line with prior findings regarding end users' mental models of encryption [79]. While overloading users with technical detail has been found to reduce willingness to engage in protective behaviors [27,37,63,98], explaining how protective mechanisms work transparently and at an appropriate level of detail may be an effective way to aptly set user mental models.

Perhaps surprisingly, we do not find that telling users 2FA enablement will take a limited amount of time improves their willingness to enable 2FA. This is despite prior work suggesting that the time cost of 2FA and/or security behaviors more generally is a barrier to users wanting to enable 2FA or other protective behaviors [13, 41, 71, 73]. We hypothesize that our message stating 2FA would take "a few minutes" to enable may not have reduced the perceived time cost of enablement enough for us to observe an effect.

UX design patterns, especially personalization, effectively improve 2FA adoption. Beyond evaluating whether different messaging used in prompts could improve user enrollment in 2FA, we also evaluated the impact of three UX

design patterns: personalization (adding the user's name to the prompt), interstitials (blocking the user's screen until they interact with the prompt), and opinionated reminders (that offer a "Not Now" button that is colored less appealingly than the enablement button). All three UX design patterns encouraged secure behavior, significantly improving the proportion of users who clicked to enable 2FA. Personalization was the most effective (a 26.3 % improvement), followed by the interstitial prompt (22.1 % improvement). Offering an opinionated reminder increased the proportion of users who clicked to enable 2FA by 11.1 %, perhaps because explicitly offering this option increases user trust.

While interstitial prompts have potential downsides — users may find them annoying and they may decrease engagement if users leave the platform instead of navigating past the prompt – personalization and opinionated reminders offer few downsides. Thus, future implementations of security prompts should strongly consider integrating these two design patterns and carefully consider when it makes sense to use interstitial prompts to protect users.

Prompts are only one piece of the 2FA — and broader security behavior — puzzle. Finally, our work also illustrates that while prompts and UX design patterns are effective at increasing 2FA enablement rates, other factors also influence users' adoption decisions. In Section 4.1, we show that user demographics have a significant impact on whether a user clicks to enable 2FA, regardless of the 2FA prompt they are shown. This finding echoes themes from prior work, which has found that the value of a user's account [73], the security information they receive [72], their security knowledge [5], and how many other accounts they have [41], influence their willingness to engage in 2FA and other security behaviors. Additionally, platforms and services should carefully consider when and how frequently to display prompts to users. Our experiments illustrate that displaying one-time prompts to users can promote proactive security behaviors; however, repeatedly showing users similar prompts could lead to fatigue and habituation [10] that decrease the efficacy of future prompts.

Future Work. Our work suggests three concrete directions for future work. First, our results show that prompts can be a powerful way to increase adoption of security behavior in-the-wild. Our findings add to the body of prior work evaluating the efficacy of security indicators and warnings in practice [4, 26, 28, 74, 86]. In this broader context, our work addresses only a subset of security messages and behaviors. There is a significant need for further development of best practices for security messaging based on in-the-wild studies.

Second, our work finds variation in the efficacy of security messaging by demographics. These findings — along with prior work [3, 64] — suggest that future research should explore methods for personalizing security prompts toward user groups and individual users. Our findings suggest that demographics, account value (e. g., friend count), and length of time using the platform may be particularly effective.

Third, while prompts can be a powerful method for encouraging protective behavior — and personalized prompts may be even more effective — prompts alone cannot be held responsible for user security behavior. Thus, additional future work into user security behavior is necessary; for example, investigating the role of feelings of individual responsibility in users' security behavior, and additional strategies that take these personalized notions into account.

6 Conclusion

This paper explores how platforms can better protect users by increasing 2FA adoption through the application of carefully designed security prompt messaging and UX design patterns. Drawing on the digital security, marketing, and HCI literature, we examined whether the design and messaging strategies recommended in these other contexts could be effectively applied in the wild to encourage proactive security behavior. First, we designed a set of prompts to test whether messages that target users' motivations, mental models, and concerns about 2FA could improve adoption. Second, our work studied whether applying different UX design patterns found to be effective in other domains could improve 2FA adoption. We evaluated these different designs in a set of controlled, in-the-wild, and large-scale experiments (with an average of over 600,000 users per experiment).

