Abstract
Installing software updates is one of the most important security actions that people can take to protect their computer systems. However, people often delay installing updates. Why would people delay installation of security updates, knowing that these updates may reduce the risk of information loss from attacks? In a laboratory experiment, we studied how people learn to make update decisions from past experiences. In a simulated “work” environment, participants could defend against low probability and high impact losses, by installing a security update. The cost of updates was variable; participants could update immediately for a high cost or wait to update for free, risking increased exposure to attacks and losses. Thus, the optimal decision was to update immediately when the update was made available. The results from our experiment indicate people learn from experience to delay security updates. The cost of the update and individual risk preference both significantly predicted the tendency to delay the update; people with higher willingness to take risks may be more likely to neglect to update, keeping the status quo even when it may be sub-optimal. We discuss the implications of these findings for the design of interventions to reduce delays in update installations.

Key words: security updates; decision-making; risk preference; cost; rare events; decisions from experience

Introduction
Systems running vulnerable versions of software, particularly from providers with widespread usage (e.g. Microsoft, Adobe, and OpenSSL), are commonly targeted during cyberattacks [1]. Updates or patches are periodically released to mend such security vulnerabilities. Timely installation of security updates is an important security measure individuals can take to reduce their exposure to attacks [2–4]. While many updates can be applied automatically (e.g. updates to software applications), critical updates, such as an update to the operating system, continue to require human consent and intervention [5–7]. However, people often delay or fail to take this important protective action [8–11]. The delay to install a manual update could be a few days, few weeks, or even months in many instances [8, 10–12]. For example, in the case of the WannaCry ransomware attack, an update to address the vulnerability exploited by that malware was made available weeks before the actual attack. Failure to update caused millions of devices worldwide to be infected [13].

Why would people delay installation of critical security updates that could reduce the risk of information loss from a cyberattack? Understanding what drives people to delay this important protective action is a first step toward solving this problem. Here, we build on behavioral economics and decision-making research to investigate the influence of three possible factors that may lead end-users to delay taking protective decisions: experience, opportunity cost, and individual risk preference.

First, we investigate the effect of individual experience. Every day, people make many recurring decisions with possible adverse outcomes such as crossing a street, wearing a seat belt, choosing to vaccinate, backing up a hard drive, using a strong password, and installing security updates. For such everyday decisions, people typically do not have access to explicit description of the risk. Instead, they primarily rely on their own past experience. For example, one
may decide to reuse a simple, familiar password for an online account because a similar decision from her past experience (as retrieved from memory) did not cause her any harm; in contrast, the decision to use a long password had problematic consequences in the past because she forgot that long password. Studies on decisions on risky choices made from experience have repeatedly found that people tend to underweight the probability of rare events [14, 15]. In the case of security updates, from an end-user perspective, the consequence of delaying to install an update being an attack or breach can be considered a rare event [16]. The more probable outcome of delaying to update would be that nothing happens and the end-user is repeatedly prompted with annoying update reminders. We expect that previous experience would influence people’s beliefs regarding the probabilities of attack, leading them to believe that an attack is less common than it really is, thus influencing their decision to delay an update.

Second, we investigate the effect of opportunity cost. The primary goal of end-users is to use a particular application or system to accomplish their tasks; security is usually a secondary goal, valuable only to the extent that it allows them to preserve their primary goal. Therefore, the cost of choosing a protective action (install update) could involve disruption to their primary work, which will require time, effort, and/or money [16]. For example, a security update may require a system reboot that takes time; or the new update may not function according to individual’s expectation [6, 7, 17, 18]. Here, we investigate whether this opportunity cost of installing an update plays a role in end-user’s choice to delay this action.

Third, we investigate the impact of individual risk preference. Consider two individuals with identical financial condition (Person A and Person B), are presented with a risky, but high-payoff investment. Let’s assume, Person A chooses to make the risky investment whereas Person B rejects the presented opportunity. The difference in their observed behavior could be explained by their individual willingness to take financial risk [19]. Similarly, different individuals choose to update at different speeds. Some choose to update early whereas others typically delay installing an update [20]. Difference in update speeds between individuals could also be explained by their underlying risk-taking “trait” or characteristic. We expect that people with low risk-taking preference would choose to update early [21]. So, in a laboratory experiment, we analyze people’s update decisions (speed of update) and risk-taking behavior with repeated experiences in an environment with variable cost conditions: a costly function according to individual’s expectation [6, 7, 17, 18]. Here, we investigate whether this opportunity cost of installing an update plays a role in end-user’s choice to delay this action.

In what follows, we present a review of relevant literature regarding security updates and behavioral research. Then, we present a novel experimental paradigm, “Repeated Protective Decisions (RPD),” that emulates the end-user’s two main types of decisions: a primary decision task (representing users’ ongoing work) and a secondary task of security update decisions (representing users’ protective decisions), over a course of “days” (trial and periods (e.g. “weeks”). We present the results from this experiment and use a regression model to explain the factors that predict update decisions. Results from this work can be helpful in the design of policies and solutions to mitigate the delay of update decisions and inform the development of security risk models that account for the gaps in human protection actions [22–24].

Related work

With the growing awareness that security is not only a technical problem, but also a social and economic one, recent works on security updates span disciplines such as economics, game theory, and Human-Computer Interaction. From an economics perspective, the current literature has addressed the incentives that drive human decisions to update [25]. Numerous models have been developed to understand the optimal timing of security patch release in relation to the release of vulnerability disclosure [26–29]. However, the majority of these models make idealistic assumptions about human decision-making process, including rationality, homogeneity in human’s risk and cost preferences, and full information conditions, suggesting that humans can interpret situations and make optimal choices based on complete knowledge of the incentive structure (e.g. probability and severity of hazards) [23]. From human factors perspective, several factors have been proposed to explain delay in installing updates, such as disruption to primary work, difficulty in understanding update messages, and individual risk-taking ability.

Disruption to primary work

Disruption to primary work, complementary to the argument about cost and incentives put-forth in the economics literature, is a reason commonly self-reported by users for their delay in installing updates [7, 11, 18, 20, 30–33]. One theory, based on “present bias” [34], suggests people could be delaying the installation of updates because they may be discounting future benefits of updating (avoiding the loss from an exploit) for immediate gratification from their primary task [35, 36]. Many others have suggested the role of past experience influencing security update decisions [6, 7, 18, 31]. For example, Vaniea et al. found that users learn to avoid or delay installing updates for certain applications that made surprise changes to its user interface, impacting productivity and user interaction [31]. Employing forced reboots at unfortunate times as part of an automatic update is another common annoyance self-reported by people as reasons for perceiving updates as a disruption to their work [6, 18, 20]. In this research, we further study the role of past experience and opportunity cost—disruption (time, work, interaction) incurred for the benefit of protection from threats—on repeated update decisions in a laboratory experiment.

Risk communication

The issue of end-users’ difficulty in understanding update messages, and why updates are important is another common reason widely reported by users as a cause for their delay in installing updates [30, 33, 37–41]. People report being frustrated by the lack of information on the urgency of an update [31], emphasizing the need for better risk communication [33, 41–44]. At the heart of this approach stands the assumption that humans are either not aware, and that better communication of these risks, or framing them differently, would increase their willingness to take the appropriate protective actions [33, 41, 45, 46]. While risk communication is certainly relevant to help answer our research question, other possibilities are also relevant and less explored. As mentioned before, many times, individuals are not explicitly aware of the probability of cyberattack and rely heavily on their experience, which has been shown to lead to systematic behavioral patterns such as underweighting of rare events, in this case, underweighting the possibility of an attack from experience [43].

