Security When it is Welcome: Exploring Device Purchase as an Opportune Moment for Security Behavior Change

Simon Parkin*, Elissa M. Redmiles†, Lynne Coventry‡ and M. Angela Sasse§
*University College London
Email: s.parkin@ucl.ac.uk
†University of Maryland
Email: eredmiles@cs.umd.edu
‡Northumbria University
Email: lynne.coventry@northumbria.ac.uk
§Ruhr University Bochum and University College London
Email: a.sasse@ucl.ac.uk

***Abstract*—Many security experts bemoan that consumers behave insecurely. Yet, current approaches to improving behavior either fail to consider when people may be most receptive to an intervention, or only consider experiences of threat (e.g., getting hacked) when identifying opportune moments for behavior change. We instead explore how an exemplar, positive experience – buying a new device – can serve as a "security trigger moment". Through in-situ interviews with customers (n=85) and sales staff (n=21) across four branches of a major UK retailer, we characterise the potential for behavior change during device purchase. Further, rather than assuming that users are always ready for an intervention, we explore how the abilities and motivations of users and sales staff can influence the power of a security trigger moment to drive behavior change. Our work lays the foundation for identifying additional trigger moments and deploying targeted interventions when they are most welcome.**

I. Introduction

Computer users get advice and pointers about how to behave securely from a number of sources, such as news articles, family and friends, and expert webpages [20]. This information can support building good security behaviors [21], yet users often do not respond or turn it into action [25]. Industry has offered a range of security solutions for the home user (e.g., anti-virus software, secure hard drives), yet many do not use these tools [35]. This is despite the risks, that for instance 23% of computer incident reports (n=410,000) in the UK in 2017 involved the loss of money or goods [2].

Behavior change literature suggests that for a behavior to be adopted, a person must (1) have sufficient *motivation*, (2) have the *ability* to perform the behavior, and (3) be *triggered* to perform the behavior [10]. Fogg suggests that the trigger for successfully performing a behavior must be present at an *opportune moment*, supporting a person to go beyond the "behavior activation threshold." Here we explore whether this model can generalize to security behavior.

We investigate "trigger moments" for security within the act of purchasing a new computing device in a store. Prior work suggests that configuring a new device can promote discussion about security [8], and lead to new security behaviors. The moment of device purchase then serves as a focal point to consider consumer perceptions and intentions when interacting with a retailer, and how device owners can be encouraged to adopt secure behaviors. It is also at this point that a consumer will have likely made a significant investment and be keen to ensure that the device will work as expected. We evaluate these hypotheses through in-situ interviews with 85 customers and 21 staff members at four branches of a UK retailer where computing devices are sold. Specifically, we seek to understand:

- RQ1: Are there distinct motivations and abilities to enact secure behaviors amongst retail customers, which relate to the purchase of a device?
- RQ2: For consumers lacking the ability to adopt cybersecurity behaviors, can sales staff (or other stakeholders) supplement customer ability to enable behavior change?
- RQ3: is there existing infrastructure or processes in the moment of device purchase, where either sales staff or other stakeholders in the retail environment can create trigger moments for otherwise untriggered customers, or are completely new capabilities required?

To evaluate these questions, we interviewed consumers who were browsing or purchasing a new computer or tablet. We also interviewed sales staff about their experiences discussing security advice and add-on products (such as anti-virus) with customers. We identified a number of the *enablers* and *blockers* for security behavior change. To our knowledge, the retail environment has not been previously studied in terms of security habits in this way.

Through conducting the interviews with customers and

Workshop on Usable Security (USEC) 2019
24 February 2019, San Diego, CA, USA
ISBN 1-891562-57-6
https://dx.doi.org/10.14722/usec.2019.23024
www.ndss-symposium.org

staff, subsequent thematic analysis, and consideration of behavior change mechanisms, we identify distinct opportunities to intervene and encourage behavior change in the device purchase process. These include not only the availability of security advice, but also the inclusion of trusted stakeholders, positively-framed triggers (distinct from any which may leverage fear of loss), and avenues for tailoring security advice and products to users' favoured online activities.

The paper is arranged as follows: we summarize relevant behavior change approaches and how they relate to consumer security behaviors in Section II. The Methodology for engaging with customers and staff is detailed in Section III, followed by Results in Section IV. Wider implications of the outcomes follow in the Discussion in Section V, closing with Conclusions in Section VI.

II. Background and related work

Here, we review prior work on how and why home computer users adopt security behaviors and related work on security education. We conclude by contextualizing this prior work and our work in the broader context of behavior change theory, especially regarding teachable moments.

A. Security Behavior Adoption Among Home Users

Prior work has explored how computer users make decisions about security for their non-work (e.g., home) devices, including cues that trigger security decisions, the stakeholders in the decision-making process, the context relevant to the decision, the advice sources upon which users rely, and the security mental models that permeate their decisions [19], [24], [39], [40].

Two findings from these works are especially relevant to our study: First, Thompson et al. [33] hypothesize that vendor representatives and other security experts may be able to support positive behavior change. We empirically explore this theory through our sales staff interviews. Second, Redmiles et al. and Wash et al. identify digital inequalities (differences) in behavior and support sources available to users with less education [25] and those who are older [39], respectively. They suggest that (a) new channels should be explored for helping these under-resourced users find effective support and (b) that more research is necessary on these populations. Our work takes strides toward filling both gaps: the retail setting provides an additional, previously unexplored support source to under-resourced users, and our participant sample skews older, providing insight into a typically under-sampled demographic in security studies.

B. Opportunities for Security Behavior Change

Beyond examining users' decision-making processes and support sources, prior work has explored how negative experiences [21], [24], [36], games [30], comics [32], warnings [24], [5], [42], and even television shows can influence security behavior [24].

