

Laptop Theft in a University Setting can be Avoided with Warnings

Azqa Nadeem¹

Delft University of Technology,

The Netherlands

azqa.nadeem@tudelft.nl

Marianne Junger

University of Twente,

The Netherlands

m.junger@utwente.nl

¹ Corresponding author | Postal address: Van Mourik Broekmanweg 6, 2628 XE, Delft, the Netherlands

Laptop Theft in a University Setting can be Avoided with Warnings

Azqa Nadeem¹, Marianne Junger²

¹ Delft University of Technology, ² University of Twente, The Netherlands

¹ azqa.nadeem@tudelft.nl, ² m.junger@utwente.nl

ABSTRACT

Laptops have become an indispensable asset in today's digital age. They often contain highly sensitive information, such as credentials and confidential documents. As a result, the value of a laptop is an accumulation of the value of both the physical device itself and the cyber assets it contains, making it a lucrative target for theft. Educational institutions have a large population of potential victims of laptop theft. To mitigate this risk, we investigate whether a simple warning sign can reduce the opportunity for potential offenders. To this end, we have conducted an empirical study to observe the prevalence of students/staff leaving their laptops unattended at a university study hall at the Delft University of Technology in the Netherlands, both with and without a warning sign. We observed 148 out of 220 subjects leaving their laptops unattended in just three weeks. The results also showed that without the warning banner, 75.5% (83 out of 110) of subjects left their laptops unattended and with the warning, only 59.1% (65 out of 110) of subjects showed the same behavior, which is a significant reduction of 16.4%. In addition, a qualitative analysis was performed on the responses of subjects who left their laptops unattended after the warning banner was placed. The results showed a mix of convenience, and a blind trust on the safety of the faculty. In conclusion, a simple banner was effective in reducing the opportunity for laptop theft. However, the percentage of laptops left unattended was still high even after the introduction of the banner.

Keywords: Cybercrime; Field Experiment; Laptop Theft; Warning Banner; Situational Crime Prevention

1. INTRODUCTION

Laptops have become an indispensable asset in today's digital age. Owning a laptop nowadays is a necessity due to its ever-increasing portability, functionality, and storage capacity ("The Importance of Having a Laptop | Techwalla.com," n.d.). Due to the convenience offered by laptops, many users store sensitive information on them, such as passwords, credit card information, and confidential documents. According to Kensington, 50% of all mobile device users keep sensitive information on their devices (Strom, Curry, Sponsors, Andersen, & Church, 2012). Additionally, a survey conducted by AlertSec revealed that laptops contain more sensitive information than smartphones but they are less frequently encrypted ("Laptops hold more sensitive data, but they're less protected than smartphones | Enforce Encryption on Third-Party Devices – Laptop Encryption as a Service – AlertSec," n.d.-a), which renders their cyber assets vulnerable to thefts. Hence, a laptop can be considered a highly valuable "cyber-physical asset", where not only does the physical value of the laptop matter, the cyber assets it contains might even exceed the physical value of the laptop itself. Therefore, to adequately protect cyber-physical systems, both their cyber and physical aspects need to be protected (Baheti & Gill, 2011). In a 2009 Intel study, the average value of a lost laptop was estimated to be \$50,000 and a jointly increasing trend with the cost of data breaches was also identified (Ponemon, 2012). In addition, improvements in application security are displacing the crime from hacking an application to stealing a device containing the credentials to that application. For instance, (Keane, 2016) reports that with the current state of database security, it is much easier to steal a laptop containing the credentials to

the database than to hack the database itself. Therefore, it is not surprising that laptops are a lucrative target for attackers.