Our results show that:

1. Carefully designed prompts encouraging users to enable 2FA can significantly increase the number of users who choose to engage in 2FA as a protective behavior.

2. Prompts that emphasize individual responsibility for protective behavior are more effective than those that omit mention of responsibility or those that emphasize corporate responsibility. This finding validates the applicability of protection motivation theory to encouraging digital security behavior [78].

3. Prompts that correctly establish users' mental models of the mechanism through which 2FA offers protection are more effective at increasing adoption than prompts that address the costs of 2FA or prompts that generically reference the benefits of 2FA.

4. Prompts leveraging UX design patterns found effective in other applications — specifically, personalization [40, 80], interstitials [34, 44], and opinionated reminders [28, 29] — effectively increase 2FA adoption. This suggests that UX design patterns for other types of behaviors like product purchases or avoidance of phishing websites generalize well to encouraging protective security behavior.

5. Demographics significantly influence (i) how well different prompts encourage a user and (ii) their general

willingness to adopt 2FA. Combined with findings from prior work [3, 64], this result highlights the potential value of future work that explores how accounting for user demographics and personalizing prompts can improve users' security behavior.

Taken together, our work illustrates that prompts can effectively promote good security behavior in the wild through a variety of messaging and UX strategies. Although prompts cannot bear the sole responsibility of improving account security or user security behavior, our results underscore the value of developing an understanding for how different factors, ranging from UX design, to cognitive biases, to demographics, can influence and promote good security behavior in practice.

Acknowledgments

The authors wish to thank John Lyle at Facebook for his work facilitating and conceiving of this paper and Laura Woodroffe at Facebook for her work on content strategy and design. The authors also wish to thank the USENIX Security reviewers for their constructive feedback in improving this work. Grant Ho was supported in part as a postdoc through the UCSD CSE Fellows program.

References

[1] Jacob Abbott and Sameer Patil. How Mandatory Second Factor Affects the Authentication User Experience. In *ACM Conference on Human Factors in Computing Systems*, CHI '20, pages 1–13, Honolulu, Hawaii, USA, April 2020. ACM.

[2] Preston Ackerman. Impediments to Adoption of Two-factor Authentication by Home End-Users. Technical Report 37607, SANS Institute, February 2017.

[3] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Computing Surveys*, 50(3):44:1–44:41, August 2017.

[4] Devdatta Akhawe and Adrienne Porter Felt. Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness. In *USENIX Security Symposium*, SSYM '13, pages 257–272, Washington, District of Columbia, USA, July 2013. USENIX.

[5] Yusuf Albayram, Mohammad Maifi Hasan Khan, and Michael Fagan. A Study on Designing Video Tutorials for Promoting Security Features: A Case Study in the Context of Two-Factor Authentication (2FA). *International Journal of Human–Computer Interaction*, 33(11):927–942, March 2017.

[6] Monica Anderson and Andrew Perrin. Tech Adoption Climbs Among Older Adults. Technical Report PRC-2017-05-17, Pew Research Center, May 2017.

[7] Joseph Bonneau. The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. In *IEEE Symposium on Security and Privacy*, SP '12, pages 538–552, San Jose, California, USA, May 2012. IEEE.

[8] Giorgio Brajnik and Silvia Gabrielli. A Review of Online Advertising Effects on the User Experience. *International Journal of Human–Computer Interaction*, 26(10):971–997, September 2010.

[9] Christian Bravo-Lillo, Lorrie Faith Cranor, Julie S. Downs, and Saranga Komanduri. Bridging the Gap in Computer Security Warnings: A Mental Model Approach. *IEEE Security & Privacy*, 9(2):18–26, March 2011.