Relating to our work, literature on phishing in particular has explored the effect of targeting interventions after negative experiences – that is, leveraging 'teachable moments' – to improve efficacy. Specifically, Kumaraguru et al. studied the impact of delivering phishing training immediately after a user clicked on a link in a fabricated phishing email [16], noting that the delivery method for their intervention influenced how effective it would be for users. Raja et al. [22] theorized that personal firewall warning messages could be a similar teachable moment, where the right visual and textual information would need to be targeted at the moment when a prompt supports a security decision. The authors found some support for this theory, but note that participants were frustrated by prompts which were too regular.

C. Behavior Change Theories

The concept of a teachable moment has existed long before consideration in phishing and firewall studies.

While there are a wide range of factors (personal: e.g., experiences, beliefs, personality; social: interactions with others; and environmental: economic, physical) that behavior change theories identify as influencers of behavior and behavior change [6], a review of over 80 theories of behavior shows that they all share three common elements: to afford change a person must have capability, opportunity and motivation [17], [18]. The Fogg model articulates this point particularly well: for a target behavior to happen, an individual requires sufficient motivation and ability, and an effective trigger to stimulate the behavior (or behavior change). While cues and triggers can serve to remind us of how to behave, over time behaviors become habitual, operating independently of formerly effective triggers [10]. Changing such habitual behaviors is difficult.

Prior work suggests that transitions – such as a new job – are times of particular motivation and opportunity, which can serve to trigger behavior change [12], [41]. Public health research has explored such triggers empirically, finding that smoking interventions are more likely to succeed if targeted at key life events like pregnancy [28], [29], [34] and exercise levels are more likely to change when moving to university [41].

Transitions need not be as significant as pregnancy or starting college: changes in individuals' interactional and/or physical context can disrupt habits and provide 'cues' (triggers) for new behaviors [38]. During such transitions, a person may be more receptive to information indicating alternative ways of doing things (e.g. using public transport, reducing energy consumption, etc.) [37], [38]. There is thus increasing evidence that habit change interventions delivered at these 'Moments of Change' can be more effective than if delivered at another time [7]. As such, we hypothesize that the transition to a new device may sufficiently raise motivation and opportunity for security behavior adoption. However, it is important to note that increasing motivation alone is not always the solution: to achieve behavior change, users must have the appropriate capability and / or receive sufficient support, and the behavior must be sufficiently easy-to-adopt [10]. As such, we explore not only the potential power of device purchase as a moment for motivating behavior change, but also how sales staff and other factors in the retail context can increase users' capability and smooth the path to security behavior change.

III. Methodology

We conducted an ethnographic interview [31] study involving 85 interviews with customers and 21 interviews with

sales staff in-situ, at retail locations of a retailer that sells computers and tablets to the public. Interviews were conducted at four different branches in the UK. The study fulfilled the requirements of the ethical review process.

We conducted semi-structured interviews in and around the moment of purchase to best understand participants motivations, abilities, and potential to be triggered to adopt a cybersecurity behavior. Conducting such interviews in the retail setting adds external validity as there are real, in-the-moment risks to consider [15]; this external validity, and the avoidance of recall bias, are among the benefits of ethnographic interview methodology [31]. The top-level questions asked in the customer and staff interviews are listed in Appendices A and B respectively – interviews were structured around these questions, with noteworthy responses probed further by the interviewer. For customer interviews, interviewers allowed customers to talk about their purchases to see how participants framed/phrased features that might relate to security.

A. Recruitment

The researchers used opportunistic sampling to invite customers (not all customers present in the store during each day) to be interviewed by handing them a flyer describing the study, which allowed the customers to continue browsing or purchasing a device while considering participation. The flyer described the study as a computer-buying survey (without mentioning security). The flyer noted the maximum 15-minute duration of interviews, an incentive payment being offered for participation (a £20 gift card), and that interviews would not collect any personally identifying information (such as contact information). Consent was obtained before proceeding with an interview.

Staff interviews were described as being about how the salesperson approaches selling generally, and how they approach computer security in customer interactions (with the customer as the focus of the conversation). Staff interviews were arranged on an ad-hoc basis during breaks or relatively quiet periods, and took place away from the shop floor.

We chose to interview staff as well as customers for two reasons: (1) staff have a well-rounded view of "typical" customer conversations, motivations, and abilities and thus can contribute information on general trends among customers, and (2) staff are in a position to leverage customer motivations and ability toward new cybersecurity behavior.

Each of the four stores, in three different regions, was visited over at least two consecutive days. At each site, at least one of the authors joined for the staff briefing on the first morning, introducing themselves and the research. Following ethnographic research principles, the researchers observed and interacted with customers and sales staff in a way that minimized disruption.

B. Demographics

During the customer interviews we had time only to query age, gender, and respondents' computer literacy and cybercrime exposure. 42 participants were female, 38 participants were male, and five interviews were with a male and female couple (where two people count as one participant, making one purchase, for the purposes of this study). Table I lists the reported age group of participants (mean=˜54.5).

TABLE I. AGE OF PARTICIPANTS (WHERE THIS INCLUDES COUPLES, THE AGE OF THE PERSON LEADING THE PURCHASE WAS RECORDED).

Age Group	Count
18-30	8
31-40	8
41-50	14
51-60	18
61-70	26
71 or over	11
TOTAL	**85**

C. Thematic Analysis

Each interviewer took written notes during the interviews, as recording interviews would have been disruptive in the midst of a busy retail environment, consequently violating ethnographic interview best practices [31]. Structured capture forms, listing both top-level aims and agreed questions, helped to maintain consistency and allow some freedom for semi-structured discussion.

Three authors discussed and agreed a set of overarching themes that emerged from both customer and staff interviews, populating an initial codebook that informed Thematic Analysis [4] conducted by one of the interviewers. The populated set of codes and higher-level code families that emerged from customer interviews then informed coding of the sales staff interviews according to the same overarching themes. As mentioned in Section III-A, the customer is the centre of the purchase process – although some of the staff questions (detailed in Appendix VI) refer to staff competency (and related interventions for them), ensuring that staff selling devices are competent in security will be necessary in the future (see Section IV-D). Three of the authors conducted the interviews (at least 19 customer and three staff interviews each).

