

The Framework of Security-Enhancing Friction: How UX Can Help Users Behave More Securely

Verena Distler

University of Luxembourg
Esch-sur-Alzette, Luxembourg
verena.distler@uni.lu

Carine Lallemand

University of Luxembourg
Eindhoven University of Technology
Esch-sur-Alzette / Eindhoven, Luxembourg / Netherlands
carine.lallemand@uni.lu

Gabriele Lenzini

University of Luxembourg
Interdisciplinary Centre for Security, Reliability and Trust
Luxembourg, Luxembourg
gabriele.lenzini@uni.lu

Vincent Koenig

University of Luxembourg
Esch-sur-Alzette, Luxembourg
vincent.koenig@uni.lu

ABSTRACT

A growing body of research in the usable privacy and security community addresses the question of how to best influence user behavior to reduce risk-taking. We propose to address this challenge by integrating the concept of user experience (UX) into empirical usable privacy and security studies that attempt to change risk-taking behavior. UX enables us to study the complex interplay between user-related, system-related and contextual factors and provides insights into the experiential aspects underlying behavior change, including negative experiences.

We first compare and contrast existing security-enhancing interventions (e.g., nudges, warnings, fear appeals) through the lens of friction. We then build on these insights to argue that it can be desirable to design for moments of negative UX in security-critical situations. For this purpose, we introduce the novel concept of security-enhancing friction, friction that effectively reduces the occurrence of risk-taking behavior and ensures that the overall UX (after use) is not compromised.

We illustrate how security-enhancing friction provides an actionable way to systematically integrate the concept of UX into empirical usable privacy and security studies for meeting both the objectives of secure behavior and of overall acceptable experience.

CCS CONCEPTS

• **Security and privacy** → **Usability in security and privacy**; *Social aspects of security and privacy*.

KEYWORDS

Usable Security, User Experience, Trust, Friction Design.

ACM Reference Format:

Verena Distler, Gabriele Lenzini, Carine Lallemand, and Vincent Koenig. 2020. The Framework of Security-Enhancing Friction: How UX Can Help

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

NSPW '20, October 26–29, 2020, Online, USA

© 2020 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-8995-2/20/10.

<https://doi.org/10.1145/3442167.3442173>

Users Behave More Securely. In *New Security Paradigms Workshop 2020 (NSPW '20)*, October 26–29, 2020, Online, USA. ACM, New York, NY, USA, 14 pages. <https://doi.org/10.1145/3442167.3442173>

1 INTRODUCTION

Users are exposed to privacy and security risks on a daily basis, and as technology becomes more pervasive, security risks linked to technology use continue to increase [25]. Usable privacy and security (UPS) researchers have developed a wide variety of security-enhancing interventions (e.g., nudges [1], warnings [2, 19], attractors [8, 9], fear appeals [50]) aiming to help users stay secure and protected by avoiding risky behaviors. In this paper, we aim to identify similarities and differences between these interventions, as security-enhancing interventions are often studied separately, making it difficult to compare their effects. Additionally, there is no standardized way of measuring the effects of such security-enhancing interventions. In particular, there is a lack of systematic measurement of experiential factors, which could provide a nuanced understanding of why interventions correlate with certain behavioral outcomes, and overall experience is not always assessed.

We argue that the field of user experience (UX) can help respond to these challenges, as it holds rich insights into emotional, subjective and temporal aspects that affect how a user perceives their interactions with systems [52]. We believe that applying the concept of friction to address security- and privacy-relevant risk-taking behaviors is a promising direction and a highly relevant way of bridging UX and UPS. We thus introduce the concept of *security-enhancing friction* and describe actionable ways to transfer the concept into practice using the large variety of UX methods already available.

This article makes the following contributions:

- We compare and contrast existing security-enhancing interventions through the lens of friction design.
- We introduce the concept of security-enhancing friction and explain how it can help reduce or prevent risk-taking behaviors while keeping overall UX at an acceptable level, thus further bridging the disciplines of UPS and UX.
- We suggest practical guidelines for the use of UX methods to gain a better understanding of the underlying reasons for

privacy- and security-relevant behaviors. In so doing, we contribute to consolidating the objectives of “better security” and “better UX” by developing a framework that integrates both.

2 EXISTING SECURITY-ENHANCING INTERVENTIONS

UPS researchers have designed a large variety of interventions to help people avoid risk-taking behaviors. For the purpose of this article, we term these attempts “security-enhancing interventions”, interventions that intend to reduce, avoid, or correct risk-taking behavior. In the following sections, we summarize important attempts that have been made to encourage more secure behavior. The cited studies are meant to be illustrative rather than exhaustive. In selecting which publications to include, we conducted a search of the ACM Digital Library and gave particular attention to studies appearing in top-tier conferences and journals.

2.1 Nudges

Thaler and Sunstein [56] describe nudges as thoughtful “choice architecture” that can be used to direct users in beneficial directions, that is, to guide them to make decisions that are beneficial to them, without restricting freedom of choice. Nudging acknowledges that subtle differences in system design (e.g., defaults, saliency of features, or feedback) can impact users’ behavior, leading to better or worse outcomes for users [1]. In privacy and security, nudges can guide users to make more privacy-conscious choices. For instance, on social networks, users who attempt to post content publicly can be nudged to reconsider their privacy settings [1]. Another example stems from Twitter, where users are nudged to check their application access settings right after changing their password. This makes it more likely that users will take the suggested action. Nudges can be considered an instance of “soft paternalism” that supports decision-making without restricting the user’s choices. Nudges have also been applied to direct users towards more secure public wireless networks [57] and to encourage users to make more privacy-conscious decisions on Facebook and mobile permissions interfaces [61, 62, 64]. Peer et al. [45] studied the impact of personalizing nudges to match people’s decision-making styles, rather than using “one-size-fits-all” nudges, and found that personalized nudges can lead to stronger passwords.

Frik et al. [21] explored the use of commitment devices to nudge users towards complying with security mitigations. A commitment device is a mechanism that allows the “present self” to commit to a future action, so that the “future self” is more likely to follow through later. They find that giving people the opportunity to take action at a later time may increase compliance with security mitigations. Renaud and Zimmermann [51] address the ethical questions related to nudging, which is usually based on the premise that nudging should be done for the good of the nudgee, rather than “for profit” or other objectives that are not beneficial to the nudgee, as criticized by the opponents of nudging. Of course, simply “avoiding” nudges is not a realistic option, since there is no such thing as a neutral choice architecture [1]. For instance, in the context of GDPR consent notices, Utz et al. [59] describe how graphical interface

properties such as the position, type of choice and content framing influence people’s consent choices. Renaud and Zimmermann [51] suggest a number of guidelines for ethical nudging based on the principles of ethical research: respect for others, beneficence, justice, scientific integrity and social responsibility.

2.2 Fear appeals

Fear appeals attempt to scare people into taking a particular recommended action to secure their information and devices [50]. The rationale is that emotions can help prompt action, with fear being a powerful emotion. Fear appeals have been applied in various contexts, including phishing [30] and smartphone locking behavior [3, 48]. Renaud and Dupois [50] point out, however, that strong emotions can backfire, lead to adverse outcomes and be ethically questionable. The authors also emphasize the wide variety of measurements used to evaluate the effectiveness of fear appeals, ranging from post-appeal attitudes, general attitudes, behavioral intentions and attitudes, actual behavior and attitudes, attention and behavioral outcomes. This lack of consensus on what needs to be measured makes it difficult to compare the efficacy of fear appeals across different studies, leading the Renaud and Dupois to call for a recommended experiment design protocol that would make it easier to compare studies.

In addition, it is unclear whether fear appeals actually succeed in inducing fear, with many studies relying on a one-item measure that has been found insufficient to evaluate whether fear was induced [7].

2.3 Warnings

Warnings usually aim to remind users about security risks, and are displayed to users when there is a potential threat to information security [63]. While some warnings merely alert users to the presence of a hazard, the most effective warnings generally provide clear instructions about how to avoid it. Effective warnings must capture users’ attention and convince them to take an action to avoid or mitigate a hazard [12]. Warnings are frequently used in UPS, for instance in the context of SSL/TLS warnings, where they are intended to guide confused users to a safe path of action [19].

Another case in which warnings seem to produce security-enhancing results comes from a study by Gorksi and colleagues [23], who asked software developers to complete a short set of programming tasks; they were either assigned to the control group (no warnings) or to the test group, which worked with an API version that integrated security warnings providing secure programming tips. The developers who were exposed to the security warnings created significantly more secure code than the developers in the control group. A later participatory design study with software developers found that design guidelines for end-user warnings are only partially applicable to warnings for developers, who were interested in details such as message classification, title message, code location, link to detailed external resources and color [22].