[10] Cristian Bravo-Lillo, Lorrie Faith Cranor, Saranga Komanduri, Stuart Schechter, and Manya Sleeper. Harder to Ignore? Revisiting Pop-Up Fatigue and Approaches to Prevent It. In *Symposium on Usable Privacy and Security*, SOUPS '14, pages 105–111, Menlo Park, California, USA, July 2014. USENIX.

[11] Michael Chromik, Malin Eiband, Sarah Theres Völkel, and Daniel Buschek. Dark Patterns of Explainability, Transparency, and User Control for Intelligent Systems. In *IUI Explainable Smart Systems Workshops*, ExSS '19, pages 1–6, Los Angeles, California, USA, March 2019. ACM.

[12] Stéphane Ciolino, Simon Parkin, and Paul Dunphy. Of Two Minds about Two-Factor: Understanding Everyday FIDO U2F Usability through Device Comparison and Experience Sampling. In *Symposium on Usable Privacy and Security*, SOUPS '19, pages 339–356, Santa Clara, California, USA, August 2019. USENIX.

[13] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Faith Cranor, and Nicolas Christin. "It's Not Actually That Horrible": Exploring Adoption of Two-Factor Authentication at a University. In *ACM Conference on Human Factors in Computing Systems*, CHI '18, pages 456:1–456:11, Montreal, Quebec, Canada, April 2018. ACM.

[14] Lorrie Faith Cranor and Simson Garfinkel. *Security and Usability: Designing Secure Systems that People Can Use*. O'Reilly, Sebastopol, California, USA, 1 edition, 2005.

[15] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. The Tangled Web of Password Reuse. In *Symposium on Network and Distributed System Security*, NDSS '14, San Diego, California, USA, February 2014. ISOC.

[16] Sanchari Das, Andrew Dingman, and L. Jean Camp. Why Johnny Doesn't Use Two Factor: A Two-Phase Usability Study of the FIDO U2F Security Key. In *Financial Cryptography and Data Security*, FC '18, pages 160–179, Nieuwpoort, Curacao, February 2018. Springer.

[17] Sanchari Das, Andrew Kim, Ben Jelen, Lesa Huber, and L. Jean Camp. Non-Inclusive Online Security: Older Adults' Experience with Two-Factor Authentication. In *Hawaii International Conference on System Sciences*, HICSS '21, pages 6472–6481, Kauai, Hawaii, USA, January 2021. AIS.

[18] Emiliano De Cristofaro, Honglu Du, Julien Freudiger, and Greg Norcie. A Comparative Usability Study of Two-Factor Authentication. In *Workshop on Usable Security*, USEC '14, San Diego, California, USA, February 2014. ISOC.

[19] Jonathan Dutson, Danny Allen, Dennis Eggett, and Kent Seamons. Don't Punish all of us: Measuring User Attitudes about Two-Factor Authentication. In *European Workshop on Usable Security*, EuroUSEC '19, pages 119–128, Stockholm, Sweden, June 2019. IEEE.

[20] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. You'Ve Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In *ACM Conference on Human Factors in Computing Systems*, CHI '08, pages 1065–1074, Florence, Italy, April 2008. ACM.

[21] Serge Egelman, Andreas Sotirakopoulos, Ildar Muslukhov, Konstantin Beznosov, and Cormac Herley. Does My Password Go Up to Eleven?: The Impact of Password Meters on Password Selection. In *ACM Conference on Human Factors in Computing Systems*, CHI '13, pages 2379–2388, Paris, France, April 2013. ACM.

[22] Facebook, Inc. A New Suite of Safety Tools, April 2011. https://www.facebook.com/notes/10160198855746729, as of June 2, 2021.

[23] Facebook, Inc. Facebook Reports First Quarter 2021 Results, April 2021. https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-First-Quarter-2021-Results/default.aspx, as of June 2, 2021.

[24] Facebook, Inc. What Is Two-Factor Authentication and How Does It Work on Facebook?, January 2021. https://www.facebook.com/help/148233965247823, as of June 2, 2021.