Individual differences

Individual characteristics (e.g. gender, attitude, perception, and risk-taking) are another dominant factor that has been found to influence a variety of security behaviors, including security updates [21, 47–51]. One study compared expert and non-expert users’ attitude
toward security updates [32]. They found that 35% of experts considered installing updates as one of the top three things they do to stay safe while just 2% of end-users made the same recommendation [32]. Others have explored individual characteristics such as cost perception and risk-taking [21, 27, 53, 54]. Farhang and colleagues found that people who frequently updated, perceived the cost of update to be lesser than individuals who seldom updated. However, it was not clear whether this perception was influenced by the real cost or if they were due to differences in individual preferences [53].

Egelman and Peer found that individuals who were more willing to take financial risks (e.g. invest in stock market) were also less likely to demonstrate proactive security behaviors such as timely installation of security updates [21]. Follow-up research has also found evidence for this relationship [54]. In contrast, a survey conducted by Mathur and Chetty with Android users found that users with lower willingness to take financial risk (risk averse) were also more likely to “avoid/disable” auto updates, refusing automatic protection [6]. They argue the reason for such a contradiction to earlier work may be due to the difference in underlying risk associated with auto updates—undesirable consequences to user interaction instead of considering risk from attacks [6]. In this research, we test whether there is a relationship between financial risk-taking and individual’s likelihood to delay a “manual” update.

Intention-behavior gap
Research using controlled laboratory experiments to study factors impacting the optimality of security update decisions is limited. The majority of user-centered research on security updates was addressed via surveys and interviews or through one-shot decisions [35]. An important limitation of survey-based research on update decisions is the intention-behavior gap, where expressed security preferences and actual behavior do not align [7]. Specifically, studies report a discrepancy in the speed of updates between reported intention and the actual behavior [18, 20]. For example, Redmiles et al. compared actual speed of update to self-reported speed by survey respondents and found a systematic over-reporting of update speed among survey respondents [20]. When respondents were asked to recommend an update speed for a friend, they recommended people update “immediately,” whereas when asked about their own behavior, they said they would update within 1 week [20]. However, actual measurements revealed most users on average delayed their update by several weeks [20]. Similarly, Wash et al. found that people who reported that they “update when convenient” were actually most often forced to update by the operating system [18]. A possible explanation for this disconnect is that respondents’ description about their experience with security updates could be based on their memory about a single, salient update instance that may not be consistent with their regular interaction or recent decisions on the update. Hence, it is necessary to test update decisions in interactive experimental settings, where people’s actions can be tracked and cognitive processes can be analyzed.

A decision from experience perspective
The study of protective decisions has been a topic of interest in decision sciences, from insurance decisions to health decisions (e.g. sunscreen use, vaccinations). Indeed, some of the approaches in studying human behavior in cybersecurity were inspired by existing models of protective decisions in healthcare and transportation research [44]. However, research on the economics and psychology of decision making in the field of cybersecurity has been limited to studies on threat response and adversarial behaviors [55–59]. Previous research has shown that experience-based and Description-based (one-shot decisions with full information) decisions lead to different choices. For example, when people are asked to make decisions based on a description of the problem, they tend to overweight rare events [60–62]. However, when they are asked to make repeated decisions from experience, they appear to underweight rare events [14, 15]. This, in turn, affects their tendency to take safety measures. For example, in the study of safety devices, Yechiam and colleagues showed that drivers who purchased safety devices (e.g. radio with a detachable panel) “learned” to stop using them within a year [63], because people do not experience radio thefts as an everyday event, leading people to believe that a safety measure was unnecessary.

Taken together, the current literature suggests that when making decisions from experience, humans tend to behave as if low probability events would happen even less often than they occur in reality. As cyberattacks don’t occur very frequently (from an individual end user’s perspective), and it is likely that they may not occurred very recently either, resulting in decay of the memory of attacks and to underweighting the probability of an attack. Combined with the cost of security updates, we predict that with feedback and experience, participants would learn to avoid and delay security updates, in agreement with past research [63]. We also expect that the tendency to delay updates would be more pronounced for individuals who are willing to take more risks. We contribute to the existing literature by introducing the naturalistic assumption that the cost of taking protective actions may vary over time, and that people adapt their decisions to update according to their experience. We focus on security updates because of its periodic nature: an update provides protection only for a limited time, forcing users to repeat their decisions periodically. In this context, feedback from previous decisions is especially important for future decisions.

Experiment
The repeated protective decision paradigm
The Repeated Protective Decision (RPD) paradigm is a task emulating the primary task of end-users and their security actions. This is a novel paradigm based on paradigms used in the field of decisions from experience with features specific to security update decision making. Building on the literature, three assumptions guided the design of the task: (i) update is a secondary task, (ii) update decisions are repeated, and (iii) update is usually a costly action that takes time away from a primary (income-making) task. Figure 1 presents the task interface. The initial instructions explain that the task includes 20 periods, and each period includes 10 days (see Figure 2). On each day, participants are asked to make binary choices (i.e. the primary task, “investment choice”); and, if security updates are available, to choose whether they want to install an update. In the binary choice task, option “A” yielded an outcome of +2 points with certainty, and option “B” yielded either +4 or 0 points with P = 0.5, ensuring that the expected value (EV) of the two options is equivalent (EV = 2). Thus, the choices in the primary task should not affect participants’ overall payoffs. The simplicity and routine nature of the primary task were intended so that it does not require much attention.

In addition, the participants are asked to decide if they want to “update their system” to protect against possible loss of 100 points, the result from a security failure. Updating the system may be costly (i.e. 10 points), but an update reduced the probability of losses by
more than a half until the end of the period. Notice that this design implies that updating is a secondary task, to simulate real-life security scenarios. The decision to update could be made any day during a period—from the time the update is available at the start of the period until the end of the period. We assume the cost for making an update is dynamic: on certain days the cost for updating is higher while on other days they may be zero (e.g., automatic updates). The player is informed about the cost of update for each day, even on days following an update decision in the period. Choosing to update implies immediate cost for the user, but this cost is significantly lower than a possible loss from an attack. Finally, based on previous research [64] we assume the information that participants receive is asymmetrical. Thus, participants receive feedback on the cost of updates at any day (regardless of the decision), but do not receive information on prevented attacks (participants are generally aware of the lowered risk but not of whether they could have been attacked).

**Participants**

We collected data from 97 participants (39% females, median age = 32 years) from Amazon MTurk [65]. Participants were paid $1.50 as base payment for their time. In addition, participants could earn up to $1.50 as bonus rewards corresponding to amount of points they accumulated in the experiment. The bonus is used to incentivize participants to pay attention and perform the task to the best of their abilities. To avoid actual losses, if the reward accumulated at the end of the experiment was negative, participants received $0 as bonus. All experiment protocols were approved by the university institutional review board (IRB).

**Experimental design**

Table 1 summarizes the incentive structure used in the experiment. In a within-subjects design, we primarily manipulated the cost of updates. In this experiment, the cost of update represents opportunity cost for the end-user that can be variable. Taking time off the primary task to update that involves rebooting the system is usually “costlier” on most days whereas there might be days when it is less costly to take time off the primary task to reboot and update the system. For example, on weekdays, while at work, rebooting a personal laptop to update is likely to be seen as a costly effort as opposed to on a weekend. We only capture this cost at a day-level and not a time-of-day level. It is not intended to represent update specific costs such as the cost of installing a large-sized, slow update whose cost may not vary between days [20]. For simplicity, we included only two levels of cost: high cost (10 points) and low cost (0 points). The

**Investment decisions and security failures**

In this study, you will play through a simulation in which you will make repeated work-related decisions.