While warnings have proven effective in many contexts, users become habituated when they are exposed to a large number of warnings. In a 2013 study on SSL, malware and phishing warnings in Chrome and Firefox, Chrome users were significantly more likely to ignore SSL warnings than Firefox users [2]. The authors

hypothesize that this might be because Chrome did not have an exception storing mechanism for certificate errors, which could result in many false positives (warnings that are displayed in non-risky situations) and produce habituation, which the authors called “warning fatigue”. Both polymorphic warnings and attractors aim to counteract warning fatigue, or habituation following repeated exposure to warnings, and encourage users to pay increased attention to warnings or other messages.

2.4 Polymorphic warnings

In order to force users to pay attention to warnings and prevent habituation effects, polymorphic warnings intentionally delay and continuously change the form of the required user inputs [10]. The results demonstrated that users took fewer unjustified risks when presented with polymorphic dialogues compared to traditional warnings. “Audited” polymorphic dialogues, dialogues that warn users that their answers will be forwarded to auditors, who can then quarantine users who provide unjustified answers, performed even better in terms of security, but were not perceived as acceptable. Polymorphic dialogues seem to be more resistant to habituation than static warnings [60], and multiple studies have measured their effect in terms of brain response (functional magnetic resonance imaging or fMRI) [5, 60].

2.5 Attractors

Attractors are user interface modifications that attempt to draw users’ attention to the most important information for decision-making. These attractors can either be purely visual, or temporarily inhibit dangerous behaviors to redirect users’ attention to salient information [9]. Attractors that require the user to interact with the salient information (e.g., retype parts of information) were found to be resistant to habituation [8]. Similarly, Karegar and colleagues [32] investigated the effect of interaction modes and habituation on user attention to privacy notices, concluding that that certain types of interactions (e.g., drag and drop, checkboxes) performed best at getting users’ attention.

3 SIMILARITIES AND DIFFERENCES BETWEEN EXISTING SECURITY-ENHANCING INTERVENTIONS

The security-enhancing interventions described above vary in their level of disruptiveness. To acknowledge these varying levels of disruptiveness, we suggest that security-enhancing interventions can be classified on a scale from high friction to low friction, similarly to how Cranor [12] suggested that “communications that are relevant for security tasks” could be classified on a scale from active (interrupt user’s primary task) to passive (available to the user, but easily ignored).

While some of the security-enhancing interventions above are undoubtedly “high friction” and interrupt the user’s primary task (warnings, polymorphic warnings), others can be located anywhere on the scale and can take more or less disruptive forms (attractors, fear appeals, nudges) as shown in Figure 1.

Table 1 compares and contrasts existing security-enhancing interventions using the following criteria: the objective the intervention



Figure 1: Scale of security communications from low friction (no interruption, easily ignored) to high friction (interruptive, cannot be ignored).

is intended to meet, the intended friction, and how and when the effectiveness of the intervention is measured.

4 SHORTCOMINGS OF EXISTING SECURITY-ENHANCING INTERVENTIONS

Table 1 compares the interventions’ similarities and differences, making some shortcomings apparent:

- The interventions address different focus areas, and are usually studied separately. This makes it hard to compare effectiveness across approaches.
- The sample studies evaluate success very differently, there is no systematic measurement of experiential factors that could provide a nuanced understanding of why interventions correlate with the intended behavioral outcomes, or why they fail.
- The time of measurement also differs substantially across approaches, with most measuring success after exposure. Habituation is not always measured.
- Finally, the interventions are often studied with a focus on the behavioral outcome, that is, whether participants take the intended action; the overall experience and acceptance of the security-enhancing intervention are not always assessed. However, security interventions can lead to negative emotions (e.g., annoyance, circumvention, resignation, avoidance) and could, in the worst-case scenario, lead users to stop using the services that apply such interventions to improve security. Such potential negative outcomes are not always controlled for and mitigated.

In light of the aforementioned difficulties that many security interventions face, we argue that the design of security interventions should build on research from the fields of psychology and user experience, which provide in-depth insights into users’ emotions and psychological needs as well as the temporal aspects of the user experience. Building upon these concepts to work towards more secure user behaviors holds the potential to address existing shortcomings. Therefore, in this paper, we integrate UX theory, in particular research on friction and negative experience, with security research to present a novel, interdisciplinary concept to address the described challenges: security-enhancing friction.

First, it is essential to provide a short overview of UX theory.






Intervention and Objective	Intended friction	Sample evaluation measures	Time of measurement		
			During	After	Long-term
Nudges – Direct users to more privacy- and security-conscious choices	Low  High	Behavioral intention [57, 64], behavioral data [4, 61, 62], usefulness, willingness to use [62], level of comfort [62, 64], creepiness, perceived control of information disclosure, perceived relevance of information requested, privacy concern [64], understanding, reaction after multiple nudges [4]	[4]	[4, 57, 62, 64]	[61]
Fear appeals – Direct users to more privacy- and security-conscious choices using fear	Low  High	Perceived vulnerability [30], perceived security [30], fear [30, 48], response efficacy [3, 30, 48], self-efficacy, response costs [3, 30, 48] S/P concerns [3, 48], perceived severity [3, 48], behavior [3, 48], perceived data value [3]		[3, 30, 48]	[3, 48]
Warnings – Direct users to a choice that prevents a specific hazard	Low  High	Behavioral data (adherence with warnings) [2, 16, 19, 23, 46] understanding of threat source, data risk, and false positives [19], thoughts during exposure to warning, comprehension, attitudes and beliefs, motivation and behavior [16]	[2, 16, 19, 46]	[16, 19, 23, 46]	[16, 19]
Polymorphic warnings – Direct users to a choice that prevents a specific hazard while avoiding habituation effects	Low  High	Behavioral data (adherence with warnings) [10]; time for completing tasks [10], brain response [5, 60], mouse cursor tracking [5], eye tracking [60]	[5, 10, 60]	[5, 10]	[60]
Attractors – Draw users' attention to the most important information	Low  High	Behavioral data (adherence to recommended action), survey questions on whether participants clicked and whether their decision was informed [9]	[9]	[9]	

Table 1: A comparison of security-enhancing interventions according to their objective, intended friction (representing a range), sample evaluation measures and time of measurement. Note that the intended friction can be lowered through habituation: The first time a user is exposed to a warning, friction may be high, but as they continue to be exposed, habituation could make the friction appear lower.

5 USER EXPERIENCE, A GOOD CANDIDATE TO PROVIDE A NUANCED UNDERSTANDING OF SUBJECTIVE EXPERIENCE

User experience (UX) focuses on emotional, subjective and temporal aspects that play a role when users interact with systems [52], taking into account both hedonic (non-instrumental) and pragmatic (instrumental) qualities of experience [40, 41]. Pragmatic qualities are similar to the aspects measured by usability, which has traditionally focused on improving “the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use” (ISO 9241-11). Pragmatic qualities can also be described as “a product’s perceived ability to support the achievement of do-goals” [37], such as sending a text message to someone. Pragmatic qualities relate to the functionality and utility of the product, while hedonic qualities refers to a product’s perceived ability to support the achievement of “be-goals”, such as “being competent” or “being special”. Hasenzahl [27] argues that the fulfilment of be-goals is the driver of experience, meaning that hedonic quality contributes directly to

the core of positive experience. The fulfilment of do-goals can often be seen as a means to fulfilling be-goals. Standardized scales for measuring UX include the Attrakdiff scale, which measures UX along the dimensions of hedonic and pragmatic qualities [28] and the UEQ, which evaluates UX along the dimensions of attractiveness, perspicuity, efficiency, dependability, stimulation, and novelty [36].

Positive experiences are considered to result from fulfilling the human needs for autonomy, competence, security, relatedness, self-actualization/meaning, physical thriving, pleasure/stimulation, money/luxury, self-esteem and popularity/influence [55]. UX is a multi-faceted concept, and security-enhancing interventions can impact different dimensions of UX to varying degrees. For instance, we can hypothesize that an attractor (described in section 2.5) that temporarily inhibits an action could create a moment of negative UX, since the pragmatic quality (achievement of do-goals) of the experience is momentarily compromised, but a carefully designed attractor might not have a negative impact on the overall experience, given that the user’s psychological needs for security and

competence are fulfilled thanks to the slower interaction. A momentary interruption in the user’s action does not necessarily have a negative impact when the user reflects back on the experience.

Thus, when discussing UX, it is important to be conscious of the fact that UX can refer to various time frames (Figure 2). Depending on the context, researchers might be interested in momentary UX (a specific change in feeling during an interaction), episodic UX (perceptions related to a specific usage period) or cumulative UX (views on a system after having used it for a while) [52].