Multiple sources suggest that the threat of laptop theft has been prevalent and persistent. The top most affected organizations by theft of mobile devices like laptops are education and research institutes (Strom et al., 2012). In one report, Kensington reports that one laptop is stolen every 53 seconds (“News & Press Center - Kensington - Kensington - A Mobile Device is Stolen Every Minute; Most Thieves Strike in the Office or During a Meeting,” n.d.). In addition, employees frequently expose themselves to the risk of laptop theft by leaving them unattended. In a survey of 800 U.S. citizens, *“46% of the respondents admit that they have exposed themselves to cybersecurity threats while using a laptop”*, out of which the top risk was leaving the laptop unattended (“Laptops hold more sensitive data, but they’re less protected than smartphones | Enforce Encryption on Third-Party Devices – Laptop Encryption as a Service – AlertSec,” n.d.- b). Even with the knowledge of laptop theft being such a big risk, organizations do not have any specific solution which seems to work. In a survey of companies, it was found that *“in 64% of the enterprises, respondents reported that users’ devices containing sensitive or proprietary data had been lost or stolen, but few had specific solutions in place to protect those devices”* (Morrow, 2012). Hence, there have been multiple reported incidents of laptop thefts. The studies by (Dimkov, Pieters, & Hartel, 2010) and (Strom et al., 2012) report that around 46% of the laptop thefts that they studied occurred when the owner of the laptop left it unattended in a public setting, such as a cafeteria or a meeting room.

Several security researchers have emphasized that cyber security needs to encompass the complete chain of protecting the human, the physical devices as well as the digital information (Choo, 2011;

Ghernouti-Hélie, Tashi, & Simms, 2010). Therefore, it is important for computer security professionals to look outside the technical realm and understand the intricacies of the human behavior as well. Even though security specialists and managers put controls and policies in place to ensure the effective operation of the organization and to stop malicious adversaries from entering the premises, the human factor is a crucial aspect in ensuring the success of those controls and policies. This has been shown by (Dimkov et al., 2010) where the authors state that *“surveillance cameras and access control have a limited role in the security of the organization and that the level of security awareness of the employees plays the biggest role in stopping theft”*. In other words, the opportunity for potential offenders can be reduced by increasing the security awareness of the potential victims working in that organization.

Organizations invest a significant amount of their security budget in figuring out solutions to their security problems (Filkins & Hardy, 2016). However, in many cases cheaper and simpler interventions can also be effective. To identify which controls would be effective, it is important to test them. In this paper, we demonstrate this concept by presenting a case study of a university setting. Since technical universities are a hub of laptop-carrying individuals, it gives offenders a lot of potential targets. Therefore, through the case study, we highlight deviant human behavior and the effectiveness of a simple intervention to alter it.

The Delft University of Technology is considered as the best technical university in the Netherlands (“Best universities in the Netherlands,” 2017). The building of the faculty of Electrical Engineering, Mathematics and Computer Science (EEMCS) is iconic for the university. As students of this faculty, we wanted to evaluate the security of the building in terms of its individuals’ awareness. Moreover, there have been hearsay regarding the occurrence of laptop

thefts at some faculties but so far, no supporting evidence has been presented to prove so. Therefore, in a field experiment, we aim to get an insight into the opportunity for potential offenders by studying the prevalence of students and staff leaving their laptops unattended while studying in the faculty's study hall.

A warning banner is chosen as a simple intervention to reduce the risky behavior of leaving laptops unattended. The warning was designed using guidelines from the literature (Wogalter, Laughery, & Mayhorn, 2012), which suggest that warnings should be brief and kept simple even for low competence audience. Therefore, the warning was designed to be subtle enough to increase the awareness of the individuals, and at the same time not too intrusive that it would require them to spend extra effort or time on it.

As such, there are two main contributions of this paper. 1) We make the first attempt at collecting statistics about the prevalence of students/staff leaving their laptops unattended in a university setting, and 2) we evaluate the effectiveness of a simple warning banner in correcting the behavior of the students/staff. The results show that the warning banner was successfully able to reduce the frequency of laptops left unattended by 16.4% in just three weeks.

The rest of the paper is organized as follows: Section 2 states the related literature studied for conducting the present study. Section 3 describes the detailed methodology of the field experiment. Section 4 and 5 state the results and discusses them in the context of available literature, respectively. Finally, we conclude in Section 6.