*Your work consists of making investment decisions* over 20 work periods. Each work period consists of 10 days (see figure below). On each day, you must choose between safe Investment A, which provides you a guaranteed return of 2 points, and risky Investment B, which gives you 0 or 4 points.

During the course of your work, a failure in the security of your business may randomly arise. This failure is very costly to your business; every time you have a security failure, you lose 100 points. Your security team estimates the chance of a security failure on any given day is 3%.

At some point during your work, security updates to lower the risk of failure will be made available. The cost of an update is most often (85% of the time) 10 points, but sometimes (15% of the time) an update will be available for free (0 points). If you choose to update, your chance of confronting a security failure reduces from 3% to 1%.

You will start this task with 100 points. As you make investment decisions each day (i.e., choosing between “A” and “B”), you will receive feedback on the points you earned from your decision and the total number of points accumulated within the period. You will be informed when a security update is available and at what cost.

**Payment:** At the end of the study, your accumulated points will be converted to US dollars at a rate of 100 points = $0.25. If your accumulated points are below zero, you will get a bonus of $0, and depending on your decisions, your bonus may be as high as $1.50. This bonus will be added to your $1.50 base payment.

**PERIOD 1**

**PERIOD 4**

Figure 1: The interface of the task. This screen shows the primary task (i.e., choose between two investment options, A and B), and the secondary task, indicating that an update is available and that the cost of the update is 10 points at Day 1 of Period 4.

Figure 2: The instructions participants received at the start of the experiment.
Table 1: Incentive structure of the study: risk, rewards, and EVs

| Experiment variables | Initial endowment | Attack loss | High-cost update | Low-cost update |
|----------------------|-------------------|-------------|------------------|----------------|
| +100                 | −100              | 10          | 0                |

Proportions and EVs

| P (discount) | P (attack) | P (attack after update) | EV for immediate update | EV for delayed update |
|--------------|------------|-------------------------|-------------------------|-----------------------|
| 0.15         | 0.03       | 0.01                    | −19                     | −19.25                |

In the consecutive periods (Periods 4–20), a security update was made available from Day 1 of each period. Per the design, the cost was always high (10 points) on the first day of every period. Thus, cost of doing an immediate update was always high. From Day 2, there was a 15% chance [P (Discount)] that the cost would be reduced to zero points. Participants were at risk of losing points from “security failures or attacks,” if the system was left unprotected (if participants decided not to update). The probability of an attack was 0.0 on Day 1, and 3% on Days 2–10. Choosing to update reduced the risk of such attacks for the rest of the period by more than half (from 3% to 1%) [see “P (Attack) after Update” in Table 1]. For example, if a participant updated immediately on Day 1, their risk reduced for all the nine remaining days in the period; if a participant updated on Day 5, the risk reduced only for the five remaining days; and if a participant chose not to update the risk remained high throughout the period. Each instance of an attack led to a loss of 100 points, which were deducted from the cumulative earnings from the primary choice task. Participants were not attacked on Day 1, to give them an opportunity to make an update decision before experiencing an attack in a period. Also, updates were not made available on days after experiencing the first attack in a period.

The incentive structure (see Table 1) was designed so that an immediate update (Day 1) is the optimal decision in each period: the EV is highest on Day 1 than on any other days; and even higher than not updating at all. The comparison between the EV of two strategies “Immediate Update” (update on Day 1) and “Delayed Update” (update only if the update is free) indicates that the more optimal strategy was to update on Day 1 of each period, paying the 10 points. We use this optimal strategy to compare the participants’ behavior in the results section. The expected cost for immediate update was −19 because it is a combination of the cost for updating on Day 1 (−10) and the expected loss from possible attacks after update on one of the remaining days of a period: (−100) (P (Attack) after Update = 0.01) * 9 days = −9. However, the expected cost of waiting to update is a combination of the probability of experiencing a zero-cost update on one of the days in a period (PD) and the expected loss from waiting for zero cost update (ELD), see Equation (1):

\[
EV(\text{Wait}) = \sum_{i=2}^{9} PD_i \times ELD_i
\]

\[
PD_i = P(\text{Discount}) \times (1 - P(\text{Discount}))^{(i-1)}
\]

\[
ELD_i = -100 \times [(i-1) \times P(\text{Attack}) + (10-i) \times P(\text{Attack after update})]
\]

Procedure

After providing informed consent, participants entered basic demographic information (age and gender); they then read a hypothetical scenario, which provided a context for the experiment task (see Figure 1). As part of the context, participants were told they were making routine investment decisions and that a security failure may randomly arise that could be avoided by choosing to update. Participants were not made aware of probabilities for the two choices in the primary task; they were simply informed that “A” was a safe choice with low payoff and “B” was risky choice with high payoff (see Figure 2). But, participants received full information about all the game variables pertinent to security update decision making, such as the attack probability, loss from attacks, and

Figure 3: Proportion of immediate updates (in red), delayed updates (in green), and no updates (in blue) by period, Periods 4–20.
variable cost of update (see Figure 2). Participants were also made aware of the conversion rate from experiment points to bonus in actual dollars (see section on payment in Figure 2). Each participant conducted 200 trials (framed as “Days”) divided into 20 periods. As part of the training phase, from Periods 1 to 3, participants made repeated decisions only on the primary task and experienced one certain loss in Period 2. At the end of training phase (Period 3) and before Period 4, participants were informed that security updates were now available to them; they were also reminded about the variability in the cost of update and the effect of update on reducing the probability of attacks. In consequent periods, from 4 to 20, they made decisions on both primary investment task and secondary update task. At the end of each period, participants received feedback about the points they accumulated so far, and any attacks suffered during the 10 days in that specific period. We collected all the decisions, including the decisions on the primary task. We analyzed decisions from only the main phase (Periods 4–20) of the experiment.

Results

We analyzed participants’ update decisions made between Period 4 (period in which the updates were first made available) and Period 20. As mentioned earlier (see Table 1), the optimal decision was to update immediately on Day 1 of every period (“immediate update”). More the participants’ delayed their update during a period, the greater was the risk of experiencing an attack (more days during which the system was unprotected). Updates later than Day 1 (“delayed update”) or no update was sub-optimal.

Proportion of immediate updates, delayed updates, and no updates

On average, across all 17 periods, participants updated 53.7% of the time (SD = 0.07); they updated immediately on 34.1% (SD = 0.47) of the periods. Figure 3 breaks down the proportion of immediate updates, delayed updates, and no updates over the course of the 17 periods. As seen in the figure, we observe a sharp decrease in the rate of Day 1 updates across periods, from 71.1% of participants updating on Day 1 in Period 1 to 43.3% in Period 5 and in Period 6 to 31.2%, followed by a relatively stable rate of immediate updates in the rest of the periods. Supporting this observation, the figure also shows an increase in the rate of delayed updates and specifically, an increase in no updates across periods. For example, we observe a sharp increase in the rate of no-updates from 21.6% in Period 4 to 46.3% in Period 5. These observations suggest that participants made increasingly more sub-optimal decisions with additional experience.

The increase in the proportion of delayed updates over the periods provides some support for the hypothesis that participants may be delaying the decision with the intention of updating for lower cost. To test this, we compared the rate of two kinds of delayed updates: costly versus free delayed updates. The proportion of delayed updates when the cost was zero was 74.3%, higher than the 25.6% of delayed updates when the cost was 10. A Wilcoxon signed-rank task indicated that this difference is statistically significant ($Z = 13488$, $P < 0.001$). It should be noted, this does not imply that participants updated every time a zero-cost update was available. We observe many participants who neglected to update in a period even though updates were made available for free in that period (e.g. no update rate in Figure 3). Hence, cost is not the only significant predictor of an update decision in a period.