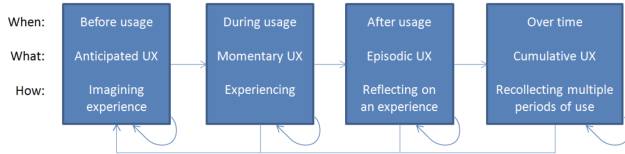


Figure 2: The temporal dynamics of UX [52]

6 DESIGNING FOR NEGATIVE EXPERIENCE AND FRICTION

UX theory and practice tend to focus on positive experiences, leaving many open questions on how negative experiences are created and the effects they may have. To apply UX theory in UPS, we need to take a closer look at negative experiences. In this section, we describe work on negative experiences and build on these examples to illustrate what security-enhancing friction might look like.

Fokkinga and Desmet [20] suggest enriching UX by purposefully involving negative emotions in user-product interaction. They develop the rich experience framework, which combines a negative stimulus that triggers a negative emotion (e.g., anger, sadness, frustration) with protective frames. Their approach involves three steps, in which the designer decides (1) which negative emotion to incorporate into the design, (2) how and when to elicit it and (3) which protective frame to use. The protective frame is defined as an element that takes away the unpleasant aspects of the negative emotions to allow the user to enjoy their beneficial aspects. For example, seeing a lion triggers fear in most people. Adding a protective frame (a cage) to the experience makes it a positive experience. Without fear, the experience would not be enjoyable, as an empty cage would be dull. The authors suggest that there are four types of protective frames: the safety-zone frame (people perceive negative a stimulus but feel protected from it), the detachment frame (people observe an event without participating in it, e.g., watching a movie), control frame (people are in the danger zone but trust they have the skills to protect themselves from harm) and the perspective frame. The perspective frame provides a window to the wider implications of a situation. For instance, one participates in a charity run and feels tired, yet the experience is positive since the pain contributes to an important cause.

Cox and colleagues [11] also highlight that designing friction into interactions by introducing “microboundaries” can have positive effects. The authors define microboundaries as interventions that provide a small obstacle that prevents users from rushing from one context to another by creating a brief moment of reflection.

They define design frictions as points of difficulty encountered during users’ interaction with a technology and describe their potential advantages, such as reducing the likelihood of errors in data entry tasks or supporting health behavior change. They suggest that introducing friction into experiences can disrupt automatic, “mindless” interactions with positive effects, which seems relevant for the security context. The authors compare microboundaries to a smaller version of keeping a credit card encased in a block of ice: you can still get the card out and make purchases, but the time needed for the ice to melt away allows you to think about whether you really want to spend the money.

Studies on design friction indicate that friction might be a powerful way to help people avoid undesirable behaviors, such as wasting electricity [34] or procrastination [35], and instead adopt a “desirable” behavior (help the user attain their goals, living a more energy-efficient life). In order to help people engage in their desired behaviors (e.g., working out or cleaning) instead of procrastinating, Laschke et al. design an object that introduces friction when the user procrastinates by dropping a puck representing the desired task to the floor [35]. This friction intervention induced reflection about procrastination and behavioral change. Another study [34] designed friction to combat standby power consumption by creating a caterpillar-like object connected to a device’s power cord. It “breathes slowly” during normal power consumption, but friction is introduced as soon as the device is left in standby mode, wasting energy. The caterpillar starts twisting awkwardly, creating a link between the abstract concept of energy use and the consequences for the environment. The authors suggest using feedback designed to create situational friction as a way of disrupting routines and suggesting alternative courses of action, while still being perceived as acceptable and meaningful [34]. In some instances, friction can intentionally slow down and interaction to reassure users. For example, a time bar indicating the progress of sending an email can reassure people that their email is being sent; it also provides room for an undo in case of a quick change of mind or a “send” pressed by mistake.

We define friction as follows:

Definition 6.1 (Friction). **Friction** is a momentary perturbation in an otherwise uninterrupted interaction that a user has with a system that does not compromise the user’s experience in the long run or disrupt the user’s trust in the service.

In Section 7.1, we will reflect on how friction can be used to discourage insecure behaviors in digital spaces, but for the time being, let us consider examples of friction that are already used to discourage unsafe behavior in the physical world, for example, while driving.

6.1 Friction in the physical world

Figure 3 shows an example of friction in the physical world. **Speed bumps** are commonly used to discourage drivers from going too fast by introducing friction into the road that the driver cannot avoid. In theory, the option to speed is still open to the driver, but it is easier and more comfortable to adopt the safe behavior of slowing down than to opt for the unsafe option. Another interesting attribute of the pictured speed bump is that it allows bicycles to pass by on the side without slowing down. We can see this as

symbolic for different types of users, some of which need to be exposed to friction to adopt better behaviors, while others do not. It is also important that friction is used in contexts where it is useful (e.g., speed bumps before pedestrian crossings) rather than in places where it may seem superfluous. If the driver understands the reason of the bumper, for example, close to a school, they may eventually adopt that behavior automatically. In general, however, it is not required that users understand the reason of a friction, or even that they realize the presence of friction, for the friction to have an effect on the users' behavior. A modern ATM machine that delays a user's taking back the money only after they removed the card, eventually will change how users act while withdrawing money, having helped them to grow the habit to expect to see and take back the card first and then the money, which is the reason why the friction was introduced in the first place.

Of course, this example of friction in the real world has some limitations that we can overcome in digital spaces. In this example, the behavior we want to discourage is speeding, and the intended behavior is driving more slowly. In the digital world, simply slowing users down would not always be our sole objective. Instead, we want to redirect their actions to a more secure path, making insecure behaviors harder or less comfortable, and making the encouraged behavior easier to adopt and more comfortable in comparison. While the option to engage in the insecure behavior remains available, the secure behavior is relatively easier to choose.

Another example of friction in the physical world is **rumble strips on highways**. When a driver starts to leave their lane, thus attempting to engage in unsafe behavior, these strips introduce physical friction. Instead of encouraging drivers to slow down, they direct them back to the safe course of action and encourage them to stay in their lane.

Friction is frequently used to improve safety in contexts beyond driving. Firearms include safety mechanisms to prevent accidental firing, child-proof medication bottles use a push-and-turn mechanism to make access more difficult for children. In contexts where security and safety are of highest importance, two persons with separate sets of credentials can be required to perform a high-risk action, from accessing data to launching missiles.

These examples of friction in the physical world demonstrate how friction can encourage certain behaviors over others. Similar approaches are used in the digital sphere. According to Definition 6.1, fear appeals [3, 30, 48], for instance, are attempts to design for friction with short spikes of fear in order to make users behave more securely. However, taking up the notion of friction from a UX perspective, there are several more dimensions we can consider with respect to a negative experience. These call for a better understanding of the interplay between momentary friction, subjective user perceptions, emotions and, eventually, behavioral change for better security. To incorporate these dimensions, we introduce a new concept, which we call "security-enhancing friction".

7 INTRODUCING SECURITY-ENHANCING FRICTION

Based on the theoretical foundations presented in Section 6, we define security-enhancing friction as follows:



Figure 3: Friction in the physical world: speed bumps are used to encourage vehicles to adopt the safer behavior: slowing down. In digital spaces, friction can help encourage a large variety of secure behaviors beyond slowing users down. (Picture by the authors)

Definition 7.1 (Security-enhancing friction). **Security-enhancing friction** is friction that is designed to mitigate the risk of a certain attack by lowering the occurrence of risk-taking behavior without affecting overall episodic UX. Security-enhancing friction can encourage a defined, more secure behavior. Security-enhancing friction may have a momentary negative effect on a user's UX, but overall UX remains within acceptable levels to avoid disuse.

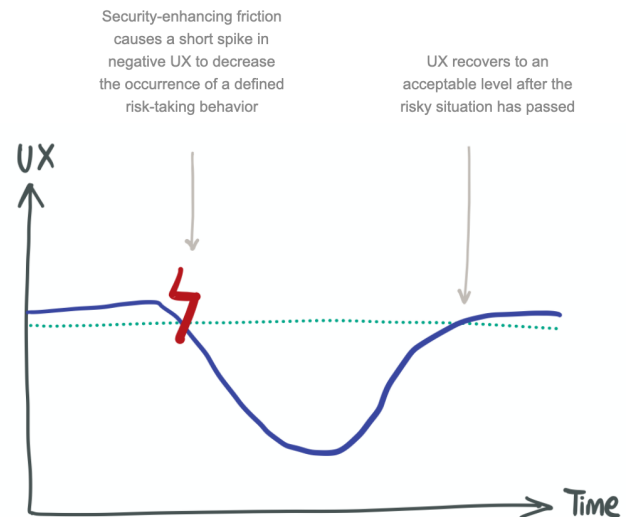


Figure 4: The impact of security-enhancing friction on UX. After the risky situation has passed, UX recovers to an acceptable level.