2. RELATED WORK

(Dimkov et al., 2010) have performed a case study on laptop theft to study the efficacy of security mechanisms in open organizations. The results showed that the security awareness of employees is the most important factor in the overall security of an organization, and that most security mechanisms are deterrent rather than protective. In a survey regarding laptop thefts by (Wood, n.d.), the authors found that one third of the organizations did not provide any formal training to their laptop users. The present study primarily builds upon the aforementioned studies, but it is novel in that it goes one step further in presenting and evaluating a simple intervention. It is based on the rational choice model of crime.

The rational choice model of crime assumes a utilitarian (Wikipedia contributors, 2018) approach and assumes that humans are reasoning actors who weigh means and ends; costs and benefits to make a rational choice (Coleman, 1958; Gigerenzer & Goldstein, 1996; Simon, 1955). This general model was extended to the explanation of crime by Cornish and Clarke to explain short term offender decision making and assist in the development of situational crime prevention (Cornish & Clarke, 1987; Cornish, Clarke, Wortley, & Mazerolle, 2008). It is assumed that crime is a goal-directed behavior designed to meet the offender's commonplace needs such as money, status, sex, and excitement. Meeting these needs involves the making of (sometimes quite rudimentary) decisions and choices, which are constrained by limits, ability, and the availability of relevant information (Cornish & Clarke, 1987; Cornish et al., 2008; Felson & Eckert, 2017). Situational Crime ("Center for Problem-Oriented Policing | 25 Techniques," n.d.) includes three principles that directly affect the cost/benefits ratio which impacts an offender's morality. They are: 1) target hardening: making a crime more difficult to commit, 2) increasing risks to increase the likelihood of detection, and 3) decreasing rewards to reduce the benefits of a crime. In addition, two

psychological principles also affect the offender's morality. They are 1) reducing provocations, for instance, to neutralize peer-pressure to drink, and 2) removing excuses to remind potential offenders of rules, for instance signs such as 'no eating or drinking on the train'. For an introduction on situational crime prevention, see (Clarke, 1997).

In the present study we want to reduce the opportunity for crime, i.e. laptop thefts. Opportunity, in this context, is defined as the ability of a potential offender to steal a laptop as a consequence of leaving it unattended. We apply the principle of increasing the risk and effort of committing the crime by increasing guardianship of the laptops. We achieve this by advising the potential victims to take care of their laptops and to not to leave them unattended.

Warning signs have been successful in influencing behavior (Argo & Main, 2004; Wogalter et al., 2012). A literature review by Wogalter showed that in the physical world, warnings can be quite effective in notifying people about dangers (Wogalter et al., 2012). However, the design of the warning may affect how the audience reacts to it (Knowles & Linn, 2004). For example, a study conducted by (Nettle, Nott, & Bateson, 2012) showed the impact of warning signs which contain pictures of watchful eyes followed by a related verbal message in reducing bicycle thefts in a university campus. Their warning banners reduced the thefts significantly. However, the crime migrated to places where the warning banners were not placed. This phenomenon is known as "Crime displacement" ("Crime displacement - Securipedia," n.d.). The authors concluded that watchful eyes were responsible for the crime displacement. This suggests that humans are highly sensitive to watchful eyes, a conclusion which is also supported by (Beaman, Klentz, Diener, & Svanum, 1979). Additionally, warnings may sometimes also be counterproductive, which is the

case in the field of smoking & alcohol (Snyder & Blood, 1992). Therefore, it is imperative to test the warnings carefully before implementing them.

Since the aim of this study was to increase the implicit awareness among potential victims rather than to change the behavior of offenders, the watchful eyes were removed from the design. The content of the banner was kept friendly and functioned more as a reminder than a warning. However, the term ‘warning banner’ has been used in the rest of the paper for brevity.