Model of update decisions in a period

An update Decision ($y$) in each period $j$ can be represented using an ordinal variable with three levels indicating the three possible types of update decisions made in each period: Immediate Update, Delayed Update, and No Update. For each participant $i$ and period $j$, $y_{ij} = 2$, if the participant $i$ immediately updated on Day 1 in period $j$; $y_{ij} = 1$, if the participant $i$ delayed the update in period $j$ and $y_{ij} = 0$, if the participant $i$ did not update on any of the days in period $j$.

Using such a representation, we fit a mixed-effects, ordered logistic regression model to determine the effect of recent events on update decisions in a period. We examine the effect of events in one period on the update decision in the following period. For example, update decision of a participant in Period 5 is predicted using events that occurred in the previous period (Period 4). Specifically, the model was used to estimate the effect of points earned in a previous period ($Production_{i,j-1}$), number of days with zero cost updates experienced in the previous period ($ZeroCostDays_{i,j-1}$), whether an update was done in Day 1 in the previous period ($IUPP_{i,j-1}$) and whether an attack occurred in the previous period ($APP_{i,j-1}$). The results of this model are summarized in Table 2.

Estimates from the model reveal that participants who updated immediately in one period were also more likely to update immediately in the following period ($β_{IUPP} = 1.238$, $z = 6.302$, $P < 0.001$) (See Table 2). Across participants, comparing updates between every pair of periods, we found that in 71% of instances a Day 1 update was preceded by a Day 1 update in the previous period. It is also likely that failure or delay to update in one period will lead to failure or delay in update in the following period. The results explain the eventual stability observed with different types of update decisions across periods after the initial drop in immediate updates and increase in the proportion of no-updates (Figure 3). We did not find a significant effect of period on the type of update decision ($β = -0.094$, $z = 1.5$, $P = 0.116$). Also, the model results show that there is no effect of the points accumulated in the previous period (“Production”) or the number of zero-cost days experienced in the previous period.

| Period | Beta estimate | Std. error | z-Value | Pr ($>|z|)$ |
|--------|--------------|------------|---------|-------------|
| Production | 0.043 | 0.106 | 0.408 | 0.683 |
| Zero-cost days | -0.075 | 0.062 | -1.219 | 0.223 |
| Immediate update in previous period (IUPP) | 1.238 | 0.196 | 6.302 | 0.001*** |
| Attack in previous period (APP) | 0.651 | 0.189 | 3.444 | 0.001*** |
| APP*IUPP | -0.982 | 0.414 | -2.374 | 0.018* |

$^*P < 0.05$, **$P < 0.005$, ***$P < 0.001$. 

Table 2: Mixed effects ordinal logistic model predicting update decisions in a period

---

Downloaded from https://academic.oup.com/cybersecurity/article-abstract/6/1/tyaa002/5788613 by guest on 07 March 2020
Effect of experiencing an attack
Delaying updates exposed participants to the risk of attacks. We found that 96% of participants experienced at least one attack in the entire experiment. Among the 93 participants who faced at least one attack, only 47 participants updated in the period following the attack, and not necessarily on the first day.

In what follows, we examine how recent experience of an attack affects the participants’ decision to update in the period following the attack. Estimates from the model (Table 2) show that having experienced an attack in the previous period significantly influenced the update decision in the following period $\beta_{APP} = 0.651, z = 3.44, P < 0.001$. We also found a significant negative interaction effect between having experienced an attack in the previous period and updating on day 1 in the following period, $\beta_{APP\times UPP} = -0.98, z = -2.37, P = 0.018$. Since these are discrete variables, these effects are interpreted as follows. If a participant was attacked in the previous period after making an immediate update in that period, they are less likely to update in the following period. If participants did not update on Day 1 in the previous period and they were attacked in one of the following days of the period, they were more likely to update in the following period (see Table 3).

Individual differences in update patterns
The results above raise the question of whether different participants employed a specific update strategy overall. To explore this issue, we counted the number of update decisions made by each participant $(N_{uw,i})$ using Equation (2), where $UD_i$ is whether or not the participant updated in period $j$ and $UDD_i$ is the day in which the participant updated in period $j$.

Using this formula, if a participant did not update in a period, it will be counted as a 0 because both $UD_i$ and $UDD_i$ will be zero; if a participant updated immediately on Day 1 it will be counted as 1 because both $UD_i$ and $UDD_i$ will be equal to 1; if a participant updated on Day 2 it will be counted as 0.9 because $UD_i = 1$ whereas $UDD_i = 2$.

$$N_{uw,i} = \sum_j UD_i \times \frac{11 - UDD_i}{10} \quad (2)$$

This measure ranges from 0 (the participant did not update in any of the periods) to 17 (the participant updated on Day 1 in all 17 periods). Figure 4 shows the distribution of $N_{uw,i}$ across all participants. The figure reveals substantial individual differences in the way participants updated across the periods. We see that few participants never updated, few participants always updated immediately, whereas majority of them occasionally updated either immediately or later during a period.

To further understand the effect of individual differences on update behavior, we test the effect of two factors—Individual risk-taking tendency and Individual preference for lower update cost—on the average update delay. Next, we discuss how these individual-level variables are measured and the statistical model to describe their relationship.

### Table 3: Interpretation of interaction effect between attack and immediate update in previous period

| Immediate update in previous period? | Attacked in previous period? | Immediate update? |
|-------------------------------------|-----------------------------|------------------|
| Yes                                 | Yes                         | Less likely      |
| No                                  | Yes                         | More likely      |

### Risk-taking
Decisions made as part of the primary task in the experiment (choice between a safe and a risky choice) were used to measure the level of risk-taking tendency for each individual participant. We observe a large variance in participants’ preference for risk in the primary task. The total possible risky choices are 170 (17 periods $\times$ 10 days each period). We counted the total number of risky choices made by each participant and used that as a measure of risk-taking $R_i$. The higher the $R_i$ is, the higher is the participant’s tendency toward risk-taking.

We found that the average $R_i$ was 76.42 that indicates that on average participants chose around 76 risky choices. The minimum number of safe choices made by few participants was 0 that indicates very-high risk aversion because these participants “never” chose the risky option and the maximum number of risky choices made by each participant and used that as a measure of risk-taking $R_i$. The higher the $R_i$ is, the higher is the participant’s tendency toward risk-taking.

### Preference for zero-cost updates
Here we measure individuals’ overall preference for zero-cost updates and whether preference for zero-cost varies between individuals. Individual preference for zero-cost updates is measured by counting the number of update decisions made each participant for zero-cost, weighted by the availability of zero-cost updates to each individual and the total number of update decisions made by each individual. The chance of experiencing a zero-cost was 15% and there was a possibility that some of the participants never observed a zero-cost day in some periods. Therefore, it is necessary to measure one’s preference for zero-cost update based on its availability. For example, if a participant experienced zero-cost updates only in 4 out of the 17 periods but updated on all those four periods for zero-cost, she may have a strong preference for zero cost, compared to another participant who may have also updated on 4 times for zero-cost but had access to zero-cost updates in all 17 periods. Also, the total number of update decisions each participant made varied between individuals and hence, it is necessary to weigh individual’s preference for zero-cost updates based on the total number of decisions they made. For example, if a participant updated on all the periods including for zero-cost in some periods and in other instances for 10-points, she may not have a strong preference for zero-cost updates. However, if a participant updated for zero-cost in all periods containing zero-cost days and never updated in other periods for 10 points, she should be measured to have a strong preference for zero-cost updates.
This measure of zero-update availability ($ZCA_i$) participant experienced a minimum of 1 day with zero-cost update made by participant $i$. $ZCA_i$ is the measure of zero-cost availability for participant $i$. $Ni$ is the total number of decisions made by participant $i$. $ZCA_i$ is the number of periods in which the participant experienced a minimum of 1 day with zero-cost update. This measure of zero-update availability ($ZCA_i$) ranged from 9 to 17 periods where participants on average experienced 13 periods with at least 1 zero-cost update day. We found that only one participant experienced a minimum of 1 day with zero-cost update day in all 17 periods.