IV. RESULTS

In this section we first present findings on the influence the device purchase process has on participant customers' security-related *motivations* and *ability* (in support of RQ1, Section 1). Perceptions that participating staff have of customer ability and the impact of the purchase process (RQ2) are also described. Outcomes are then considered within customers' existing *facilitator* model, to explore the capacity of sales staff to serve as cybersecurity *facilitators* (RQ3): we draw from our results on motivations and abilities to synthesize a set of best practices for encouraging them to do so. Customers are assigned a participant number (P##), as are sales staff (S##).

A. Motivations

1) Security as part of the purchase of a new device: Ten participants said explicitly that they would be amenable to discussing add-on software with sales staff as part of the purchase, where this identifies the process as a reminder to consider add-ons including security. 19 participants stated that they would not consider security add-ons alongside purchase of the new device (thereby restricting which topics they were willing to discuss with staff, and *signaling* that the purchase

process did not serve as a security trigger). The remaining participants did not volunteer any opinions about add-on security, although most responded to our query about security for their device by saying that they already have anti-virus software on their devices.

46 participants stated explicitly that they would be the sole user of the new device, while 14 participants expected that they would share use of the device with someone else in the home, such as a partner or one or more family members (the remaining participants did not articulate a use case for their new device). In nine instances, the device was purchased and intended for sole or shared use by a child. These participants were then expressing a *motivation* to protect these other users as they go online.

2) Transitioning from old devices affects motivation: The majority of participants stated that they were buying the computer as a replacement for another device. From the 13 participants who mentioned the age of the older device, this could be in the range of four to seven years old. Reasoning ranged from a device no longer allowing updates, affecting other applications, or a general sense that it 'had died'. Participants then had a *motivation* to use a new and more capable device. While participants did not explicitly mention a security motivation around older devices, we discuss in Section IV-C how the *motivation* to maintain the integrity of the new device can be redirected toward security.

28 participants said that they preferred to try or see the device in person before making a decision. 38 conducted some research – either online or at other stores – prior to visiting the retailer/store where they were interviewed. Effectively, they were motivated to find the right device for their needs (another spark which could be the trigger to also think about security).

Interviews also captured purchase criteria. Purchases were for the most part driven by physical characteristics of the device chassis or its computing hardware. For instance, 27 participants wanted a device that was easy to carry or portable, 17 sought performance, and 12 device interoperability/connectivity. 14 participants focused on budget, and six sought a device that would last a long time from purchase. Security did not emerge as a distinct purchase factor.

3) Device use motivates security: Sales staff participants noted that consumers mention plans to pursue a range of activities on newly-purchased devices. Staff mentioned that these behaviors were not explicitly security-related, but rather *motivated* users to consider security when prompted by the salesperson. For example, when asked during interviews about intended Device usage, most activities invariably required the device user to go online, including Email (47), and Searching / browsing online (44). 19 participants mentioned accessing cherished photos (family photos etc.), which were often described as something the participant was motivated to protect.

Considering the Device environment, 29 participants explicitly stated that they would be using the device for a mix of personal and work-related activities. Having work-related information on a device was a driver that led participants to think about keeping the device secure at the point of purchase. For instance, many of the 29 wanted to protect work emails accessed on the device, even in cases where that was the only work-related activity the device would be used for.

B. Abilities

We found in our discussions with consumers about their security concerns for their new devices, that abilities fell in two categories: actions and awareness.

1) Awareness of security threats: When discussing security concerns, a large number of participants (34) explicitly stated that they were aware of various kinds of scams, including scam phone calls and spam emails. Eight participants were concerned about being 'hacked', whereas viruses and malware making their way onto a device was a concern for ten participants. 13 participants would not conduct any banking activities online (in some cases because they thought it was too risky). P31 simply believed that *"Nowadays, the less you do on the Internet the safer you are"*. Nthala and Flechais [19] noted that their home user participants were also aware of unwanted phone calls and scams, classifying these as 'nuisances'.

2) Ability to apply personal security practices: When asked about security concerns, nine participants stated that they installed or configured parental controls on devices used by or shared with their children (such as dedicated device management Apps or YouTube settings), or otherwise intended to discuss good online behavior with their child.

When asked about whether security add-ons were considered as part of the purchase of a new device, nine participants used the security software recommended by their bank or Internet Service (ISP) rather than purchasing separate software. Five others focused their security efforts on their browsing activities, relying on browser or internet security features to keep them safe. Conversely, eight participants remarked that the built-in security features of their devices would be sufficient to keep them secure. P85, who was replacing a computer that was no longer able to connect to the internet, would be *"really careful"* with the websites they visit, and *"try to avoid things that way."*

Considering Anti-virus (AV) software specifically, four participants believed that AV software alone provided all the protection that they would need. Looking further at AV, 23 participants stated that they already had an existing paid-for anti-virus product, in many cases a subscription (which could be renewed). That they have existing AV is itself a *facilitator*, and individuals may benefit from a *signal* to check if their existing subscriptions can be used on the new device. Eight participants stated that they used free anti-virus products. Five participants noted that they had AV or believed they should install it, despite not knowing what it did (high *motivation* with low *ability*). Eleven participants had negative views of AV, ranging from it being annoying to unnecessary. For P67, *"Security add-ons irritate me; they are very intrusive"*, whereas for P03, *"I would not use AV, it slows the computer down."* This may require a *facilitator* (sales staff in this case) to discuss these reasons and explore whether other options for personal security are more appealing.

Many of the interviews with participating sales staff members echoed themes that emerged from customer interviews. Regarding Security Controls, S01 noted that customers may not know the difference between anti-virus and internet security at first, but that differences could be explained. S08 noted that customers may say that they get security through their

broadband provider or online banking, but that they may not know the level of the security that they are getting.