[25] Florian M. Farke, Lennart Lorenz, Theodor Schnitzler, Philipp Markert, and Markus Dürmuth. "You still use the password after all" – Exploring FIDO2 Security Keys in a Small Company. In *Symposium on Usable Privacy and Security*, SOUPS '20, pages 19–35, Virtual Conference, August 2020. USENIX.

[26] Adrienne Porter Felt, Alex Ainslie, Robert W. Reeder, Sunny Consolvo, Somas Thyagaraja, Alan Bettes, Helen Harris, and Jeff Grimes. Improving SSL Warnings: Comprehension and Adherence. In *ACM Conference on Human Factors in Computing Systems*, CHI '15, pages 2893–2902, Seoul, Republic of Korea, April 2015. ACM.

[27] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. Android Permissions: User Attention, Comprehension, and Behavior. In *Symposium on Usable Privacy and Security*, SOUPS '12, pages 3:1–3:14, Washington, District of Columbia, USA, July 2012. ACM.

[28] Adrienne Porter Felt, Robert W. Reeder, Hazim Almuhimedi, and Sunny Consolvo. Experimenting at Scale with Google Chrome's SSL Warning. In *ACM Conference on Human Factors in Computing Systems*, CHI '14, pages 2667–2670, Toronto, Ontario, Canada, April 2014. ACM.

[29] Alisa Frik, Nathan Malkin, Marian Harbach, Eyal Peer, and Serge Egelman. A Promise Is A Promise: The Effect of Commitment Devices on Computer Security Intentions. In *ACM Conference on Human Factors in Computing Systems*, CHI '19, pages 604:1–604:12, Glasgow, Scotland, United Kingdom, May 2019. ACM.

[30] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce S. Lee, Florian Schaub, and Serge Egelman. Privacy and Security Threat Models and Mitigation Strategies of Older Adults. In *Symposium on Usable Privacy and Security*, SOUPS '19, pages 21–40, Santa Clara, California, USA, August 2019. USENIX.

[31] Maximilian Golla, Björn Hahn, Karsten Meyer zu Selhausen, Henry Hosseini, and Markus Dürmuth. Bars, Badges, and High Scores: On the Impact of Password Strength Visualizations. In *Who Are You?! Adventures in Authentication Workshop*, WAY '18, Baltimore, Maryland, USA, August 2018. USENIX.

[32] 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 *ACM Conference on Computer and Communications Security*, CCS '18, pages 1549–1566, Toronto, Ontario, Canada, October 2018. ACM.

[33] Dan Goodin. Thieves Drain 2FA-Protected Bank Accounts by Abusing SS7 Routing Protocol, May 2017. https://arstechnica.com/?p=1090379, as of June 2, 2021.

[34] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. The Dark (Patterns) Side of UX Design. In *ACM Conference on Human Factors in Computing Systems*, CHI '18, pages 534:1–534:14, Montreal, Quebec, Canada, April 2018. ACM.

[35] Hana Habib, Pardis Emami Naeini, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. User Behaviors and Attitudes Under Password Expiration Policies. In *Symposium on Usable Privacy and Security*, SOUPS '18, pages 13–30, Baltimore, Maryland, USA, August 2018. USENIX.

[36] Tzipora Halevi, James Lewis, and Nasir Memon. A Pilot Study of Cyber Security and Privacy Related Behavior and Personality Traits. In *The World Wide Web Conference*, WWW '13, pages 737–744, Rio de Janeiro, Brazil, May 2013. ACM.

[37] Julie M. Haney and Wayne G. Lutters. "It's Scary... It's Confusing... It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security. In *Symposium on Usable Privacy and Security*, SOUPS '18, pages 411–425, Baltimore, Maryland, USA, August 2018. USENIX.

[38] Bartlomiej Hanus and Yu "Andy" Wu. Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management*, 33(1):2–16, January 2016.

[39] Marian Harbach, Emanuel von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception. In *Symposium on Usable Privacy and Security*, SOUPS '14, pages 213–230, Menlo Park, California, USA, July 2014. USENIX.