As described in this definition, and as shown in Figure 4, security-enhancing friction causes a short spike in negative UX, which then recovers to an acceptable level to avoid disuse. Definition 7.1 suggests that we can assess whether a perturbation qualifies as friction by applying UX methods. In order to decide whether a

friction is “security-enhancing”, however, we need to compare it to a solution without friction or with another type of friction so that we can observe its effect on the occurrence of a defined risky behavior. By measuring the occurrence of secure/insecure behavior and UX in combination, we can avoid security interventions that lead to bad UX, and in the worst case, disuse.

What is the advantage of introducing the concept of security-enhancing friction?

Security-enhancing friction, as a concept:

- Helps design interactions that encourage users to avoid risk-taking behaviors while keeping overall UX at an acceptable level, thus contributing to bridging UX theory and usable privacy and security with a useful framework that systematically considers both security concerns and UX concerns. Security-enhancing friction can help avoid interactions that are perceived as “too annoying” or disruptive, and thus avoid disuse of secure technologies.
- Provides a new perspective for understanding security-enhancing interventions through the lens of friction.
- Encourages the use of methods from the fields of psychology and UX to gain a better understanding of the psychological reasons why people engage in certain behaviors. It attempts to facilitate the transfer to practice by providing a set of methods that can be combined to measure the effect of the intervention on security-relevant behavior and on a given user’s experience (both momentary and overall).

We can use the insights from negative experience design described in the previous section to suggest examples of security-enhancing friction.

7.1 Examples of security-enhancing friction

In the digital realm, there are various ways friction can be used to improve security behaviors in design interventions. We will discuss three examples that can improve security behaviors while also providing acceptable UX: password meters, anti-phishing interventions, and SSL/TSL warnings. Note that these examples, and the impact of the described friction design on UX, still need to be backed up by empirical data (as described in Section 9). We use them here to illustrate the concept of security-enhancing friction.

7.1.1 Password meters. Password meters indicate whether a user’s password is strong or weak (for an example, see Figure 5). They can employ a variety of interaction attributes, including the strategic use of colors, a comparison to other people’s passwords [17], size of the password meter, presence of suggestions for improvement, or the presence of a visual indicator vs. text only [58]. Overall, they have a positive impact on the security of chosen passwords [17, 58].

- Insecure behavior that should be avoided: Use of “insecure” passwords.
- Intended behavior: Set password that is harder to crack.
- Interaction attributes used to induce friction: Colors, comparison to others’ passwords, size of password meter, presence of suggestions for improvement.
- UX is acceptable because: Users can easily evaluate the progress they have made in coming up with a more secure password.

Figure 5: Example of the password meters studied by Ur et al. [58]. Appearance and scoring changed depending on the condition.

Figure 6: To protect against phishing attempts, security-enhancing friction can be used when a link is recognized as suspicious (e.g., button text and link destination do not match) in order to draw the user’s attention to the URL they intend to visit.

7.1.2 Anti-phishing intervention. The second example builds on ideas from Bravo-Lillo and colleagues [8, 9], who successfully tested interventions similar to Figure 6 in the context of plugin installation dialogues. Turning to the context of phishing attempts, we can imagine a system that recognizes suspicious elements in an email, such as a button whose text (e.g., “Go to Amazon”) does not match the associated URL (e.g., “amaz0n.com”). By asking the user to re-type the security-relevant information (the URL), security-enhancing friction could help re-direct the user’s attention and encourage the safer behavior. It is crucial, of course, that such warnings do not appear every time users want to click on a link in an email. Instead, such pop-ups should be a rare exception whenever suspicious elements are discovered in an email.

- Insecure behavior that should be avoided: Clicking mindlessly on a link in an email that seems to be a phishing attempt.

- Intended behavior: Verify certain properties of the email (e.g., sender address, contextual cues, does the URL correspond to what the button says).
- Interaction attributes used to induce friction: Color, contrast, de-activated button, re-typing security-relevant information.
- UX is acceptable because: the threat is clear, the interruption is short.

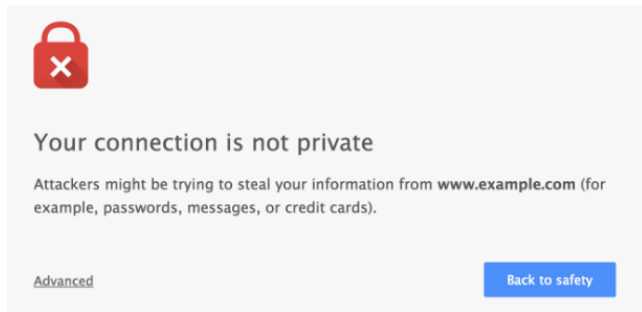


Figure 7: Felt et al. [19] designed a warning for SSL/TLS certificate errors and improved adherence to secure behavior by promoting the secure choice and demoting the insecure choice.

7.1.3 SSL/TLS warnings. Web browsers use SSL/TLS warnings to inform users that the privacy of their connection could be at risk [19]. Their objective is to allow informed decision-making, or at least guide the user to safety. Felt et al. [19] tested different variants of warnings, and found that a modified button placement and design was able to promote the safe choice and demote the unsafe choice (see Figure 7). While not all certificate errors indicate an insecure website, the authors were still able to increase the default secure behavior and lead users back to the previous website. Note that their warning design did not improve user understanding, but nevertheless increased secure behavior.

- Insecure behavior that should be avoided: Visiting a website without a valid SSL/TLS certificate.
- Intended behavior: Go back to the previous website.
- Interaction attributes used to induce friction: Color (red for danger), placement (button hard to find). Users are often forced to leave their navigation path, leading to strong friction.
- UX is acceptable because: Users can still go to the insecure website if they really want to; disruption stays within acceptable bounds.

7.2 Example of a failed attempt at security-enhancing friction

To demonstrate which types of security interventions may lead to disuse of technology, imagine attempting to sign up for an online newspaper subscription. To encourage new subscribers to choose more secure passwords, the website reacts to each attempt to type in an insecure password by changing the placement of the sign-up button and decreasing its contrast, making it harder to see. Thus, after each attempt to sign up with an insecure password, it becomes

harder to sign up, but the user does not get detailed feedback on why the process is so difficult. The UX curve of such a sign-up process would likely look similar to Figure 8, where UX drops at the security-enhancing friction (button changes contrast and placement), but does **not** recover after the intervention. We can consider this a failed attempt to create security-enhancing friction, since UX does not recover, and such a scenario would likely lead users to switch to another website providing similar services.

- Insecure behavior that should be avoided: Use of “insecure” passwords.
- Intended behavior: Set password that is harder to crack.
- Interaction attributes used to induce friction: Placement of sign-up button, contrast.
- UX is **not** acceptable because: Friction is too high and user does not get sufficient feedback explaining the difficulties.

Note that this is an imaginary use case intended to illustrate the possibility of introducing friction that is too strong and leads to a persistent drop in overall UX. To confirm whether this example is really a failed attempt, the impact of the described design interventions would need to be measured empirically (see Section 9). This example also illustrates how business interests and security interests can impact each other. Secure passwords improve the user’s resilience to attacks, but strong friction as described above will lead to disuse and lack of sign-ups to the service. This exemplifies the importance of empirical user research when implementing security measures that impact a users’ experience with a product or service.

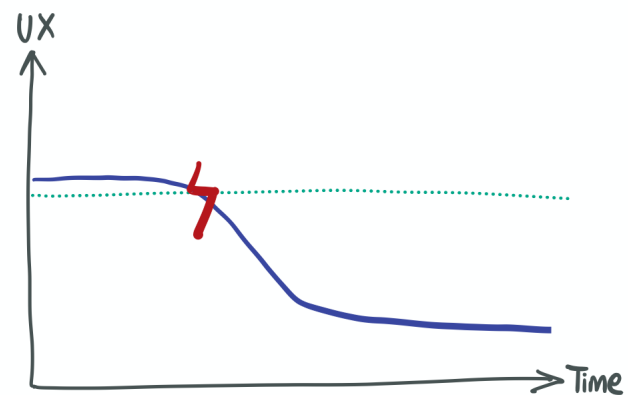


Figure 8: When UX does not recover to an acceptable level after the risky situation has passed, friction can lead to disuse, and thus does not fulfill the requirements of security-enhancing friction.

8 HOW TO INDUCE SECURITY-ENHANCING FRICTION

The examples in the previous section demonstrate a wide variety of ways design can be used to induce friction. Color, contrast, step-wise advancement, placement of buttons, sound and more can be used. We refer to these ways of *how* to induce friction as interaction attributes, similar to the interaction attributes used in UX design when defining interaction aesthetics [38].