19 participants described approaches to staying secure that were not driven by software – their own caution and vigilance was seen as sufficient. Considering 'digital natives' and self-described 'IT experts', their self-perceived adeptness online was seen as removing the need to rely on distinct protection measures provided by others. Ion et al. [14] found that experts reported clicking on links and opening unsolicited emails more often than non-experts. Similarly, these are then users who would likely ignore the *trigger* to revisit their skills, believing that they have sufficient *ability*.

3) Instances of low perceived ability: Twelve participants worried that they would be 'left behind' by technology. For these participants, *facilitators* (e.g., sales staff or other support sources) may seek to increase actual and perceived *ability*, for instance by conveying that secure behavior is within reach and doable.

Additionally, participants' advice sources and methods for managing their devices also hint at their *ability* (be it actual or perceived). Eight of our participants relied on family and/or friends to help them manage computer security; prior work has found that family or friends may be more heavily utilized advice sources among those users with lower skill or resources [25], [26].

Many of our participants reported delegating the responsibility for the security of their devices to others. Nine of our participants relied completely on an IT professional (whose services were often paid for) to manage and protect their computers (*"my IT guy"*, as P05 put it). Similarly, eight participants would rely on IT professionals in their workplace to set up a device or fix any problems (if they were using the device to access work data, e.g., for their own company). P37 referred to this as a *"bit of a grey area"*. We hypothesize that these users' choice to pass the responsibility for their devices on to others implies low *ability* and/or low *motivation* to personally engage with security, although these participants nonetheless delegated – rather than ignored – the security of their device(s).

4) Device purchase influences ability: Several participants implied that a new device may be so different to the much older device they were replacing, that initial *ability* to use the device generally is low. Additionally, large gaps in time between device purchases may mean that consumers' prior security knowledge is now out of date. Thus, *facilitators* may need to use the *signal* that time has passed to prompt consumers' that their previously secure practices need to be brought up to date to account for changes in security threats.

C. Facilitators and the Facilitation Process

This section explores findings for RQ3 (Section 1).

1) Openness to staff facilitation: Participants described a range of approaches for choosing a device, motivated by what they were looking for from the interaction with the retailer. In a few cases another person, such as an IT-knowledgeable friend, had provided specific advice as to what to look for (11 participants), usually detailing hardware specifications. Reaching customers in the retail environment, at the point where they may be interacting with the devices, was then key to understanding the drivers for purchase decisions. In cases where the customer arrives to the store with a specific feature, make, or model already in mind, they are not necessarily open to discussion of options (such as peripherals, or security add-ons).

Twenty participants indicated that they would appreciate receiving security advice or pointers from sales staff (mean age=˜59.4, lowest 31-35 and highest 71-75), most notably if it were tailored to their needs. Ten participants further stated that they would want security advice given to them by staff without needing to ask for it. Thus, we find support for the potential of sales staff to serve as *facilitators* of secure behavior, but with an expectation that they would fulfill this role. However, 17 participants stated that they would not ask salespeople for security advice (mean age=˜53, lowest 18-24 and highest 76 or over), often because they had already identified steps to take that they believed would keep them secure; these are then cases where the trigger would not work.

2) Capacity of sales staff to serve as security facilitators: Our interviews with staff suggest that they already conduct *"very customer led"* (S09) sales processes, asking customers what they want and for what they are going to use the device. This implies that (at least some) staff working with customers during the Point-of-Sale are already comfortable crafting or prioritizing advice based upon customer needs.

S12 noted that customers may react against what they perceive as add-on sales – *"they ask 'doesn't it have built-in protection?"'*, but that *"updating is key – some think once they have installed it, that's it"*. This hints at the purchasing experience as being an opportune moment to promote new behaviors, but that a sustained behavior must be supported beyond the point of the trigger moment.

Currently, some staff engage in a discussion of security add-ons during a sales conversation, as a prompt to make decisions about the security of the device (even if in end the customer decides themselves that add-ons are not the way to achieve security). It was also noted that devices often have some security features available in their operating systems which can provide basic security – this would for instance be raised with customers who would say that they did not want to spend money on anti-virus (where Fogg considers money as an element of *ability* [10]). Many interviewed staff members were nonetheless keen to ensure that customers recognised a need to have 'at least some security'. This was balanced against not wanting to 'scare off' customers with an overbearing discussion of security; it was in a sense naturally necessary to align the way security was discussed with the motivations and abilities of the customer.

There was a theme of balancing mentions of security precautions to customers without marring the excitement of buying a new computer; that is, advice may be offered to prospective customers, but if it is not matched to their needs (as perceived by the sales staff through the sales conversation), the mention of security may alienate the customer and prevent a discussion of security altogether.

3) Financial ability and excitement necessitate careful facilitation: Staff noted that customers may react against what

they perceive as add-on sales. Some customers may be sufficiently triggered to think about security behavior, but *facilitators* should be cognizant of mismatches in *ability* (financial ability to purchase add-on software) and potential expectations (for example that the cost of the device should already include any necessary security features). As noted for the customer interviews (Section IV-A2), any additional cost of the security solutions suggested by staff – above the cost of the device itself – could go against the driving factor for their purchase, e.g., their available budget.Thus, while retail staff may be well-placed to offer security advice and pointers, if the discussion is not matched to a customer's needs, the mention of add-on purchases for security may put the customer off the discussion of any security behavior altogether.

Additionally, sales staff acting as *facilitators* must balance promoting secure behavior with consumers' excitement around buying a new computer (the *'spark'* of expectation around what the new device can do): S09 noted that they would not want to *"bog [customers] down, or have them scared to use it or scare them out of the purchase."* S10 noted that *"For people not using computers, its hard to reach them through IT."*

4) Demographic effects on facilitation styles: Finally, participating sales staff noted that older people may be happy to buy security software, but that younger people tend to comment that they know where to get free software or plan to rely on a 'techy friend' rather than the sales staff. Saying nothing of whether this would actually keep them secure, these observations imply that staff facilitation may be more effective for older users, and that staff may need to prompt younger users or leverage different *motivations* to trigger conversations around personal device security.