3. METHODOLOGY

The experiment conducted in the present study has two main objectives. First, to conduct an exploratory study to identify whether students and staff (called ‘subjects’ hereafter) actually leave their laptops unattended in the first place. Second, to determine whether an intervention in the form of a warning sign has a significant effect on the behavior of subjects, specifically towards their physical assets. Accordingly, we aim to answer two research questions:

Research question 1: *How often do subjects at the faculty of EEMCS leave their laptops unattended?*

Research question 2: *How successful is a warning sign in reducing the frequency of subjects leaving their laptops unattended?*

3.1. Experimental Setup

The experiment was conducted in two phases as shown in Figure 1. Each phase had a time span of one week, with a break of one week in between. Each phase consisted of five *observation sessions*

(see Section 3.1.1) where the experiment was conducted for 2 hours (from 12:45 to 14:45). This timeslot was chosen based on the results of the pilot study (see Section 3.6), which indicated this timeslot to have the highest subject population.

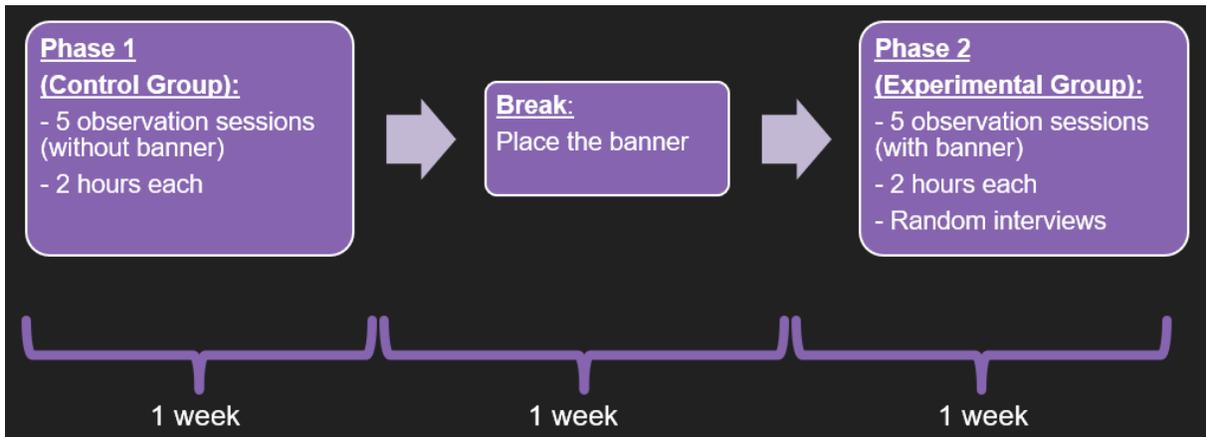


Figure 1: Overview of experimental phases

Three researchers conducted the experiment. The study hall on the 2nd floor of EEMCS was chosen as the location of the experiment. It is a big rectangular hall, with a fleet of chairs at each side facing the windows. There are 20 window seats on the left side of the hall and 20 on the right side of the hall. In addition, there are 11 tables, divided between the left and right side of the hall, with four computers on each table (see Figure 2). These tables provide a view that covers a large area of the hall, so they were the preferred observation positions for the researchers. There are two entrances/exits to the area, i.e. north and south. At its full capacity, it can facilitate approximately 80 students.