Table 2 shows examples of interaction attributes that can be used by designers to induce security-enhancing friction.

Category	Induces less friction	Induces more friction
Speed	fast	slow
Steps	one step	several steps
Color	muted	flashy
Contrast	high contrast	low contrast
Typography	more legible	less legible
Conventions	follows design conventions	does not follow design conventions
Placement	directly visible	needs scrolling
Input	no manual input, one click	needs manual inputs
Complexity	straight-forward	complex
Sound	silent	loud
Movement	static	moving
Physical vibration	slight	strong

Table 2: Examples of interaction attributes that can be used to induce security-enhancing friction. These attributes represent a continuum. The attributes can influence each other, and combining multiple attributes can lead to higher friction.

Designers may worry that introducing security-enhancing friction could lead to disuse of their product or service. Disuse would be the result of friction that creates overly negative UX (i.e., UX that does not recover to acceptable levels). To avoid such negative user experience, it is important to consider which interaction attributes are appropriate for the users of a specific interaction. For instance, when users of a website are typically pressed for time (e.g., when attempting to buy a product that sells out quickly), introducing friction that slows them down would not be a wise choice and UX would likely not recover if they were not able to buy the product in time. Instead, a designer of friction would need to align use of other interaction attributes (Table 2) with the objectives and motivations a user has for an interaction. For example, changing colour, contrast, typography, or even using physical vibration could be more appropriate for users who are typically under time pressure. A rich understanding of typical user objectives and motivations can be achieved through user research.

Second, it is imperative that designers carefully measure the impact of any friction they introduce with a representative sample of users, through empirical measures of momentary, episodic and long-term UX of an interaction that includes security-enhancing friction. Note that any friction will impact certain qualities of UX more strongly than others. For instance, slowing down an interaction by asking a user to re-type an URL (as displayed in Figure 6) could impact the pragmatic quality (achievement of “do-goals”) of an experience, but at the same time could improve hedonic quality of the experience (achievement of “be-goals”, see Section 5) by fulfilling the psychological need for security and control. When deciding which UX dimensions to retain when designing for friction

and which ones to momentarily compromise, both the objectives and motivations of the user, as well as security, need to be carefully balanced.

In the next section, we describe how designers can obtain such detailed and nuanced measures of UX in order to understand the impact of friction, fine-tune friction design and avoid disuse.

9 HOW TO MEASURE THE SUCCESS OF SECURITY-ENHANCING FRICTION

In this section, we suggest a framework for systematically measuring the effects of security-enhancing friction in a nuanced way based on UX theory. By “systematic measurement”, we mean nuanced measurements that can be applied across studies and take the temporal aspect of UX into consideration.

In order to transfer the concept of security-enhancing friction to practice, we suggest applying a range of experience evaluation methods to security- and privacy-relevant contexts to systematically integrate both experience-based and behavioral measures. Table 2 describes how researchers and designers can measure the temporal dynamics of UX throughout a privacy/security-relevant interaction in order to achieve the intended security-enhancing friction experience at each step. In addition, security-enhancing friction needs to lower the likelihood of a defined risk-taking behavior, thereby reducing the likelihood of a successful attack (while keeping overall UX at an acceptable level). The combination of empirical methods (Table 3) also enables researchers and designers to understand the impact of various types and combinations of security interventions have on their user experience and behavior.

The described methods are meant as suggestions for how to evaluate users’ experience with security-enhancing friction at various time points, which should be combined deliberately and with care. For instance, the think-aloud method is usually combined with another method, such as user tests. User tests usually also include an interview or questionnaires to obtain more complete observations of how participants interact. This remark holds true for all phases of the experience evaluation.

While, as described in Table 3, behavioral intention can be used as an approximation of behavior when behavioral data is not readily available, some measurement of behavior as a ground truth would be advisable. Redmiles et al. [49], for instance, systematically compare real-world data to self-reported results with a focus on updating behavior. They show that self-reported data largely varies consistently and systematically with measured data in the context of software updates.

Note that creating understanding of security concepts is not the primary goal of security-enhancing friction, just like physical speed bumps or rumble strips do not attempt to help drivers understand specific safety issues. Instead, the goal is to make the insecure action less attractive through friction and make the secure course of action relatively more attractive, all while keeping UX at an acceptable level.

Table 3 includes knowledge-based measures of success, since the goal may be to improve understanding of security concepts in certain contexts. An example might be “private” browsing modes, which are often perceived as more secure by users than warranted [26]. In this context, improving understanding of the actual security

What is measured	At what stage	Evaluation methods	Intended experience
Experience-based			
Momentary UX	While using a technology	<p>When assessing the effects of security-enhancing friction, participants will likely be asked to interact with a prototype or finished product – for instance, through a user test. In this context, the think-aloud method [39] can be applied to assess momentary UX. This method consists of asking people to think aloud while solving a problem or during an interaction. The think-aloud method allows researchers to understand whether the security-enhancing friction created the intended short spike of negative UX and whether UX recovers afterwards. If used in pre-tests, the think-aloud method should also be used to verify that the spike of momentary UX is not too strong.</p> <p>Psychophysiological measurements are another option to understand momentary experience. Eye tracking [47] can give insights into privacy and security perceptions, as used for instance by [43] to compare Facebook interfaces tailored for privacy support by analyzing differences in gaze patterns and areas of interest between the interfaces.</p> <p>Facial Action Coding (FACS) [18] is another promising method used to categorize facial movements and match them with categories of emotional expressions. fMRI scans are a way of understanding brain responses to stimuli, which have been used to understand habituation to warnings in the past [5, 60]. Most psychophysiological measurements work best when triangulated with other methods for richer experiential insights.</p>	Momentary UX should be lowered so that the user has an appropriate perception of their current risk (see Figure 4).
Episodic UX	After using a technology	To evaluate experience after use, qualitative tools such as focus groups or interviews can give rich insights into participants' experience with a security-enhancing friction; examples include [15, 53]. Standardized questionnaires can help gain comparable insights based on theory. Good candidates for measuring overall UX include the UEQ questionnaire [36], AttrakDiff [28], and Psychological Needs Questionnaire [55]. The Geneva Emotions Wheel can help evaluate overall emotions after use [54].	After an interaction, the user should have an acceptable UX overall; the momentary drop in UX should not have overly impeded their experience.
Long-term/cumulative UX	After multiple uses	<p>When conducting an asynchronous study on security-enhancing friction, researchers can also use the diary method [6] and ask participants to write down certain elements or take pictures of moments where they felt a short spike of negative UX in security- and privacy-related situations. The diary method has been used by [29, 42] to study privacy/security topics.</p> <p>Retrospective UX evaluation methods such as the UX Curve [33] can assist users in retrospectively reporting how their experience changed over time. The UX Curve is based on retrospective user reporting, where users themselves indicate their experience over time. For security-enhancing friction, the UX curve can help evaluate and visualize whether there was a momentary drop in UX, which then recovered to an acceptable level.</p>	After multiple uses, the user should continue to have an acceptable UX overall and have adopted the technology.
Behavior-based			
Occurrence of risk-taking behavior	After exposure to the intervention	Risk-taking behavior can take many forms (e.g., continuously postponing updates to a later point, sending sensitive data over insecure channels). If possible, the occurrence of the risk-taking behavior should be measured through activity logs or observations. If direct measurement is not feasible, behavioral intention can be an easier-to-operationalise alternative.	The occurrence of risk-taking behavior should be lowered by the security-enhancing friction as compared to a control group.
Optional: Knowledge-based			
Understanding of security-relevant processes	After using a technology	Relevant knowledge questions can be used to understand whether a security-enhancing friction improved user understanding. The level of knowledge users should acquire through an interaction must be defined a priori. Most interactions will not aim at expert understanding of a technology. Refer to [19, 26] for an example in UPS.	Note that creating understanding of security issues is not the primary goal of friction, but understanding might be an intended effect in certain contexts.

Table 3: Methods to measure effects of security-enhancing interventions in a nuanced way, enabling the design of security-enhancing friction.

properties of private browsing modes may be achieved through security-enhancing friction.

10 DISCUSSION

10.1 Novelty

Table 1 shows that a number of security-enhancing interventions already exist, and Section 7.1. gives some examples of existing interventions that might be considered security-enhancing friction. Thus, one might question the novelty of our suggested approach. To the best of our knowledge, we are the first to compare security-enhancing interventions (e.g., nudges, warnings, fear appeals), which have to date been studied extensively but mostly separately. We compare and contrast them through the notion of friction, thus providing a means to reflect on the effect these interventions may have on the user experience.