[40] Laura Haynes, Owain Service, Ben Goldacre, and David Torgerson. Test, Learn, Adapt: Developing Public Policy with Randomised Controlled Trials. Technical Report TLA-1906126, Cabinet Office (UK) – Behavioural Insights Team, June 2012.

[41] Cormac Herley. So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In *New Security Paradigms Workshop*, NSPW '09, pages 133–144, Oxford, United Kingdom, September 2009. ACM.

[42] Mat Honan. How Apple and Amazon Security Flaws Led to My Epic Hacking, August 2012. http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/, as of June 2, 2021.

[43] Alexander Jenkins, Murugan Anandarajan, and Rob D'Ovidio. 'All that Glitters is not Gold': The Role of Impression Management in Data Breach Notification. *Western Journal of Communication*, 78(3):337–357, January 2014.

[44] Ben Kaiser, Jerry Wei, Elena Lucherini, Kevin Lee, J. Nathan Matias, and Jonathan Mayer. Adapting Security Warnings to Counter Online Disinformation. In *USENIX Security Symposium*, SSYM '21, Virtual Conference, August 2021. USENIX.

[45] Brian Krebs. Google: Security Keys Neutralized Employee Phishing, July 2018. https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/, as of June 2, 2021.

[46] Kat Krol, Eleni Philippou, Emiliano De Cristofaro, and M. Angela Sasse. "They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking. In *Symposium on Network and Distributed System Security*, NDSS '15, San Diego, California, USA, February 2015. ISOC.

[47] Kenneth R. Laughery, Kent P. Vaubel, Stephen L. Young, John W. Brelsford Jr., and Anna L. Rowe. Explicitness of Consequence Information in Warnings. *Safety Science*, 16(5–6):597–613, August 1993.

[48] Kevin Lee, Benjamin Kaiser, Jonathan Mayer, and Arvind Narayanan. An Empirical Study of Wireless Carrier Authentication for SIM Swaps. In *Symposium on Usable Privacy and Security*, SOUPS '20, pages 61–79, Virtual Conference, August 2020. USENIX.

[49] Lesa Lorenzen-Huber, Mary Boutain, L. Jean Camp, Kalpana Shankar, and Kay H. Connelly. Privacy, Technology, and Aging: A Proposed Framework. *Ageing International*, 36(2):232–252, December 2010.

[50] Sanam Ghorbani Lyastani, Michael Schilling, Michaela Neumayr, Michael Backes, and Sven Bugiel. Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. In *IEEE Symposium on Security and Privacy*, SP '20, pages 268–285, Virtual Conference, May 2020. IEEE.

[51] Robbie MacGregor. Evaluating the Android Security Key Scheme: An Early Usability, Deployability, Security Evaluation with Comparative Analysis. In *Who Are You?! Adventures in Authentication Workshop*, WAY '19, pages 1–6, Santa Clara, California, USA, August 2019.

[52] Philipp Markert, Daniel V. Bailey, Maximilian Golla, Markus Dürmuth, and Adam J. Aviv. This PIN Can Be Easily Guessed: Analyzing the Security of Smartphone Unlock PINs. In *IEEE Symposium on Security and Privacy*, SP '20, pages 286–303, San Francisco, California, USA, May 2020. IEEE.

[53] Philipp Markert, Florian Farke, and Markus Dürmuth. View The Email to Get Hacked: Attacking SMS-Based Two-Factor Authentication. In *Who Are You?! Adventures in Authentication Workshop*, WAY '19, pages 1–6, Santa Clara, California, USA, August 2019.

[54] Jean Claude Marquié, Linda Jourdan-Boddaert, and Nathalie Huet. Do Older Adults Underestimate Their Actual Computer Knowledge? *Behaviour & Information Technology*, 21(4):273–280, 2002.