Higher values of $P_{zc,i}$ indicate stronger preferences for zero-cost updates. We found that many participants demonstrated no preference for zero-cost either because they consistently updated for higher-cost on Day 1 of each period or because they consistently neglected to update (see Figure 4). $P_{zc,i}$ from 0 to 0.85 with a mean preference of 0.15.

**Predictors of delay in update decisions**

In Figure 3, we observed that participants learned to delay their updates or learned to not update at all. We calculated the average delay for each individual across the 17 periods. In each period, the last available day to update was Day 10 (a sub-optimal decision). A no-update decision in a period was coded as Day 11 indicating the maximum possible delay. Figure 5 shows the distribution of the average delay across all 97 participants. We observe a right-skew in the distribution of delay indicating that a large proportion of participants, on average, chose to delay the updates. Correlation between individual’s average delay and their overall payoff accrued at the end of the experiment shows a marginally significant, negative relationship $r = -0.19, P = 0.059$; suggesting lower payoffs with longer delays. The correlation is marginal because final payoff is affected by the number of attacks experienced, $r = -0.94, P < 0.001$.

We fit a linear regression model to predict average delay in updating using individual’s level of risk-taking and preference for zero-cost updates as predictors. As shown in Table 4, both risk-taking and preference for zero-cost updates have a significant effect on the individuals’ tendency to delay the updates. Individuals with high-risk-taking and preference for zero-cost updates were more likely to delay the updates. It should be noted that there is no correlation between individual’s risk-taking and their preference for zero-cost updates, $r = 0.07, P = 0.49$.

**Table 4: Linear regression model predicting average delay in update using risk aversion and preference for zero-cost as predictors**

| Predictor                        | Coefficient | Standard Error | $t$-statistic | df | $P$-value |
|----------------------------------|-------------|----------------|---------------|----|-----------|
| Preference for zero cost         | 0.202**     | 0.098          | 2.112         | 96 | 0.037     |
| Risk-taking                      | 0.233**     | 0.100          | 2.333         | 96 | 0.023     |
| Constant                         | -0.012      | 0.098          | -0.123        | 96 | 0.903     |

Observations: 96
Residual std. error: 0.958
$F$-statistic: 4.506**

$*P < 0.1; **P < 0.05; ***P < 0.01$.

**Discussion**

In a behavioral economics experiment, we examined the role of experience with rare probability events (i.e. attacks) on update decisions. We find that people are likely to learn from experience to underweight the risk of attacks, and make sub-optimal security decisions. Although the optimal (utility-maximizing) decision in this experiment was to update immediately (on Day 1) in each period, the majority of the participants in our experiment quickly learned to delay the update or not update at all. The negative relationship between average delay and final payoffs demonstrates the negative impact of sub-optimal decisions on the payoff outcomes in the experiment. This finding is in line with a related work on two-factor authentication (2FA), which also found that people in low-risk conditions were more likely to make sub-optimal decisions, in this case failing to enable 2FA [66]. They suggested insufficient risk information as the primary explanation [66]. They did not analyze repeated decisions and therefore, did not test the effect of experience. While risk communication is certainly relevant, our results point to end-user’s past experience as a factor influencing sub-optimal security behaviors. Our results are supported by previous findings in the Decisions from Experience literature, demonstrating underweighting of rare events [67], and stand in contrast to models based on theories that build on decisions from description, such as Prospect Theory, which predict high proportion of immediate updates [23]. Thus, our results demonstrate the description-experience gap [15] and stress the need to examine the effect of experience and feedback on security decisions. Users rarely have the convenience of making updates given explicit descriptions of attack probabilities and need to rely on their own experience to make decisions.

In the experiment, in most periods, the rate of immediate updates was not higher than chance (50%). The overall speed of updates observed in this experiment is in line with previous observations and measurements. For example, Möller et al. [9] analyzed updates to mobile applications over 102 days, and found that on average only a minority of users (17%) installed an update on the day of its release and update rate significantly dropped over the period of 102 days and only 53.2% of users, on average, ended up updating within a
Not all participants in the experiment made sub-optimal decisions. We found large differences in participants’ individual update speeds (see Figures 4 and 25). Some participants in the experiment consistently updated on Day 1 in majority of the periods, whereas others consistently delayed but eventually updated, and yet a large proportion of participants consistently neglected to update at all. This general tendency of participants to repeatedly update in a certain way is consistent with results from Redmiles et al. [20] who found that people tended to anchor to their typical security behaviors [20]. They observed this effect in both survey reports and also actual measurement data. This result further reinforces the importance of efforts to augment user habits and experience to improve proactive security behaviors [20, 35, 52].

So, why did some individuals delay or neglect to take protective decisions while others did not? Overall, the majority of participants who updated late during a period did so when the update was offered for free, indicating that their preference to delay was deliberate, motivated by the expectation for a lower cost and may not be merely out of forgetfulness or irrationality [16]. At the extreme of delaying updates, we observed 15 choices (by 15 different participants) to update on the last day of the period for free. This action is of course useless, given that there is no protection gained from this action at the end of the period. This extreme deviation from maximization further demonstrates the important role of cost on update decisions.

To further understand production-security trade-off in security updates, we measured the impact of two individual-level variables on their average delay to update: number of risky choices made and individual preference for zero-cost updates. Higher proportion of risky choices indicated that the participant was willing to take higher financial risk in the expectation of accumulating higher pay-off. Higher preference for zero-cost update indicated that the participant was more willing to take protective actions when the cost was zero. Our analysis revealed a significant positive impact of both risk-taking and preference for zero-cost on the average delay. Participants with high preference for zero-cost updates were more likely to delay in making the updates. Individuals who made more risky choices in the primary task were more likely to neglect to update. This finding is consistent with similar results from prior work suggesting a strong effect of individual risk-taking on update decisions [21, 54]. Strong correlation between the number of risk choices in the primary task and the number of no-decisions indicate that people with higher affinity toward production were more likely to avoid or neglect to update. There was however no correlation between higher preference for zero-cost and the number of no-decisions. These results suggest a significant role of productivity-security trade-off on individual’s decision to update early or update late or never update at all. People with strong preference for zero-cost would be willing to accept a distraction from the primary task to take action when updating is not costly (e.g. on weekends or nights). On the other hand, people with higher risk preference may be indifferent toward security and therefore, may be willing to avoid making updates even when offered for free. It is possible that people with higher risk preference may also have intended to wait for free update, but forgot to update when made available for free, keeping the status quo even when it is sub-optimal (increased exposure to attacks); they may update only when they are eventually forced by the provider [18].

Furthermore, we found evidence for recency effects [69] where negative outcomes (i.e. experience of an attack) results in a momentary over-weighting of rare event, being more likely to update early in the following period. Our results showed that participants who did not update early but consequently experienced an attack were more likely to update in the next period, demonstrating positive recency (more cautious behavior after an aversive rare event) [69]. Interestingly, we only observe this effect given the experience of an attack (because there was no early update). It seems that the participants’ immediate regret of not protecting oneself may have motivated them to update early on in the following period. However, due to the sporadic nature of attacks, further research is needed to determine extent of the effect of attack on updates and, whether it decays with time. However, we often observe this with back up behaviors where people are more likely to back up their machine immediately after a computer failure but failed to continue doing it.