Our original contribution is the introduction of the notion of security-enhancing friction enables the systematic, actionable and controlled migration, and subsequent integration, of UX concepts into usable privacy and security. Unlike previous concepts, security-enhancing friction encompasses both the objective of stimulating secure behavior and of maintaining an acceptable overall user experience. In this work, we strive to contribute to the further bridging of UX and security, which will be of mutual benefit to both fields: security can build on methods from UX and theories grounded in psychology, while UX can be extended to include a security dimension, thus expanding the concept to the support of users' privacy and security.

10.2 Cumulative friction of security tasks and security-enhancing friction

One might question whether security-enhancing friction simply adds to the existing "friction" of having to complete certain security tasks, such as creating a new password. Note, however, that security-enhancing friction does not necessarily coincide with security tasks, instead it can support existing security tasks. As in the example of a password meter giving feedback to users, the form that requests us to choose a password, is already there. Security-enhancing friction attempts to improve the strength of the chosen password. The user could still fail the purpose of the security task, by choosing a guessable password. Actually, the "friction" of having to choose a new password and the security-enhancing friction of the password meters are not necessarily additive.

A security-enhancing friction can lighten the burden of having to choose a new password; the color of the bar can help the user's experience with the original security task of creating a new password by letting them succeed faster and with better quality of result, sparing them an otherwise long sequence of unsuccessful attempts, or the unpleasant surprise to have their password guessed by an intruder.

10.3 Habituation

Habituation might be a threat to the effectiveness of friction, as is the case for most security-enhancing interventions (e.g., warnings [2, 19, 23]). Longitudinal studies could reveal whether frictions are vulnerable to this threat. The concept and methods proposed

in this article can help address habituation given that they allow us to understand temporal dynamics linked to friction, and this understanding can be used to periodically adapt the form of a friction element for which habituation is known to occur.

UX methods even have the advantage of detecting the effects of habituation on the experience level (e.g., decrease in perceived friction) before they have behavioral consequences. As such, they can also contribute to exploring the thresholds for "sufficient" friction to reliably expect an adequate behavioral response. Habituation might not occur in other contexts, such as systems that are only used for certain occasions (e.g., e-voting). Previous studies have reported on promising approaches that seem resistant to habituation, such as the use of polymorphic dialogues (dialogues that change the required form of user input) [5, 60], opinionated design (visual design techniques to promote the safe choice as the preferred option) [19] or certain attractors (interface modifications that attempt to draw user's attention to important information, for instance by promoting interaction with salient information) [8].

10.4 Ethical challenges

There are two levels of ethical challenges that we find compelling.

First, on an experimental level, and in line with UPS experiments in general, research on friction design will inevitably run into the ethical challenge of exposing users to a certain level of risk, which can sometimes lead to the use of deception in user studies. Cranor and Buchler [13] point out that in the context of computer security warnings, it can be necessary to lead participants to believe that there is some actual risk involved. Such approaches make integrating ethical considerations at all stages of experiment design obligatory.

From another point of view, friction might seem unethical at first glance because it introduces a barrier to action, thus decreasing users' autonomy. However, given that security-enhancing friction is designed to keep UX constant, such friction is inherently positive for the user, since it aligns security and UX. We think that the concept of security-enhancing friction can help advance this discussion by providing a nuanced understanding of users' experience when using security-enhancing friction. For instance, Renaud and Zimmermann [51] outline ethical challenges linked to nudges, and suggest that there should be a reasonable plan for monitoring the effect of the intervention and for discontinuing it if unintended side effects are detected. Security-enhancing friction encourages such nuanced measurement of the effects of an intervention.

10.5 Similarities and differences to other concepts

Our definition of security-enhancing friction bears similarity to "soft paternalism" or nudges as defined by Acquisti et al., [1] in support of privacy and security decision-making. The difference is that security-enhancing friction encourages the use of UX methods for a nuanced measurement of momentary negative UX, while safeguarding an acceptable overall UX for users. The mere use of behavioral measurements does not allow researchers and designers to determine the success of security-enhancing friction.

One might also draw parallels to Kahneman's [31] dual processing theory, which differentiates between two modes of thought,

system one (fast, instinctive and emotional) and system two (slower, deliberative, logical), and was previously applied to the context of security by Dennis and Minas [14]. These authors argue that security behaviors are mostly determined by system one cognition, which may issue an alert if it detects a surprise or anomaly. In this case, system two thinking can take over and potentially trigger a more deliberate response. The authors give some examples of how to trigger a switch from system one to system two thinking. For instance, an organization could apply aversion training by regularly sending out fake phishing emails and then lock individuals who click on them out of their account for 15 minutes. Another example is triggering a loud alarm whenever a person clicks on a phishing email. One could also change situational normality by prohibiting all organizational emails from containing a clickable link; any email containing a link would thus become suspicious. This has some parallels to our approach. Dennis and Minas' suggested interventions introduce friction into an experience in order to trigger deliberate system two thinking. However, extreme interventions can lead to strong negative emotions among an organization's employees (e.g., shame, frustration), potentially decreasing motivation and productivity. These shortcomings make it unlikely, in our eyes, that such measures will be applied in organizations. In cases where users are free to switch away from a service that exposes them to such extreme interventions for security's sake, they might well choose to use another service provider. This makes it necessary to find a more balanced approach to trigger system two thinking.

Thus, while our approach has a similar objective, interventions that have a lasting deleterious effect on user experience cannot be considered security-enhancing friction according to our definition. Security-enhancing friction also requires the nuanced measurement of people's experiences during and after an interaction to ensure that lasting negative impressions or exceedingly strong negative emotions can reliably be avoided. The security-enhancing friction approach we describe in this paper could therefore enhance the dual processing framework by offering a controlled empirical approach to influencing switching between the two modes.

One might also relate our approach to dark patterns, which are part of a larger research agenda around persuasive design and nudges [44]. Dark patterns are defined as interface designs that try to guide end-users to desired behavior through malicious interaction flows [24]. The difference is that security-enhancing friction, per definition, is designed in the interest of the user (on both a UX and a security level), while dark patterns are not designed with the user's best interest in mind. However, whenever design methods are applied with the objective of changing behaviors, the question arises as to for "whose good" nudges, and by extension security-enhancing frictions, are designed [51].

11 CONCLUSION

In this paper, we argue that in the security context, it can be desirable to use UX methods to design for moments of negative UX in security-critical situations. We compare and contrast existing security-enhancing interventions that are frequently studied separately (e.g., nudges, warnings, fear appeals) through the common lens of friction. Building on these insights, we introduce the novel

framework of security-enhancing friction, which provides an actionable way to systematically integrate the concept of user experience into empirical UPS studies and ensure that both the objective of secure behavior and of an acceptable overall experience can be met. Through this work, we strive further bridge the disciplines of user experience and privacy/security, and we hope that this article is the first of many investigating how to intentionally create temporary negative experiences through nuanced friction design when it is in the user's interest.

ACKNOWLEDGMENTS

We acknowledge support from the National Research Fund (FNR) under Grant Number PRIDE15/10621687. We thank our shepherds Alisa Frik and Simon Parkin who provided valuable feedback on this paper. We also thank the anonymous reviewers and all NSPW participants for their thoughtful and constructive comments.