[55] Arunesh Mathur, Jessica Vitak, Arvind Narayanan, and Marshini Chetty. Characterizing the Use of Browser-Based Blocking Extensions To Prevent Online Tracking. In *Symposium on Usable Privacy and Security*, SOUPS '18, pages 103–116, Baltimore, Maryland, USA, August 2018. USENIX.

[56] Tamir Mendel and Eran Toch. My Mom Was Getting This Popup: Understanding Motivations and Processes in Helping Older Relatives with Mobile Security and Privacy. *ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 3(4):147:1–147:20, December 2019.

[57] Helena M. Mentis, Galina Madjaroff, Aaron Massey, and Zoya Trendafilova. The Illusion of Choice in Discussing Cybersecurity Safeguards Between Older Adults with Mild Cognitive Impairment and Their Caregivers. In *ACM Conference on Computer-Supported Cooperative Work and Social Computing*, CSCW '20, pages 164:1–164:19, Virtual Conference, October 2020. ACM.

[58] Microsoft, Inc. Sign in to Your Accounts Using the Microsoft Authenticator App, June 2020. https://docs.microsoft.com/en-us/azure/active-directory/user-help/user-help-auth-app-sign-in, as of June 2, 2021.

[59] Grzergor Milka. Anatomy of Account Takeover. In *USENIX Enigma Conference*, Enigma '18, Santa Clara, California, USA, January 2018. USENIX.

[60] Ariana Mirian, Joe DeBlasio, Stefan Savage, Geoffrey M. Voelker, and Kurt Thomas. Hack for Hire: Exploring the Emerging Market for Account Hijacking. In *The World Wide Web Conference*, WWW '19, pages 1279–1289, San Francisco, California, USA, May 2019. ACM.

[61] Tavis Ormandy. You Don't Need SMS-2FA, July 2020. https://blog.cmpxchg8b.com/2020/07/you-dont-need-sms-2fa.html, as of June 2, 2021.

[62] Kentrell Owens, Blase Ur, and Olabode Anise. A Framework for Evaluating the Usability and Security of Smartphones as FIDO2 Roaming Authenticators. In *Who Are You?! Adventures in Authentication Workshop*, WAY '20, pages 1–5, Virtual Conference, August 2020.

[63] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Why People (Don't) Use Password Managers Effectively. In *Symposium on Usable Privacy and Security*, SOUPS '19, pages 319–338, Santa Clara, California, USA, August 2019. USENIX.

[64] Eyal Peer, Serge Egelman, Marian Harbach, Nathan Malkin, Arunesh Mathur, and Alisa Frik. Nudge Me Right: Personalizing Online Security Nudges to People's Decision-Making Styles. *Computers in Human Behavior*, 109:1–9, August 2020.

[65] Thanasis Petsas, Giorgos Tsirantonakis, Elias Athanasopoulos, and Sotiris Ioannidis. Two-Factor Authentication: Is the World Ready? Quantifying 2FA Adoption. In *European Workshop on System Security*, EuroSec '15, pages 4:1–4:7, Bordeaux, France, April 2015. ACM.

[66] Shari Lawrence Pfleeger, Martina Angela Sasse, and Adrian Furnham. From Weakest Link to Security Hero: Transforming Staff Security Behavior. *Journal of Homeland Security and Emergency Management*, 11(4):489–510, October 2014.

[67] Anabel Quan-Haase and Dennis Ho. Online Privacy Concerns and Privacy Protection Strategies Among Older Adults in East York, Canada. *Journal of the Association for Information Science and Technology*, 71(9):1089–1102, May 2020.

[68] Elissa M. Redmiles. Net Benefits: Digital Inequities in Social Capital, Privacy Preservation, and Digital Parenting Practices of U.S. Social Media Users. In *AAAI Conference on Web and Social Media*, ICWSM '18, pages 270–279, Stanford, California, USA, June 2018. AAAI.

[69] Elissa M. Redmiles. "Should I Worry?" A Cross-Cultural Examination of Account Security Incident Response. In *IEEE Symposium on Security and Privacy*, SP '19, pages 920–934, San Francisco, California, USA, May 2019. IEEE.