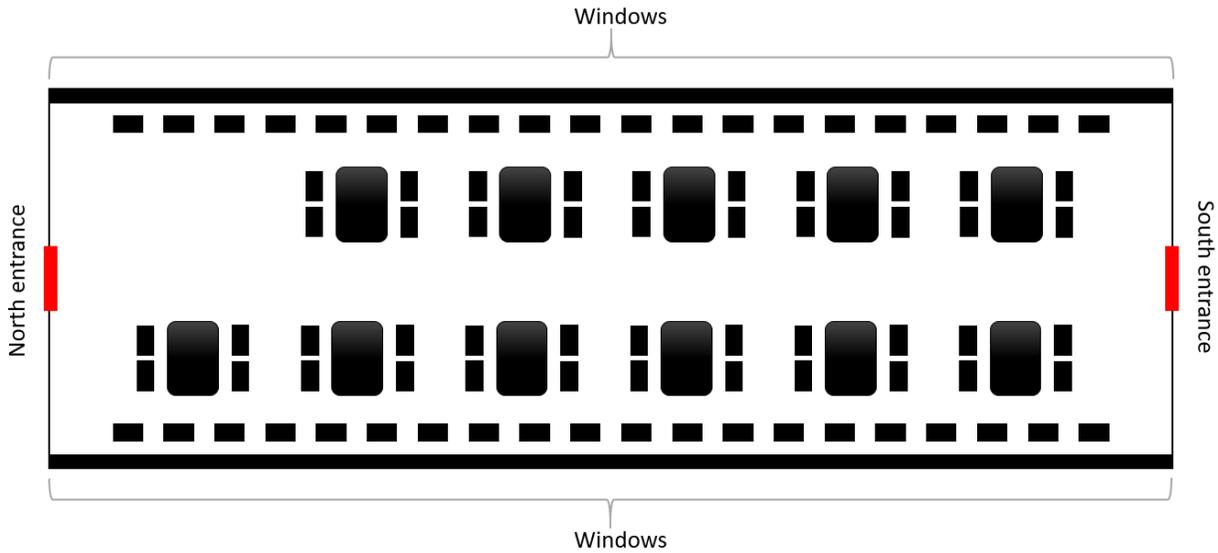


Figure 2: Floor plan of the experimental location

3.1.1. Phase 1

During the first phase of the experiment, observations were performed without any warning banner, thus forming the control group. For each ‘observation session’, the researchers positioned themselves as strategically as possible in the study area. Each had their own exclusive area to cover and they would communicate among each other via text messages. They pretended to work on their computers and observed the subjects subtly from a distance. When a subject got up and left beyond the line of sight of their device, they observed whether the subject left with their laptop or not, and whether the subject’s laptop was in a secure or insecure state. The definitions of secure and insecure are mentioned below, in Section 3.4. The researchers did not engage with any of the subjects’ laptops physically, but only observed them from where they were seated.

3.1.2. The break

After the first phase was over, a total of 12 warning banners were put up at different locations in the hall so that an individual will get to see the warning banner at least twice during his/her time in the hall. The locations included the entrances of the hall and on the pillars facing the tables. No

observations were made during this week as the goal was to provide enough time to the subjects to get acquainted with the presence of the banner.

3.1.3. Phase 2

During the following week, the researchers observed the subjects' behavior in the same manner as during the first phase. Since the warning banners were already in place, these observations formed the experimental group. In addition to the observations, subjects who left their laptops unattended, were randomly chosen for a short interview. One researcher was specifically designated with the task of interviewing the subjects (called 'interviewer' hereafter) to avoid getting unwanted attention towards the other two researchers and to avoid compromising the experiment by priming subjects' behavior. The interviewer was positioned at one of the entrances. Whenever a potential interviewee was selected, one of the researchers would notify the interviewer via a text message. The interviewer would then identify the subject and wait till he/she left the study hall to ask him/her to participate in the interview. The interviewer would inform the subject that he is conducting a study to evaluate the influence of warning banners on students' behavior. If the subject agreed to take part in the interview, he/she would sign an informed consent form (Appendix A) and answer a few questions regarding the newly placed warning signs.

The purpose of the interview was to find the subject's reasoning for leaving his/her laptop unattended. This way, it could be identified why the warning sign did not alter certain subjects' behavior. The phrasing of the interview was chosen with care (Appendix B). For example, it was not explicitly asked why they left their laptop unattended, but rather why they thought others left their laptop unattended. It was expected that the subject would speak from their own perspective,

giving a glimpse of their own intentions and reasoning. Subjects were free to not take part in the interview and were informed so in the beginning.

3.2. Intervention: the warning banner

Studies by (Beaman et al., 1979; Bhattacharjee, 2012; Nettle et al., 2012) provided guidelines for the design of the warning banner. The text of the banner was “NOTICE: Do not leave your personal belongings unattended”, followed by silhouettes of everyday use objects -- laptop, mobile phone, keys, and a notebook. The text color was chosen to be blue because it is a warm, communicative, and a peaceful color (“How Does the Color Blue Make You Feel?,” n.d.). The warning’s aim was to remind subjects to be more careful with their belongings, subconsciously increasing their awareness. The design of the warning banner is shown in Figure 3.