D. Device Purchase as a Security Trigger Moment

Our interviews with customers and sales staff identify a range of motivations catalyzed by the device purchase process and the interplay with ability and opportunities in-store. Many participants were triggered to independently consider security through the purchase process itself. At least 20 of the 85 interviewed customers reported being amenable to security advice from salespeople; of the remaining 65 who did not explicitly report this, if they lacked sufficient *motivation*, *ability*, or *trigger* to do so, then sales staff may have introduced advice into the conversation that customers did not know about.

To answer RQ3, we reconsider the two axes of the Fogg Behavior Model [10] as a two-by-two grid of Low/High motivation and ability for different kinds of customers, as below. This immediately helps to identify where a *range* of interventions can be deployed together to reach audiences with different wants and needs:

- **High Ability, High Motivation.** For those who are motivated and capable, the sales process acts as a reminder – a *prompt* – that this is a good time to start or update security habits. These customers may need no facilitation at all (examining options and new information themselves), where a leaflet, comment, or direction from sales staff toward up-to-date advice or products available in-store (such as external hard drives for performing data backups) may be sufficient to activate change.
- **High Ability, Low Motivation.** For those rare cases where an individual has low motivation and high ability (for instance, those who believe that their device is inherently safe by default), a *signal* may be required that personal action is required to avoid risks.
- **High Motivation, Low Ability.** For individuals who have high motivation and low ability, sales staff can provide support to improve ability to a level that enables behavior change. For example, some retailers act as a *facilitator* and offer basic skills classes in the familiar environment of the store.
- **Low Motivation, Low Ability.** Customers who for instance rely on somebody else to manage their device security may exhibit both low motivation and ability. One way to boost motivation and make secure behavior seem attainable would be by introducing the customer to role models (especially role models who have gone through similar experiences) – a few customers noted using applications recommended by celebrities, for instance.

Table II illustrates examples of triggers that staff may be able to leverage to target different consumer motivations and abilities.Most triggers may require an investment of time for staff, such as to understand a customer's needs and then relate products and services to their motivations and ability. Acting as a facilitator in this way may require a certain level of ability in the sales staff themselves, though this requires there to be clear and practicable security advice (which can be contentious in itself [27]). Even basic tenets of how to stay secure online are not consistent at present, such that where the trigger could be a prompt to check the latest advice, the process currently relies heavily on the salesperson to make a judgement on what the customer needs. However, a triggered behavior change can be a negative experience if not supported in a way that matches a person's ability and motivation [10]; security interventions which cannot be sustained after the point of purchase can be distracting or frustrating.

There is a wider, community-level effect that goes beyond the individual customer and the individual sales opportunity. The success of the retail environment relies on customer perception of factors, such as value of products, convenience to access, and trust in providing appropriate services. In the context of customer device security, if a customer is spending money on a device, the incentives for staff after that point are not necessarily only to maximise return on that one sale, but also to support the retail model (*potential* customers ought to perceive positive qualities in a retailer in order to want to visit their stores). Sales staff themselves may then receive *signals* or *facilitators* through their role specification and line management, towards being part of the effort to encourage customers to visit the retailer. One incentive for a retailer is then to consider factors which signal to the wider population that they deserve their custom more than another retailer, such that continuing to be an approachable retailer can potentially be just as important (if not more) than maximising the return on one individual sale at the detriment of customer satisfaction. Providing some security which contributes to customer satisfaction, even if not a security product sold alongside the device, is then from one perspective a positive outcome for

TABLE II. EXAMPLES OF ABILITY, MOTIVATORS, AND TRIGGER FORMS FOR SECURE BEHAVIORS AROUND DEVICE PURCHASE.

Ability	Motivation	Foundation for Security Trigger	Intervention Type
Low / High	Want to ensure that a device is found to match expectations and needs, by researching options (e.g., online) ahead of purchase (Low)	Make the relationship between security solutions and a new device explicit (e.g., that purchase of backup drives may be related to purchase of a new device as it can support recovery from an incident, rather than leaving it to the customer to make the connection) (signal)	Education / Environmental Restructuring
Low / High	Want a device within budget (Low)	Point to freely available sources of information (facilitator) / Talk through available solutions to find one within budget, or defer to freely available information (facilitator)	Education / Training
Low / High	The chance to have a new device that will operate predictably if it is secure (to replace an older, erratic device) (High)	Relating effective security practices to the device and what the customer expects to do with it (signal) / Relate advice for safe online behaviors to the activities a customer expects to use a device for, or signpost other resources that are accessible and relevant (signal)	Training / Education / Enablement
Low / High	Want to maintain protection of work files, photos, etc. (High)	Signpost protective products or services which can be readily purchased and operated (anti-virus, repair services, etc.) (facilitator) / Ask customers what data or activities they care about, and whether they are prepared with the implications of losing files/access (spark)	Environmental Restructuring / Enablement
Low	Want to recover from an incident (Low / High)	Identify the type of incident, be supportive, and point to appropriate recovery services, especially if beyond the capabilities of the retailer to resolve the issue (facilitator) / Point to appropriate behaviors for positive recovery (facilitator)	Enablement
Low	Someone else manages my device(s) and my security (Low / High)	Provide concise advice which can be passed on to the person(s) looking after the device (signal) / Signpost positive campaigns and role models (spark)	Enablement / Modeling
High	Focused on buying a new device as the one decision to make while in-store (Low)	Follow up with customers through reminders (signal)	Enablement

the salesperson. It can then be in the interest of a retailer to ensure that customers leave with some kind of security, rather than placing the issue of security to one side if the customer does not take up any specific solutions suggested or offered by that retailer.

A facilitator – in this case a retailer – can consider which triggers they want to manage themselves and whether there are external parties to point to, for instance by providing a signal to customers to check authoritative up-to-date sources. Identifying and planning for trigger moments potentially benefits both customer and facilitator – if customers are protected from the point of first using a new device, it may save time for both customers and staff by reducing the return of customers to the store with problems and follow-up queries. If a customer is provided with a security solution which matches their criteria (e.g., limited or fixed budget), and which then supports them to maintain their newly-purchased device and reduce the chance of needing to return with a fault, this reduces the burden on the retailer and the likelihood that dissatisfaction with the product will be communicated to other people that the customer is in contact with (such as family, friends, support forums, etc.)