Another type of regret observed was in terms of protection when an attack is experienced after making a decision to protect. Participants who were attacked after choosing to update in a period, were less likely to update in the following period. It should be noted that participants were informed there is a 1% chance of experiencing an attack even after updating. Therefore, the rare event in this case was the lack of protection offered by the update and we see that the recency effect leads to a momentary over-weighting of this rare event causing lower likelihood of making an update decision in the following period. However, follow-up research is necessary to understand the extent of such a regret.

Our results show that the positive effect of communicating users the probability of threats is short-lived, and that experience could eventually lead them to ignore this information. This is supported by previous study by Erev and colleagues, who demonstrated that when participants are presented with two gambles with known probabilities and outcome, they act as if they overweight small probabilities, however when they start receiving feedback on their choices, this phenomenon was reversed [70]. This was also observed when the dynamics of choice and experience of losses was analyzed over time: the experience of a rare loss appears to result in a momentary over-weighting of this rare outcome given the recency effect, but this effect may be stronger or weaker depending on the interplay of the frequency of the rare event, the recency, and the magnitude of the outcome [69]. Suggestions from past research that call for improving information disclosure about the importance of the security update in relation to protection of the system, as a way to improve security update decision making, may not be sufficient [7, 18, 31].

Reducing cost variability through automatic updates could be seen as a direct implication. However, past research has raised concerns with the practice of automatic updates as the default that includes diminishing security mental model by keeping humans out of the security decision loop [18, 31, 71]. When humans are constantly kept out of the decision loop, it would become harder to learn from experience and adapt to instances when automation fails [18]. Alternatively, people could be offered the option of scheduling an update at a more convenient time, reducing the disruption to present work. But such an option is likely to encourage users to further procrastinate [36]. This research proposes creating solutions that allow people to learn to update quickly from experience through feedback and reinforcements. Particularly in adversarial environment where explicit description of the attacker’s actions may not be available, as in the case of security update decisions. In addition to making security updating easier, it is essential that we focus our efforts on modifying security habits and behaviors of people to produce meaningful, system-level improvements. Modifying peoples’
behavior is a challenge but could be achieved through security training, feedback, rewards, and stringent policies. For example, training people to commit to a specific time for updating their machines and rewarding them for going through on that commitment could develop good security update habits. Subsidies for good behavior (e.g., early update) and penalties for bad behavior (e.g., delayed neglect to update) is also an approach explored in the past to improve protection decisions [24]. This is also in line with previous research on gentle and frequent reinforcement through reminders or small rewards, which have led to improvement in workers’ safe behavior [72,73]. Feedback in the form of potential attacks evaded and losses prevented due to the updates made can also be helpful in developing good security habits.

In a recent publication, we used this experiment design to explore the impact of cost variability on update decisions [74]. In this work, participants performed a similar task but under two different cost conditions with similar payoff distributions: fixed cost and variable cost [74]. As predicted, participants in the fixed cost condition—cost of update is constantly high in all trials—learned to update immediately whereas participants in the variable cost condition—cost of update on some days is low—did not show any such learning effect. They consistently delayed or ignored to update. Thus, when the cost is consistently high, people behave more optimally (learn to update) than when the cost varies. The results from this experiment suggest the “regret” theory as a possible explanation. This theory suggests that cost variability could cause people to regret updating immediately for a high-cost because one would learn that he or she could have updated at another day or time for lower cost. This would encourage further procrastination, keeping the status-quo “not updated” [74].

Limitations and future work

The Repeated Protective Decision (RPD) paradigm introduced in this paper emulates various features relevant to security update decision-making, such as probability of attack, magnitude of loss, protection guarantee after update, and cost of update. The experiment presented in the paper focused on the effect of three features hypothesized to influence security update decisions: experience, cost variability, and individual risk preference. In a subsequent work, we specifically have investigated the impact of cost variability [74]. However, this design can be extended to conduct more follow-up experiments on other relevant aspects of update decisions. For example, future experiments could study the productivity-security trade-offs involved in update decisions by manipulating the cost of update and the magnitude of loss from attacks.

Participants for this experiment were recruited from Amazon MTurk that may not be a representative sample. Compared to US demographics, MTurk participants tend to be younger, typically more educated, and technologically more savvy. This may have biased our results. Future work could validate the results from this experiment with a wider demographic, especially include older population.

Results in this paper are from a simulated laboratory experiment. Therefore, the behavior observed in the experiment may not fully represent peoples’ behavior in the real world. The parameters used to represent risk and cost are artificial, and may not accurately represent the reality. In reality, the probability of attack is likely to be even lower and therefore, the effect of experience could be stronger in the real-world. Quantifying accurately the opportunity cost and loss from attacks is often challenging. Therefore, for experiment purposes, values for these parameters were carefully chosen in relation to the EV of optimal decision, participant payoffs, and other experiment variables. The difference in EV between optimal and sub-optimal choice in this experiment was small because previous research on decisions from experience has shown high sensitivity to small differences in EV. This could be a limitation, and future work could experiment with different EVs by manipulating the probability of attack and magnitude of loss.

The abstract nature of the task is another limitation of the study. Unlike in the related work [20], we did not employ actual update messages due to the concern of specific message features confounding our results. In this experiment, we simply notified the participants an update was made available to them to protect their assets.

Results indicate that in several instances participants refrained from updating even when it was offered for zero cost. One explanation for this behavior is the lack of attention. Participants may have failed to notice that update was available for zero cost on a specific day. We did not include explicit attention checks. This is a limitation. However, the results also indicate that if a participant had a strong preference for zero cost (like some in our sample did), they were likely to wait in each period for the day with zero cost. Further, this was an incentivized experiment. So, we predict the lack of attention may not be a dominant factor. Future work should identify ways to check participant attention and filter-out low-quality responses.

Similarly, one could argue that the reluctance to update may be the result of perceived effectiveness of the update. Previous studies on the certainty effect in vaccination decisions [75] have shown that a vaccination is more attractive if it eliminates the risk completely than if it reduces the risk, even if the ultimate reduction in risk is equivalent [60]. Future research could isolate this certainty effect from the effect of update cost, by testing whether participants would be more inclined to install updates if they eliminate the risk completely even if the effect.

Finally, the paradigm introduced in this paper could be extended to study how users may choose between competing updates to the system where the expected loss is a function of multiple vulnerabilities. In the current design, participants did not receive feedback on attacks prevented due to timely update decisions. Future experiments could test the effect of such a feedback; particularly, to study whether it would encourage people to continue updating even after instances when they were breached despite choosing to update (Table 3). This design can also be extended to conduct group experiments to study the influence of social learning and feedback on individual update decisions. For example, to study what kind of social feedback is more influential in encouraging people to consistently update in a timely manner.

Conflict of interest statement. The authors declare no conflict of interest.

Acknowledgements

This research was funded by the Army Research Laboratory under Cooperative Agreement W911NF-13-2-0045 (ARL Cyber Security CRA) to Cleotilde Gonzalez. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government. The authors thank research assistants in the Dynamic Decision Making Laboratory, Carnegie Mellon University, for their help with data collection.
1. US-CERT: top 30 targeted high risk vulnerabilities. US-CERT Alert (TA15-119A), 2015. https://www.us-cert.gov/ncas/alerts/TA15-119A (9 September 2018, date last accessed).