[70] Elissa M. Redmiles, Neha Chachra, and Brian Waismeyer. Examining the Demand for Spam: Who Clicks? In *ACM Conference on Human Factors in Computing Systems*, CHI '18, pages 212:1–212:10, Montreal, Quebec, Canada, April 2018. ACM.

[71] Elissa M. Redmiles, Everest Liu, and Michelle L. Mazurek. You Want Me To Do What? A Design Study of Two-Factor Authentication Messages. In *Who Are You?! Adventures in Authentication Workshop*, WAY '17, pages 1–5, Santa Clara, California, USA, August 2017.

[72] Elissa M. Redmiles, Amelia R. Malone, and Michelle L. Mazurek. I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security. In *IEEE Symposium on Security and Privacy*, SP '16, pages 272–288, San Jose, California, USA, May 2016. IEEE.

[73] Elissa M. Redmiles, Michelle L. Mazurek, and John P. Dickerson. Dancing Pigs or Externalities? Measuring the Rationality of Security Decisions. In *ACM Conference on Economics and Computation*, EC '18, pages 215–232, Ithaca, New York, USA, June 2018. ACM.

[74] Robert W. Reeder, Adrienne Porter Felt, Sunny Consolvo, Nathan Malkin, Christopher Thompson, and Serge Egelman. An Experience Sampling Study of User Reactions to Browser Warnings in the Field. In *ACM Conference on Human Factors in Computing Systems*, CHI '18, pages 512:1–512:13, Montreal, Quebec, Canada, April 2018. ACM.

[75] Ken Reese, Trevor Smith, Jonathan Dutson, Jonathan Armknecht, Jacob Cameron, and Kent Seamons. A Usability Study of Five Two-Factor Authentication Methods. In *Symposium on Usable Privacy and Security*, SOUPS '19, pages 357–370, Santa Clara, California, USA, August 2019. USENIX.

[76] Joshua Reynolds, Nikita Samarin, Joseph Barnes, Taylor Judd, Joshua Mason, Michael Bailey, and Serge Egelman. Empirical Measurement of Systemic 2FA Usability. In *USENIX Security Symposium*, SSYM '20, pages 127–143, Virtual Conference, August 2020. USENIX.

[77] Joshua Reynolds, Trevor Smith, Ken Reese, Luke Dickinson, Scott Ruoti, and Kent E. Seamons. A Tale of Two Studies: The Best and Worst of YubiKey Usability. In *IEEE Symposium on Security and Privacy*, SP '18, pages 872–888, San Francisco, California, USA, May 2018. IEEE.

[78] Ronald W. Rogers and Steven Prentice-Dunn. Protection Motivation Theory. In David S. Gochman, editor, *Handbook of Health Behavior Research I: Personal and Social Determinants*, pages 113–132. Plenum Press, New York, New York, USA, August 1997.

[79] Scott Ruoti, Nathan Kim, Ben Burgon, Timothy van der Horst, and Kent Seamons. Confused Johnny: When Automatic Encryption Leads to Confusion and Mistakes. In *Symposium on Usable Privacy and Security*, SOUPS '13, pages 5:1–5:12, Newcastle, United Kingdom, July 2013. ACM.

[80] Navdeep S. Sahni, S. Christian Wheeler, and Pradeep K. Chintagunta. Personalization in Email Marketing: The Role of Non-Informative Advertising Content. Technical Report 3409, Stanford University Graduate School of Business, February 2016.

[81] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish. In *Symposium on Usable Privacy and Security*, SOUPS '07, pages 88–99, Pittsburgh, Pennsylvania, USA, July 2007. ACM.

[82] Imani N. Sherman, Elissa M. Redmiles, and Jack W. Stokes. Designing Indicators to Combat Fake Media. *CoRR*, abs/2010.00544:1–26, October 2020.

[83] Brian Stanton, Mary F. Theofanos, Sandra Spickard Prettyman, and Susanne Furman. Security Fatigue. *IT Professional*, 18(5):26–32, September 2016.