A retailer or other facilitator may consider different types of Intervention [18], as in Table II. Enablement interventions here may require having a solution readily available and clearly visible in-store (pointing to promotions and store layout more than crafted advice). Enablement interventions may otherwise require sales staff to weave the topic of security into the sales conversation, where the approach to Communication/marketing used by staff is then key [18]. Education interventions may be predicated by incentivizing sales staff to take the extra time with customers to do so as part of doing business; it may also require that staff be skilled enough to be able to act as *advocates* of security [13] (albeit within the remit and bounds of their role).

Overall, our findings suggest that retail staff may be well-placed to enact a range of security behavior interventions, encouraging a customer above the 'activation threshold' for a target behavior. Doing so is perhaps also in the retailer's best interest, as well, as low understanding of the purchased technology or future negative security incidents may decrease customer satisfaction and the likelihood of return for follow-up or future purchases.

V. DISCUSSION

Overall, device purchase appears to be a promising moment for potentially triggering new security behaviors, particularly if the user purchasing the device is appropriately supported by retail staff in making a behavior change.

This setting may be particularly effective for older users, who appear to lack confidence and a dependable source of digital security support or information. Eighteen of 44 participants over the age of 51 believed that family and friends knew more about security than them, and sales staff report that more older users ask them for advice. This need for support may stem not only from low confidence, but also by the transition from work to retirement. Engaging at the point of sale may then be a rare contact point for technology advice during retirement, a key life transition point [9].

Not all older users are, however, just waiting to happen upon a source of security advice: five of our older participants reported paying an IT professional to manage their security. Perhaps surprisingly, six additional, younger users also reported doing so. This suggests a proxy agency effect, where a person defers to experts to ensure that they themselves can still do the things they want to do [1]. Similarly, Forget et al. [11] consider that users may 'disengage' from security if they have already deferred the responsibility to somebody else.

Such proxy agency raises significant concerns: those users who have paid others to secure their devices may not be aware of the changes that the paid IT professionals are making to their devices [11] or may not understand the implications of having handed over device access (such as having the person freely install software). More concerning, there may be persons providing IT support who themselves are unaware of developments in security technology, or have beliefs which require interventions of their own (as alluded to in Table II).

Finally, while our work focused on device-purchase as a positive trigger moment, during our interviews some participants mentioned previous negative experiences, and the behaviors they had changed as a result of those experiences. Prior work has suggested that negative experiences may be strong triggers for security behavior [21]. While we find that negative experiences can indeed trigger behaviors, we find that these triggers may not always lead to *good* behaviors. We observed that customers motivated by previous experience of a cybersecurity incident might adopt behaviors (e.g., delegating security fully to others) that do not mitigate the original risk or severely impinged on their ability to enjoy the device they sought to protect (e.g., severely restricting online activities to avoid threats). Thus, new-found motivation from negative experiences may not always be well-spent.

A. Further Security Trigger Moments

Negative experiences are not necessarily doomed, however. We hypothesize that ineffective, or detrimental behavior changes following a negative experience are likely caused by a lack of sufficient support and understanding about what to do next. Prior work has shown that people do not necessarily know where to turn following a security incident [23], [26], [43]. Only a few staff at the retail organization mentioned that customers returned to visit a store to get advice or seek help following an incident. While stores must be mindful of costs and staff burden, providing an incident response hotline could be a useful strategy for improving brand sentiment and customer appreciation. Further, other stakeholders such as police may be well-placed to intervene and assist with both offline and online behavior improvement at the point of the incident.

While our work focused specifically on one, exemplar, positive trigger moment, there are other instances that could be reframed serve as *opportune moments* for security behavior change. For example, starting a new job in an organisation, when an individual does not yet know the rules of the organization (but is recepetive to new information as part of their orientation), and is keen to impress their new employer may be an perfect trigger moment. However, the trigger must be crafted carefully in this case so as not to appear irrelevant or burdensome, and so as not to exceed the users' 'compliance budget' for adhering to all of the rules of a new job [3]. Alternately, transitions *within* an online environment – for example, achieving a particular bank account balance or number of valuable assets (e.g., photos, documents) within an online account – could also serve as appropriate triggers for prompting new behavior such as enabling multi-factor authentication for a now more valuable account.

B. Limitations

Our analysis relied on the use of handwritten notes, which limited our ability to directly quote participant statements. However, we felt that the need to maintain the in-situ setting and conduct interviews within the retail setting during the moment of purchase was a higher priority.

Five of the customers who were interviewed were shopping with someone else. We did not include couple or pair dynamics in our interviews, in part due to limits on their duration, where future studies could be designed to account for visits to the retail environment being an experience for more than one person.

Researchers approached customers present in the store on specific days, and participants were self-selecting. They then cannot be assumed to be representative of the retailer's customers or the wider public. Discussions with sales staff implied that the time of day, day of the week – or indeed the time of year (such as school holidays) – would influence which kinds of people would be in-store when interviewers were present. The goal of this research was to begin to identify opportunities for effective security behavior interventions, where future work may then explore when best to utilise those opportunities.

VI. Conclusions

In this work, we investigated the potential for a device transition – the purchase of a new computer or tablet – to serve as a security trigger moment, leveraging opportunities for adoption of new and effective security behaviors. To do so, we conducted an ethnographic interview study, interviewing 85 customers and 21 staff across four branches of a major UK retailer. Our results provide insight into how users' capabilities and motivations can be combined with appropriate, timely security interventions from trustworthy facilitators (sales staff) to potentially effect positive behavior change.