2. CCIRC: top 4 strategies to mitigate targeted cyber intrusions. CCIRC, 2014. http://www.publicsector.ca/content/nntl-scrn/scrn-tp-strtgs-eng.aspx (9 September 2018, date last accessed).

3. Marconato GV, Nicomette V, Ka¨niche M. Security-related vulnerability life cycle analysis. In: 7th International Conference on Risk and Security of Internet and Systems (CSS). pp. 1–8. IEEE, 2012. Cork, Ireland. October 10-12, 2012.

4. Nayak K, Marino D, Efstratioupolos, P, Dumitra, T. Some vulnerabilities are different than others. In: International Workshop on Recent Advances in Intrusion Detection. pp. 426–446, Springer, 2014. Gothenburg, Sweden. September 17-19, 2014.

5. Anderson J, Bonneau J, Stajano F. Inglorious installers: Security in the app store. In: Proc. of the 36th Symposium on Security and Privacy. pp. 426–446, Oakland, CA, USA. May 27-30, 2014.

6. Mathur A, Chetty M. Impact of user characteristics on attitudes towards automatic mobile application updates. In: Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017) 175–93, 2017. Santa Clara, California, USA. July 12-14, 2017.

7. Vaniea K, Rashidi Y. Tales of software updates: the process of updating software. In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems. pp. 3215–26. ACM, 2016. San Jose, CA, USA. May 7-12, 2016.

8. Khan M, Bi Z, Copeland JA. Software updates as a security metric: passive identification of update trends and effect on machine infection. In: 2012 IEEE Military Communications Conference (MICOM 2012). pp. 1–6. IEEE, 2012. Orlando, Florida, USA. October 28-31, 2012.

9. Möller A, Michalheil F, Diewald Set al. Update behavior in app markets and security implications: a case study in google play. In: 3rd workshop on Research in the large at MobileHCI 2012, LARGE. pp. 3–6, 2012. San Francisco, CA USA. September 21-24, 2012. Association for Computing Machinery, New York NY, United States.

10. Sarabi A, Zhu Z, Xiao C, Liu, M, Dumitra, T. Patch me if you can: a study of users’ experiences and beliefs about software update messages. Comput Human Behav 2015;51: 104–19.

11. Vaniea KE, Rader E, Wash R. Betrayed by updates: how negative experiences affect future security. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 2671–74. ACM, 2014. Toronto, Canada. April 26 - May 1, 2014.

12. West R, The psychology of security. Commun ACM 2008;51: 34–40.

13. Zhang-Kennedy L, Chiasson S, Biddle R. Stop clicking on “update later”: persuading users they need up-to-date antivirus protection. In: International Conference on Persuasive Technology. pp. 302–322. Springer, 2014. Padua, Italy. May 21-23, 2014.

14. Frik A, Egelman S, Harbach M et al. Better late (r) than never: increasing cyber-security compliance by reducing present bias. In: Symposium on Usable Privacy and Security, 2018. Baltimore, MD, USA. August 12–14, 2018.

15. Frik A, Malkin N, Harbach M, Peer, E, Egelman, S. A promise is a promise: the effect of commitment devices on computer security intention In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. p. 604. ACM, 2019. Glasgow, UK. May 4-9, 2019.

16. Frik A, Malkin N, Harbach M, Peer, E, Egelman, S. A promise is a promise: the effect of commitment devices on computer security intention In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. p. 604. ACM, 2019. Glasgow, UK. May 4-9, 2019.

17. Forget A, Pearman S, Thomas J et al. Do or do not, there is no try: user engagement may not improve security outcomes. In: Twelfth Symposium on Usable Privacy and Security (SOUPS 2016). pp. 97–111. Denver, CO, USA. July 22-24, 2016.

18. Wash R, Rader E, Vaniea KE et al. Out of the loop: how automated software updates cause unintended security consequences. In: Symposium on Usable Privacy and Security (SOUPS). pp. 89–104, 2014. Menlo Park, California, USA. July 9-11, 2014.

19. Schoemaker PJ. Determinants of risk-taking: behavioral and economic views. J Risk Uncertain 1993;6:49–73.

20. Redmiles EM, Zhu Z, Kross S et al. Asking for a friend: evaluating response biases in security user studies. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. pp. 1238–55. ACM, 2018. Toronto, Canada. October 15-19, 2018.

21. Egelman S, Peer E. Scaling the security wall: developing a security behavior intentions scale (sebis). In: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing System. pp. 2873–82. ACM, 2015. Seoul, Korea. April 18-23, 2015.

22. Grossklags J, Christin N, Chuang J. Secure or insure?: a game-theoretic analysis of information security game In: Proceedings of the 17th International Conference on World Wide Web. pp. 209–18. ACM, 2008. Beijing, China. April 21-25, 2008.

23. Hota A, Sandaram S. Interdependent security games on networks under behavioral probability weighting. IEEE T Control Netw Syst, vol. 5, no. 1, pp. 262–273, March 2018.

24. Laszka A, Felegyhazi M, Buttyn L. A survey of interdependent information security games. ACM Comput Surv 2015;47:23.

25. August T, August R, Shin H. Designing user incentives for cybersecurity. Communications of the ACM 2014; 57:43–6.

26. Arora A, Telang R, Xu H. Optimal policy for software vulnerability disclosure. Manag Sci 2008;54:642–56.

27. August T, Tunca TI. Network software security and user incentives. ManagSci 2006;52:1703–20.

28. Beattie S, Arnold S, Cowan C et al. Timming the application of security patches for optimal uptime. In: LISA, 2, pp. 233–42. 2002. Philadelphia, PA, USA. November 3-8, 2002. USENIX Association.

29. Dey D, Lahiri A, Zhang G. Optimal policies for security patch management. INFORMS J Comput 2015;27:462–77.

30. Fagan M, Khan MMH, Buck R. A study of users’ experiences and beliefs about software update messages. Comput Human Behav 2015;51: 104–19.

31. Vaniea KE, Rader E, Wash R. Betrayed by updates: how negative experiences affect future security. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 2671–74. ACM, 2014. Toronto, Canada. April 26 - May 1, 2014.

32. West R, The psychology of security. Commun ACM 2008;51: 34–40.

33. Zhang-Kennedy L, Chiasson S, Biddle R. Stop clicking on “update later”: persuading users they need up-to-date antivirus protection. In: International Conference on Persuasive Technology. pp. 302–322. Springer, 2014. Padua, Italy. May 21-23, 2014.

34. Benhabib J, Bisin A, Schotter A. Present-bias, quasi-hyperbolic discounting, and fixed costs. Games Econ Behav 2010;69:205–223.

35. Frik A, Egelman S, Harbach M et al. Better late (r) than never: increasing cyber-security compliance by reducing present bias. In: Symposium on Usable Privacy and Security, 2018. Baltimore, MD, USA. August 12–14, 2018.

36. Frik A, Malkin N, Harbach M, Peer, E, Egelman, S. A promise is a promise: the effect of commitment devices on computer security intention In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. p. 604. ACM, 2019. Glasgow, UK. May 4-9, 2019.

37. Frik A, Malkin N, Harbach M, Peer, E, Egelman, S. A promise is a promise: the effect of commitment devices on computer security intention In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. p. 604. ACM, 2019. Glasgow, UK. May 4-9, 2019.

38. Frik A, Malkin N, Harbach M, Peer, E, Egelman, S. A promise is a promise: the effect of commitment devices on computer security intention In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. p. 604. ACM, 2019. Glasgow, UK. May 4-9, 2019.

39. Frik A, Malkin N, Harbach M, Peer, E, Egelman, S. A promise is a promise: the effect of commitment devices on computer security intention In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. p. 604. ACM, 2019. Glasgow, UK. May 4-9, 2019.