[84] Dennis Strouble, Gregory M. Shechtman, and Alan S. Alsop. Productivity and Usability Effects of Using a Two-Factor Security System. In *Southern Association for Information Systems Conference*, SAIS '09, pages 196–201, Charleston, South Carolina, USA, March 2009. AIS.

[85] Mary Theofanos, Simson Garfinkel, and Yee-Yin Choong. Secure and Usable Enterprise Authentication: Lessons from the Field. *IEEE Security & Privacy*, 14(5):14–21, September 2016.

[86] 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 *USENIX Security Symposium*, SSYM '19, pages 1556–1571, Santa Clara, California, USA, August 2019. USENIX.

[87] Hsin-yi Sandy Tsai, Mengtian Jiang, Saleem Alhabash, Robert LaRose, Nora J. Rifon, and Shelia R. Cotten. Understanding Online Safety Behaviors: A Protection Motivation Theory Perspective. *Computers & Security*, 59:138–150, June 2016.

[88] Blase Ur, Felicia Alfieri, Maung Aung, Lujo Bauer, Nicolas Christin, Jessica Colnago, Lorrie Faith Cranor, Henry Dixon, Pardis Emami Naeini, Hana Habib, Noah Johnson, and William Melicher. Design and Evaluation of a Data-Driven Password Meter. In *ACM Conference on Human Factors in Computing Systems*, CHI '17, pages 3775–3786, Denver, Colorado, USA, May 2017. ACM.

[89] Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L. Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation. In *USENIX Security Symposium*, SSYM '12, pages 65–80, Bellevue, Washington, USA, August 2012. USENIX.

[90] Anthony Vance, David Eargle, Kirk Ouimet, and Detmar Straub. Enhancing Password Security through Interactive Fear Appeals: A Web-based Field Experiment. In *Hawaii International Conference on System Sciences*, HICSS '13, pages 2988–2997, Wailea, Maui, Hawaii, USA, January 2013. IEEE.

[91] Meridel Walkington. Designing Better Security Warnings, March 2019. https://blog.mozilla.org/ux/2019/03/designing-better-security-warnings/, as of June 2, 2021.

[92] Rick Wash. Folk Models of Home Computer Security. In *Symposium on Usable Privacy and Security*, SOUPS '10, pages 11:1–11:16, Redmond, Washington, USA, July 2010. ACM.

[93] Jake Weidman and Jens Grossklags. I Like It, but I Hate It: Employee Perceptions Towards an Institutional Transition to BYOD Second-Factor Authentication. In *Annual Conference on Computer Security Applications*, ACSAC '17, pages 212–224, Orlando, Florida, USA, December 2017. ACM.

[94] Alex Weinert. Your Pa$$word Doesn't Matter, September 2019. https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984, as of June 2, 2021.

[95] Alex Weinert. It's Time to Hang Up on Phone Transports for Authentication, October 2020. https://techcommunity.microsoft.com/t5/azure-active-directory-identity/it-s-time-to-hang-up-on-phone-transports-for-authentication/ba-p/1751752, as of June 2, 2021.

[96] Catherine S. Weir, Gary Douglas, Tim Richardson, and Mervyn Jack. Usable Security: User Preferences for Authentication Methods in eBanking and the Effects of Experience Author Links Open Overlay Panel. *Interacting with Computers*, 22(3):153–164, May 2010.

[97] Stephan Wiefling, Markus Dürmuth, and Luigi Lo Iacono. More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-based Authentication. In *Annual Conference on Computer Security Applications*, ACSAC '20, pages 203–218, Virtual Conference, December 2020. ACM.

[98] Aiping Xiong, Tianhao Wang, Ninghui Li, and Somesh Jha. Towards Effective Differential Privacy Communication for Users' Data Sharing Decision and Comprehension. In *IEEE Symposium on Security and Privacy*, SP '20, pages 392–410, San Francisco, California, USA, May 2020. IEEE.