Currently, behavior interventions for security can miss the blockers to effective, sustainable behavior change. Similarly, when buying a new device, for instance, some customers may already have relevant security behaviors, and there is an opportunity to support the transition to the new device so that it does not result in reduced security. It is necessary to ascertain the customer's ability to manage the transition themselves, or

whether they may wish to engage in a support service which would manage that transition for them. Some participating customers were found to already be delegating management of computing devices to a seemingly IT-literate friend or a paid 'IT person' (where this first relied on having such a route available to them).

To consider the retail environment, for some participating customers the cost of security solutions, for instance, limited – but did not remove – their capacity to engage with security. If no available security solution exists to address their particular blocker to ability (for instance a free solution, or advice that can be readily communicated to them, and clearly related to their needs and motivations), they may then see no security improvements, even if engaged at an opportune moment. By identifying varying abilities and motivations, researchers and practitioners alike can act to ensure that there is a sustainable security solution matched to every level. Here we have illustrated that by considering differences in individual motivation and ability, paths toward secure behavior can be identified and explored. In the process of device purchase, we also find an opportune moment to explore the ability and motivation of the customer as part of an existing model of engagement, where security interventions can be delivered when customers are in a process of transition and receptive to new behaviors.

ACKNOWLEDGEMENTS

The authors wish to thank the collaborating retail organization and participating sales staff for their time and support. The authors also wish to thank the USEC reviewers for their comments. Elissa M. Redmiles acknowledges support from the Facebook Fellowship and the National Science Foundation Graduate Research Fellowship Program under Grant No. DGE 1322106.

REFERENCES

[1] A. Bandura, "Social cognitive theory: An agentic perspective," *Annual review of psychology*, vol. 52, no. 1, pp. 1–26, 2001.

[2] M. Bangs, "Overview of fraud and computer misuse statistics for england and wales, office of national statistics (uk)," https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudandcomputermisusestatisticsforenglandandwales/2018-01-25, 2018, accessed: 10th January 2019.

[3] A. Beautement, M. A. Sasse, and M. Wonham, "The compliance budget: managing security behaviour in organisations," in *Proceedings of the 2008 New Security Paradigms Workshop*. ACM, 2009, pp. 47–58.

[4] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative research in psychology*, vol. 3, no. 2, pp. 77–101, 2006.

[5] C. Bravo-Lillo, L. F. Cranor, J. Downs, and S. Komanduri, "Bridging the gap in computer security warnings: A mental model approach," *IEEE Security & Privacy*, vol. 9, no. 2, pp. 18–26, 2011.

[6] L. Coventry, P. Briggs, J. Blythe, and M. Tran, "Using behavioural insights to improve the public's use of cyber security best practices," *gov. uk report*, 2014.

[7] A. Darnton, B. Verplanken, P. White, and L. Whitmarsh, "Habits, routines and sustainable lifestyles," *A summary report to the Department for Environment, Food and Rural Affairs. AD Research and Analysis for Defra, London, November*, 2011.

[8] S. Das, T. H.-J. Kim, L. A. Dabbish, and J. I. Hong, "The effect of social influence on security sensitivity," in *Proc. SOUPS*, vol. 14, 2014.

[9] A. Durrant, D. Kirk, D. Trujillo Pisanty, W. Moncur, K. Orzech, T. Schofield, C. Elsden, D. Chatting, and A. Monk, "Transitions in digital personhood: Online activity in early retirement," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 2017, pp. 6398–6411.

[10] B. J. Fogg, "A behavior model for persuasive design," in *Proceedings of the 4th international Conference on Persuasive Technology*. ACM, 2009, p. 40.

[11] A. Forget, S. Pearman, J. Thomas, A. Acquisti, N. Christin, L. F. Cranor, S. Egelman, M. Harbach, and R. Telang, "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)*, 2016, pp. 97–111.

[12] A. Giddens, *Modernity and self-identity: Self and society in the late modern age*. Stanford university press, 1991.

[13] J. M. Haney and W. G. Lutters, ""it's scary... it's confusing... it's dull": How cybersecurity advocates overcome negative perceptions of security," in *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*. USENIX Association, 2018.

[14] I. Ion, R. Reeder, and S. Consolvo, ""... no one can hack my mind": Comparing expert and non-expert security practices." in *SOUPS*, vol. 15, 2015, pp. 1–20.

[15] K. Krol, J. M. Spring, S. Parkin, and M. A. Sasse, "Towards robust experimental design for user studies in security and privacy." IEEE, 2016.

[16] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Teaching Johnny not to fall for phish," *ACM Transactions on Internet Technology (TOIT)*, vol. 10, no. 2, p. 7, 2010.

[17] S. Michie, M. Johnston, J. Francis, W. Hardeman, and M. Eccles, "From theory to intervention: mapping theoretically derived behavioural determinants to behaviour change techniques," *Applied psychology*, vol. 57, no. 4, pp. 660–680, 2008.

[18] S. Michie, M. M. Van Stralen, and R. West, "The behaviour change wheel: a new method for characterising and designing behaviour change interventions," *Implementation science*, vol. 6, no. 1, p. 42, 2011.

[19] N. Nthala and I. Flechais, "If it's urgent or it is stopping me from doing something, then I might just go straight at it," *Human Aspects of Information Security, Privacy and Trust (HAS)*, 2017.

[20] E. Rader and R. Wash, "Identifying patterns in informal sources of security information," *Journal of Cybersecurity*, vol. 1, no. 1, pp. 121–144, 2015.

[21] E. Rader, R. Wash, and B. Brooks, "Stories as informal lessons about security," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, 2012, p. 6.

[22] F. Raja, K. Hawkey, P. Jaferian, K. Beznosov, and K. S. Booth, "It's too complicated, so I turned it off!: expectations, perceptions, and misconceptions of personal firewalls," in *Proceedings of the 3rd ACM workshop on Assurable and usable security configuration*. ACM, 2010, pp. 53–62.

[23] E. M. Redmiles, ""should I worry?" a cross-cultural examination of account security incident response," *arXiv preprint arXiv:1808.08177*, 2018.