REFERENCES

- [1] Alessandro Acquisti, Manya Sleeper, Yang Wang, Shomir Wilson, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, and Florian Schaub. 2017. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *Comput. Surveys* 50, 3 (Aug. 2017), 1–41. <https://doi.org/10.1145/3054926>
- [2] Devdatta Akhawe and Adrienne Porter Felt. 2013. Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness. In *22nd USENIX Security Symposium (USENIX Security 13)*. USENIX Association, Washington, D.C., 257–272. <https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/akhawe>
- [3] Yusuf Albayram, Mohammad Maifi Hasan Khan, Theodore Jensen, and Nhan Nguyen. 2017. "...better to use a lock screen than to worry about saving a few seconds of time": Effect of Fear Appeal in the Context of Smartphone Locking Behavior. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS '17)*. USENIX Association, 49–63. <https://www.usenix.org/conference/soups2017/technical-sessions/presentation/albayram>
- [4] Hazim Almuhiemedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 2015. Your Location Has Been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging. In *Proceeding of the Annual Conference on Human Factors in Computing Systems (CHI '15)*. ACM, 787–796. <https://doi.org/10.1145/2702123.2702210>
- [5] Bonnie Brinton Anderson, C. Brock Kirwan, Jeffrey L. Jenkins, David Eargle, Seth Howard, and Anthony Vance. 2015. How Polymorphic Warnings Reduce Habituation in the Brain: Insights from an fMRI Study. In *Proceedings of the Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, 2883–2892. <https://doi.org/10.1145/2702123.2702322>
- [6] Ruth Bartlett and Christine Milligan. 2015. *What is diary method?* Bloomsbury Academic.
- [7] Franklin J. Boster and Paul Mongeau. 1984. Fear-Arousing Persuasive Messages. *Annals of the International Communication Association* 8, 1 (Jan. 1984), 330–375. <https://doi.org/10.1080/23808985.1984.11678581>
- [8] Cristian Bravo-Lillo, Lorrie Faith Cranor, Saranga Komanduri, Stuart Schechter, and Manya Sleeper. 2014. Harder to Ignore? Revisiting Pop-Up Fatigue and Approaches to Prevent It. In *10th Symposium On Usable Privacy and Security (SOUPS '14)*. USENIX Association, 105–111. <https://www.usenix.org/conference/soups2014/proceedings/presentation/bravo-lillo>
- [9] Cristian Bravo-Lillo, Saranga Komanduri, Lorrie Faith Cranor, Robert W. Reeder, Manya Sleeper, Julie Downs, and Stuart Schechter. 2013. Your Attention Please: Designing Security-decision UIs to Make Genuine Risks Harder to Ignore. In *Proceedings of the Ninth Symposium on Usable Privacy and Security - SOUPS '13*. Newcastle, United Kingdom, 1. <https://doi.org/10.1145/2501604.2501610>
- [10] José Carlos Brustoloni and Ricardo Villamarin-Salomón. 2007. Improving Security Decisions with Polymorphic and Audited Dialogs. In *Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS '07)*. ACM Press, Pittsburgh, Pennsylvania, 76. <https://doi.org/10.1145/1280680.1280691>
- [11] Anna L. Cox, Sandy J.J. Gould, Marta E. Cecchinato, Ioanna Iacovides, and Ian Renfree. 2016. Design Frictions for Mindful Interactions: The Case for Microboundaries. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems - CHI EA '16*. ACM Press, Santa Clara, California, USA, 1389–1397. <https://doi.org/10.1145/2851581.2892410>
- [12] Lorrie Faith Cranor. 2008. A Framework for Reasoning about the Human in the Loop. In *Proceedings of the 1st Conference on Usability, Psychology, and Security*. USENIX Association, USA.

- [13] Lorrie Faith Cranor and Norbou Buchler. 2014. Better Together: Usability and Security Go Hand in Hand. *IEEE Security & Privacy* 12, 6 (Nov. 2014), 89–93. <https://doi.org/10.1109/MSP.2014.109>
- [14] Alan R. Dennis and Randall K. Minas. 2018. Security on Autopilot: Why Current Security Theories Hijack Our Thinking and Lead Us Astray. *SIGMIS Database* 49, SI (April 2018), 15–38. <https://doi-org.proxy.bnl.lu/10.1145/3210530.3210533>
- [15] Verena Distler, Carine Lallemand, and Vincent Koenig. 2020. How Acceptable Is This? How User Experience Factors Can Broaden our Understanding of The Acceptance of Privacy Trade-offs. *Computers in Human Behavior* 106 (May 2020), 106227. <https://doi.org/10.1016/j.chb.2019.106227>
- [16] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. 2008. You've Been Warned: an Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In *Proceedings of the Annual ACM Conference on Human Factors in Computing Systems (CHI '08)*. ACM Press, Florence, Italy, 1065. <https://doi.org/10.1145/1357054.1357219>
- [17] Serge Egelman, Andreas Sotirakopoulos, Ildar Muslukhov, Konstantin Beznosov, and Cormac Herley. 2013. Does my Password go up to Eleven?: the Impact of Password Meters on Password Selection. In *Proceedings of the Annual ACM Conference on Human Factors in Computing Systems (CHI '13)*. ACM, Paris, France, 2379–2388.
- [18] Rosenberg Ekman. 1997. *What the Face Reveals: Basic and Applied Studies of Spontaneous Expression Using the Facial Action Coding System (FACS)*. Oxford University Press, USA.
- [19] Adrienne Porter Felt, Alex Ainslie, Robert W. Reeder, Sunny Consolvo, Somas Thyagaraja, Alan Bettis, Helen Harris, and Jeff Grimes. 2015. Improving SSL Warnings: Comprehension and Adherence. In *Proceedings of the Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, 2893–2902. <https://doi.org/10.1145/2702123.2702442>
- [20] Steven Fokkinga and Pieter Desmet. 2012. Darker Shades of Joy: The Role of Negative Emotion in Rich Product Experiences. *Design Issues* 28, 4 (Oct. 2012), 42–56. https://doi.org/10.1162/DESI_a_00174
- [21] Alisa Frik, Nathan Malkin, Marian Harbach, Eyal Peer, and Serge Egelman. 2019. A promise is a promise: The Effect of Commitment Devices on Computer Security Intentions. In *Proceeding of the Annual Conference on Human Factors in Computing Systems (CHI '19)*. 1–12.
- [22] Peter Leo Gorski, Yasemin Acar, Luigi Lo Iacono, and Sascha Fahl. 2020. Listen to Developers! A Participatory Design Study on Security Warnings for Cryptographic APIs. In *Proceeding of the Annual Conference on Human Factors in Computing Systems (CHI '20)*. Association for Computing Machinery, Honolulu, HI, USA. <https://doi-org.proxy.bnl.lu/10.1145/3313831.3376142>
- [23] Peter Leo Gorski, Luigi Lo Iacono, Dominik Wermke, Christian Stransky, Sebastian Möller, Yasemin Acar, and Sascha Fahl. 2018. Developers Deserve Security Warnings, Too: On the Effect of Integrated Security Advice on Cryptographic API Misuse. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS '18)*. USENIX Association, 265–281. <https://www.usenix.org/conference/soups2018/presentation/gorski>
- [24] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. 2018. The Dark (Patterns) Side of UX Design. In *Proceeding of the Annual Conference on Human Factors in Computing Systems (CHI '18)*. ACM Press, Montreal QC, Canada, 1–14. <https://doi.org/10.1145/3173574.3174108>
- [25] Siddharth Gulati, Sonia Sousa, and David Lamas. 2017. Modelling Trust: An Empirical Assessment. In *Human-Computer Interaction – INTERACT 2017*, Regina Bernhaupt, Girish Dalvi, Anirudha Joshi, Devanuj K. Balkrishan, Jacki O'Neill, and Marco Winckler (Eds.), Vol. 10516. Springer International Publishing, Cham, 40–61. https://doi.org/10.1007/978-3-319-68059-0_3
- [26] Hana Habib, Jessica Colnago, Vidya Gopalakrishnan, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, and Lorrie Faith Cranor. 2018. Away From Prying Eyes: Analyzing Usage and Understanding of Private Browsing. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS '18)*. USENIX Association, 159–175. <https://www.usenix.org/conference/soups2018/presentation/habib-prying>
- [27] Marc Hassenzahl. 2008. User Experience (UX): Towards an Experiential Perspective on Product Quality. In *Proceedings of the 20th International Conference of the Association Francophone d'Interaction Homme-Machine (IHM '08)*. ACM Press, Metz, France, 11. <https://doi.org/10.1145/1512714.1512717>
- [28] Marc Hassenzahl, Michael Burmester, and Franz Koller. 2003. *AttrakDiff: Ein Fragebogen zur Messung Wahrgenommener Hedonischer und Pragmatischer Qualität*. Vieweg & Teubner Verlag, Wiesbaden, 187–196. https://doi.org/10.1007/978-3-322-80058-9_19
- [29] Qatrunnada Ismail, Tousif Ahmed, Apu Kapadia, and Michael K. Reiter. 2015. Crowdsourced exploration of security configurations. In *Proceedings of the Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. 467–476.
- [30] Jurjen Jansen and Paul van Schaik. 2017. Persuading End Users to Act Cautiously Online: Initial Findings of a Fear Appeals Study on Phishing. In *Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017)*.
- [31] Daniel Kahneman. 2011. *Thinking, Fast and Slow*. Farrar, Straus and Giroux.
- [32] Farzaneh Karegar, John Sören Pettersson, and Simone Fischer-Hübner. 2020. The Dilemma of User Engagement in Privacy Notices: Effects of Interaction Modes and Habituation on User Attention. *ACM Transactions on Privacy and Security* 23, 1 (Feb. 2020), 1–38. <https://doi.org/10.1145/3372296>
- [33] Sari Kujala, Virpi Roto, Kaisa Väänänen-Vainio-Mattila, Evangelos Karapanos, and Arto Sinnelä. 2011. UX Curve: A Method for Evaluating Long-term User Experience. *Interacting with Computers* 23, 5 (Sept. 2011), 473–483. <https://doi.org/10.1016/j.intcom.2011.06.005>
- [34] Matthias Laschke, Sarah Diefenbach, and Marc Hassenzahl. 2015. “Annoying, but in a nice way”: An Inquiry into the Experience of Frictional Feedback. *International Journal of Design* 9, 2 (2015), 129–140.
- [35] Matthias Laschke, Marc Hassenzahl, Jan Brechmann, Eva Lenz, and Marion Digel. 2013. Overcoming Procrastination with ReMind. In *Proceedings of the 6th International Conference on Designing Pleasurable Products and Interfaces - DPPI '13*. ACM Press, Newcastle upon Tyne, United Kingdom, 77–85. <https://doi.org/10.1145/2513506.2513515>
- [36] Bettina Laugwitz, Theo Held, and Martin Schrepp. 2008. Construction and Evaluation of a User Experience Questionnaire. In *HCI and Usability for Education and Work*, Andreas Holzinger (Ed.), Vol. 5298. Springer Berlin Heidelberg, Berlin, Heidelberg, 63–76. https://doi.org/10.1007/978-3-540-89350-9_6
- [37] Effie Lai-Chong Law, Arnold P. O. S. Vermeeren, Marc Hassenzahl, and Mark Blythe. 2007. Towards a UX Manifesto. In *Proceedings of the 21st British HCI Group Annual Conference on People and Computers: HCI...But Not As We Know It - Volume 2 (BCS-HCI '07)*. BCS Learning & Development Ltd., Lancaster, UK, 205–206. <http://dl.acm.org/citation.cfm?id=1531407.1531468>
- [38] Eva Lenz, Sarah Diefenbach, and Marc Hassenzahl. 2014. Aesthetics of Interaction: a Literature Synthesis. In *Proceedings of the 8th Nordic Conference on Human-Computer Interaction (NordiCHI '14)*. ACM Press, Helsinki, Finland, 628–637. <https://doi.org/10.1145/2639189.2639198>
- [39] Jacobijn A.C. Sandberg Maarten W. van Someren, Yvonne F. Barnard. 1994. *The Think Aloud Method: A Practical Guide to Modelling Cognitive Processes*. Academic Press.
- [40] Sascha Mahlke. 2005. Understanding Users' Experience of Interaction. In *Proceedings of the 2005 Annual Conference on European Association of Cognitive Ergonomics*. 251–254.
- [41] Sascha Mahlke. 2008. *User Experience of Interaction with Technical systems*. Doctoral Dissertation.
- [42] Shirrang Mare, Mary Baker, and Jeremy Gummeson. 2016. A Study of Authentication in Daily Life. In *Twelfth Symposium on Usable Privacy and Security (SOUPS '16)*. USENIX Association, 189–206. <https://www.usenix.org/conference/soups2016/technical-sessions/presentation/mare>
- [43] Moses Namara and Curtis John Laurence. 2019. What Do You See? An Eye-tracking study of a Tailored Facebook Interface for Improved Privacy Support. *ACM Symposium on Eye Tracking Research & Applications (ETRA)* (2019), 7.
- [44] Midas Nouwens, Ilaria Lliccardi, Michael Veale, David Karger, and Lalana Kalag. 2020. Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence. In *Proceeding of the Annual Conference on Human Factors in Computing Systems (CHI '20)* (Honolulu, HI, USA) (CHI '20). Association for Computing Machinery, New York, NY, USA, 1–13. <https://doi.org/10.1145/3313831.3376321>
- [45] Eyal Peer, Serge Egelman, Marian Harbach, Nathan Malkin, Arunesh Mathur, and Alisa Frik. 2020. Nudge me Right: Personalizing Online Security Nudges to People's Decision-making Styles. *Computers in Human Behavior* (2020), 106347.
- [46] Justin Petelka, Yixin Zou, and Florian Schaub. 2019. Put Your Warning Where Your Link Is: Improving and Evaluating Email Phishing Warnings. In *Proceedings of the Annual ACM Conference on Human Factors in Computing Systems (CHI '19)*. ACM Press, Glasgow, Scotland UK, 1–15. <https://doi.org/10.1145/3290605.3300748>
- [47] Alex Poole and Linden J. Ball. 2006. Eye tracking in HCI and Usability Research. In *Encyclopedia of Human-Computer Interaction*. IGI Global, 211–219.
- [48] Elham Al Qahtani, Mohamed Shehab, and Abrar Aljohani. 2018. The Effectiveness of Fear Appeals in Increasing Smartphone Locking Behavior among Saudi Arabians. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS '18)*. USENIX Association, 31–46. <https://www.usenix.org/conference/soups2018/presentation/qahtani>
- [49] Elissa M Redmiles, Ziyun Zhu, Sean Kross, Dhruv Kuchhal, Tudor Dumitras, and Michelle L Mazurek. 2018. Asking for a Friend: Evaluating Response Biases in Security User Studies. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. 1238–1255.
- [50] Karen Renaud and Marc Dupuis. 2019. Cyber Security Fear Appeals: Unexpectedly Complicated. In *Proceedings of the New Security Paradigms Workshop (NSPW)*. ACM, San Carlos Costa Rica, 42–56. <https://doi.org/10.1145/3368860.3368864>
- [51] Karen Renaud and Verena Zimmermann. 2018. Ethical guidelines for nudging in information security & privacy. *International Journal of Human-Computer Studies* 120 (Dec. 2018), 22–35. <https://doi.org/10.1016/j.ijhcs.2018.05.011>
- [52] Virpi Roto, Effie Law, Arnold Vermeeren, and Jettie Hoonhout. 2011. User Experience White Paper. In *Result from Dagstuhl Seminar on Demarcating User Experience, September 15–18, 2010*. 12.
- [53] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth

- Churchill. 2018. “Privacy is not for me, it’s for those rich women”: Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS '18)*. USENIX Association, 127–142. <https://www.usenix.org/conference/soups2018/presentation/sambasivan>
- [54] Klaus R. Scherer. 2005. What are Emotions? And how can they be Measured? *Social Science Information* 44, 4 (Dec. 2005). <https://doi.org/10.1177/0539018405058216>
- [55] Kennon M. Sheldon, Andrew J. Elliot, Youngmee Kim, and Tim Kasser. 2001. What is Satisfying about Satisfying Events? Testing 10 Candidate Psychological Needs. *Journal of Personality and Social Psychology* 80, 2 (2001), 325.
- [56] Richard H. Thaler and Cass R. Sunstein. 2008. *Nudge: Improving Decisions about Health, Wealth, and Happiness*. New Haven, CT, US.
- [57] James Turland, Lynne Coventry, Debora Jeske, Pam Briggs, and Aad van Moorsel. 2015. Nudging Towards Security: Developing an Application for Wireless Network Selection for Android Phones. In *Proceedings of the 2015 British HCI conference*. 193–201.
- [58] 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. 2012. How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation. In *USENIX Security Symposium (USENIX Security '12)*. USENIX, Bellevue, WA, 65–80.
- [59] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un) informed Consent: Studying GDPR Consent Notices in the Field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. London, United Kingdom, 973–990.
- [60] Anthony Vance, Brock Kirwan, Daniel Bjornn, Jeffrey Jenkins, and Bonnie Brinton Anderson. 2017. What do we Really Know About how Habituation to Warnings Occurs Over Time?: A Longitudinal fMRI Study of Habituation and Polymorphic Warnings. In *Proceeding of the Annual Conference on Human Factors in Computing Systems (CHI '17)*. 2215–2227.
- [61] Yang Wang, Pedro Giovanni Leon, Alessandro Acquisti, Lorrie Faith Cranor, Alain Forget, and Norman Sadeh. 2014. A Field Trial of Privacy Nudges for Facebook. In *Proceeding of the Annual Conference on Human Factors in Computing Systems (CHI '14)*. 2367–2376.
- [62] Yang Wang, Pedro Giovanni Leon, Kevin Scott, Xiaoxuan Chen, Alessandro Acquisti, and Lorrie Faith Cranor. 2013. Privacy Nudges for Social Media: an Exploratory Facebook Study. In *Proceedings of the 22nd International Conference on World Wide Web*. 763–770.
- [63] Bo Zhang, Mu Wu, Hyunjin Kang, Eun Go, and S. Shyam Sundar. 2014. Effects of Security Warnings and Instant Gratification Cues on Attitudes Toward Mobile Websites. In *Proceeding of the Annual Conference on Human Factors in Computing Systems (CHI '14)*. ACM, 111–114. <https://doi.org/10.1145/2556288.2557347>
- [64] Bo Zhang and Heng Xu. 2016. Privacy Nudges for Mobile Applications: Effects on the Creepiness Emotion and Privacy Attitudes. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (CSCW '16)*. ACM Press, San Francisco, California, USA, 1674–1688. <https://doi.org/10.1145/2818048.2820073>