40. Frik A, Malkin N, Harbach M, Peer, E, Egelman, S. A promise is a promise: the effect of commitment devices on computer security intention In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. p. 604. ACM, 2019. Glasgow, UK. May 4-9, 2019.
Cryptography and Data Security. pp. 94–111. Springer, 2013. Okinawa, Japan. April 1–5, 2013.

40. Morgner P, Mai C, Koschate-Fischer N et al. Security update label: establishing economic incentives for security patching of IoT consumer products. arXiv: 1906.11094 2019

41. Qu L, Wang C, Xiao R et al. Towards better security decisions: applying prospect theory to cybersecurity. In: Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems. LBW2613, ACM, 2019. Glasgow, UK. May 4-9, 2019.

42. Aytes K, Connolly T. Computer security and risky computing practices: a rational choice perspective. J Organ End User Comput 2004;16:22–40.

43. Mulligan DK, Schneider FB. Doctrine for cybersecurity. Daedalus 2011; 140:70–92.

44. Workman M, Bommer WH, Straub D. Security lapses and the omission of information security measures: a threat control model and empirical test. Comput Human Behav 2008;24:2799–816.

45. Chen J, Gates CS, Li N et al. Influence of risk/safety information framing on android app-installation decisions. J Cogn Eng Decis Mak 2015;9:149–168.

46. Rajivan P, Camp LJ. Influence of privacy attitude and privacy cue framing on android app choices. In: Wprip SOUPS, 2016. Denver, CO, USA. July 22-24, 2016. USENIX Association.

47. Egelman S, Peer E. The myth of the average user: improving privacy and security through individualization. In: Proceedings of the 2015 New Security Paradigms Workshop. pp. 16–28, ACM. 2015. Twente, The Netherlands. September 8-11, 2015.

48. Furnell SM, Bryant P, Phippen AD. Assessing the security perceptions of personal internet users. Comput Security 2007;26:410–17.

49. Herrero J, Uruená A, Torres A et al. My computer is infected: the role of users’ sensation seeking and domain-specific risk perceptions and risk attitudes on computer harm. J Risk Res 2017;20:1466–79.

50. Howe AE, Ray I, Roberts M et al. The psychology of security for the home computer user. In: 2012 IEEE Symposium on Security and Privacy. pp. 209–223, IEEE, 2012. San Francisco, CA, USA. May 20-23, 2012.

51. Whitty M, Doodson J, Creese S et al. Individual differences in cyber security behaviors: an examination of who is sharing passwords. Cyberpsychol Behav Soc Netw 2015;18:3–7.

52. Ion I, Reeder R, Consolvo S. “ . . . no one can hack my mind”: comparing expert and non-expert security practices. In: SOUPS 2015;15:1–20.

53. Farhang S, Weidman J, Kamani MM et al. Take it or leave it: a survey study on operating system upgrade practices. In: Proceedings of the 34th Annual Computer Security Applications Conference. pp. 490–504, ACM, 2018. San Juan, Puerto Rico, USA. Dec 3-7, 2018.

54. Gratta M, Bindi S, Cukier M et al. Correlating human traits and cyber security behavior intentions. Comput Secur 2018;73:345–58.

55. Abassi Y, Kar D, Sintov N, Tambe, M, Ben-Asher, N, Morrison, D, Gonzalez, C. Know your adversary: insights for a better adversarial behavioral model. 38th Annual Meeting of the Cognitive Science Society (CogSci 2016). Aug 10-13, Philadelphia, USA.

56. Christin N, Grossklags J, Chuang J. Near rationality and competitive equilibria in networked system In: Proceedings of the ACM SIGCOMM Workshop on Practice and Theory of Incentives in Networked Systems. pp. 213–19, ACM, 2004.

57. Cranford E, Lebiere C, Gonzalez C, Cooney, S, Vayanos, P, Tambe, M. Learning about cyber deception through simulations: predictions of human decision making with deceptive signals in Stackelberg security games. 40th Annual Meeting of the Cognitive Science Society (CogSci 2018), July 25-28, 2018. Madison, USA.

58. Grossklags J, Christin N, Chuang J. Security investment (failures) in five economic environments: a comparison of homogeneous and heterogeneous user agents. In: Proc. of the 7th Workshop on the Economics of Information Security (WEIS ’08), June 25-28 2008. Dartmouth, Hanover, New Hampshire, USA.

59. Rajivan P, Gonzalez C. Human factors in cyber security defense. In: Human Factors and Ergonomics for the Gulf Cooperation Council. Edited by Shatha Saman. CRC Press, Boca Raton, Florida, 2018, 85–104.

60. Kahne man D, Tversky A. Choices, values, and frames. Am Psychol 1984; 39:341–50.

61. Kahne man D, Tversky A. Prospect theory: an analysis of decision under risk. In: Handbook of the Fundamentals of Financial Decision Making: Part I. 2013, 99–127. Edited by Leonard C MacLean and William T Ziemba. World Scientific Publishing Co, Singapore.

62. Tversky A, Kaheman D. Advances in prospect theory: cumulative representation of uncertainty. J Risk Uncertain 1992;5:297–323.

63. Yechiam E, Erev I, Barron G. The effect of experience on using a safety device. Saf Sci 2006;44:515–22.

64. Barkan R, Zohar D, Erev I. Accidents and decision making under uncertainty: a comparison of four models. Organ Behav Human Decis Process 1998;74:118–44.

65. Buhrmester M, Kwang T, Gosling SD. Amazon’s mechanical turk: a new source of inexpensive, yet high-quality, data? Perspect Psychol Sci 2011;6:3–5.

66. Redmiles EM, Mazurek ML, Dickerson JP. Dancing pigs or externalities?: measuring the rationality of security decision. In: Proceedings of the 2018 ACM Conference on Economics and Computation. pp. 215–32. ACM, 2018. Ithaca, NY, USA. June 18-22, 2018.

67. Hertwig R, Erev I. The description–experience gap in risky choice. Trends Cogn Sci 2009;13:517–23.

68. Nappa A, Johnson R, Bilge L et al. The attack of the clones: a study of the impact of shared code on vulnerability patching. In: Security and Privacy (SP), 2015 IEEE Symposium. pp. 692–708. IEEE, 2015. SAN JOSE, CA, USA. MAY 18-20, 2015.

69. Harman JL, Gonzalez C. Allais from experience: choice consistency, rare events, and common consequences in repeated decisions. J Behav Decis Mak 2015;28:369–81.

70. Erev I, Ert E, Plonsky O et al. From anomalies to forecasts: toward a descriptive model of decisions under risk, under ambiguity, and from experience. Psychol Rev 2017;124:369–409

71. Camp LJ. Mental models of privacy and security. IEEE Technol Soc Mag 2009;28:37–46.

72. Erev I, Rodensky D, Levi MA et al. The value of ‘gentle reminder’ on safe medical behaviour. BMJ Qual Saf 2010;19:qshc–2009. BMJ Publishing Group Limited, London, UK.

73. Zohar D, Erev I. On the difficulty of promoting workers’ safety behaviour: overcoming the underweighting of routine risks. Int J Risk Assess Manag 2007;7:122–36.

74. Aharonov-Majar E, Rajivan P, Gonzalez C et al. The impact of variability and prechoice experience on taking safety measures: the case of security updates. J Behav Decis Mak. 2020, 33: 3–14. Wiley. 10.1002/bdm.2131.

75. Šlović P, Fischhoff B, Lichtenstein S. Why study risk perception? Risk Anal 1982;2:83–93.