[24] E. M. Redmiles, S. Kross, and M. L. Mazurek, "How I learned to be secure: a census-representative survey of security advice sources and behavior," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016, pp. 666–677.

[25] ——, "Where is the digital divide?: A survey of security, privacy, and socioeconomics," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 2017, pp. 931–936.

[26] E. M. Redmiles, A. R. Malone, and M. L. Mazurek, "I think they're trying to tell me something: Advice sources and selection for digital security," in *Security and Privacy (SP), 2016 IEEE Symposium on*. IEEE, 2016, pp. 272–288.

[27] R. Reeder, I. Ion, and S. Consolvo, "152 simple steps to stay safe online: Security advice for non-tech-savvy users," *IEEE Security & Privacy*, 2017.

[28] M. Schäfer and S. Bamberg, "Breaking habits: Linking sustainable consumption campaigns to sensitive life events," in *Proceedings sustainable consumption and production: Framework for action, conference of the sustainable consumption research exchange*, 2008, pp. 213–228.

[29] M. Schäfer, M. Jaeger-Erben, and S. Bamberg, "Life events as windows of opportunity for changing towards sustainable consumption patterns?" *Journal of Consumer Policy*, vol. 35, no. 1, pp. 65–84, 2012.

[30] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, "Anti-phishing phil: the design and evaluation

of a game that teaches people not to fall for phish," in *Proceedings of the 3rd symposium on Usable privacy and security*. ACM, 2007, pp. 88–99.

[31] J. P. Spradley, *The ethnographic interview*. Waveland Press, 2016.

[32] S. Srikwan and M. Jakobsson, "Using cartoons to teach internet security," *Cryptologia*, vol. 32, no. 2, pp. 137–154, 2008.

[33] N. Thompson, T. J. McGill, and X. Wang, ""security begins at home": Determinants of home computer and mobile device security behavior," *Computers & Security*, vol. 70, pp. 376–391, 2017.

[34] S. Thompson, J. Michaelson, S. Abdallah, V. Johnson, D. Morris, K. Riley, and A. Simms, "'moments of change' as opportunities for influencing behaviour," 2011.

[35] K. Vaniea and Y. Rashidi, "Tales of software updates: The process of updating software," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 2016, pp. 3215–3226.

[36] K. E. Vaniea, E. Rader, and R. Wash, "Betrayed by updates: how negative experiences affect future security," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2014, pp. 2671–2674.

[37] B. Verplanken and D. Roy, "Empowering interventions to promote sustainable lifestyles: Testing the habit discontinuity hypothesis in a field experiment," *Journal of Environmental Psychology*, vol. 45, pp. 127–134, 2016.

[38] B. Verplanken, I. Walker, A. Davis, and M. Jurasek, "Context change and travel mode choice: Combining the habit discontinuity and self-activation hypotheses," *Journal of Environmental Psychology*, vol. 28, no. 2, pp. 121–127, 2008.

[39] R. Wash, "Folk models of home computer security," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM, 2010, p. 11.

[40] G. White, T. Ekin, and L. Visinescu, "Analysis of protective behavior and security incidents for home computers," *Journal of Computer Information Systems*, vol. 57, no. 4, pp. 353–363, 2017.

[41] W. Wood, L. Tam, and M. G. Witt, "Changing circumstances, disrupting habits," *Journal of personality and social psychology*, vol. 88, no. 6, p. 918, 2005.

[42] M. Wu, R. C. Miller, and S. L. Garfinkel, "Do security toolbars actually prevent phishing attacks?" in *Proceedings of the SIGCHI conference on Human Factors in computing systems*. ACM, 2006, pp. 601–610.

[43] Y. Zou, A. H. Mhaidli, A. McCall, and F. Schaub, ""I've got nothing to lose": Consumers' risk perceptions and protective actions after the equifax data breach," in *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*. USENIX Association, 2018.

Appendix A: Customer Interviews – Questions

1) Who are you looking to buy a computer for today?
2) Would this be their/your first computer or a replacement? If a replacement, why is it needed?
3) Would the computer be for business/personal/both?
4) What types of activities do you see a computer being used for?
5) Are there any features that make one or another computer stand out?
6) Would you consider buying any add-on (software / hardware)?
7) Where did you get information from to help you decide which computer to buy?
8) Why have you decided to buy this computer at [this retailer]?
9) Will the computer be connected to any other devices? Will any software/files/data be put on it? Would there be just one person using it?
    a) Do you have any concerns relating to those connections, files, or people?
    b) Are there any other (security) concerns you have heard or read about, which you would say affect other people more than you? If so, why?
    c) Have you ever had anything go wrong with a computer you use (which you would consider being a security issue)?
10) Did you discuss any security concerns or security precautions as part of this purchase?
    a) *(If they asked staff)* what advice did you ask for, what did you think of the advice you were given?
    b) *(if staff raised the issue or it was not discussed)* Is there any advice on computer security that you would expect to receive from shop sales staff, and why?

Appendix B: Staff Interviews – Questions

1) Is there any information you would typically give a customer buying a computer, should they ask for guidance about how to protect the machine?
2) Is there anything that might change the advice you give from one device to another? (e.g., across different device manufacturers)
3) Is there any central guidance at [this retailer] for customers, around computer protection?
    a) Is there any training or guidance about computer security that you would like to have available to you, or are you already prepared?
    b) Is there any guidance you would provide to customers without them prompting you? If so, why?
4) Does the advice you give customers and your own sources of knowledge change at all over time?
5) Do you encourage customers to buy security software when they buy a computer?
    a) What packages would you typically recommend, and why?
    b) How do customers typically react to this?
6) What questions have you been asked about security when people are buying a computer?
    a) Are there any you feel particularly comfortable answering?
    b) Are there any you feel uncomfortable answering?
    c) Are there any questions you have not been able to provide an answer to?
7) Are there any materials you would like to see available for the customers?
8) Would you ever point customers to external resources relating to security?
    a) If so, which ones?
    b) If not, what prevents you from doing this?