Figure 3: Design of the warning banner used as the intervention

3.3. Participants

The subjects of the experiment were individuals with laptops who studied or worked in the study area of EEMCS. The studied sample mainly included students though it could have been any individual who entered the building. The subjects were self-selected based on their decision to get up and leave from their place during the observation session.

3.4. Variables

There was one independent variable, i.e. the presence of the warning banner (the control/experimental condition). There were two dependent variables, i.e. ‘attended/unattended laptop’ and ‘state of the laptop’.

- *Attended/unattended laptop.* A laptop is defined as unattended when a subject gets up and leaves beyond the line of sight of his/her device. On the contrary, a laptop is defined as attended to when a subject gets up, takes his/her laptop with him/her while leaving some of his/her belongings on the table. The fact that some personal belongings were left behind provides a reasonable expectation that the subject had not left for good.
- *State of the laptop.* When a laptop is left unattended, it can have two states: secure or insecure. A secure state is defined as a visibly locked screen, screen down, or a black screen. A black screen is not necessarily secure. However, the default setting on many computers is to lock the device when the display automatically turns off. It also increases the effort for an offender to find out whether the laptop is indeed unlocked. On the contrary, an insecure state is defined as a clearly unlocked screen, with an application or the desktop visible to the researchers from a distance.

The information from both variables was combined in one dependent variable. This accounted for a total of three possible outcomes -- 1) the subject took the laptop along, 2) the subject left the laptop unattended in a secure state, 3) the subject left the laptop unattended in an insecure state.

It should be noted that the laptops that were already left unattended were not taken into consideration because their true state could not be determined at the time they were left. Moreover, the only consideration for whether a device was secure, was the state of the device itself. However,

a device which may be considered insecure according to definitions stated above but is guarded by a friend in close proximity is unlikely to be stolen. Therefore, this simple consideration can introduce hidden variables in the present study, a limitation which has been reiterated in the discussion section.

The experiment also noted whether any additional variables influenced the dependent variable.

Therefore, four control variables were measured:

- *Gender*. The apparent gender of the subject.
- *Estimated age*. An approximation of the subject's age according to researchers' experience. It was coded as a range, and during data preprocessing these ranges were further narrowed into two categories: '23-25' and 'other'.
- *Number of people present in the surrounding area*. An ordinal range of people (low, medium, high) present in the surrounding area. Low represents [0-1], medium represents [2-3], and high represents [\geq 4] individuals.
- *Location of the laptop in the study hall*. A nominal variable (center, side) stating where the subject was seated in the study hall.

The researchers also collected the following additional information per sample:

- *Datetime*. The date and time when the subject was observed.
- *Remarks about any out of ordinary behavior exhibited by the subject*. A summary of remarks about the subject's behavior.

3.5. Data Handling

Each researcher maintained a local copy of an excel sheet where the measurements were noted down. Since the data was collected by three different researchers, often the terminology did not

match, or certain values were missing because they could not be determined. Therefore, standard vocabulary for the different variables was chosen after the experiment. Then, the readings were calibrated based on that vocabulary and incomplete entries were discarded. Since no Personally Identifiable Information (PII) regarding the subjects was collected, there was no need for anonymization.

3.6. Pilot study

A pilot study was performed before starting the actual experiment to identify and eliminate problems in the research design. The pilot study was a condensed version of the main study explained in Section 3.1 and was performed on two consecutive Mondays -- one day without the banner and one with the banner. Several time slots were experimented with. Moreover, the maximum visibility areas in the study hall and the optimal position of the warning banners were identified. It was noticed that the researchers might have duplicate results, so it was decided that each researcher would have an exclusive area to cover and that they would communicate via text messages.

3.7. Ethical committee

The permission for this study was granted by the ethical committee of Delft University of Technology. The permission to put up warning banners was granted by the building management of the faculty of Electrical Engineering, Mathematics and Computer Science under the number C170414348.

4. RESULTS

During the two-week run, over 220 subjects were observed leaving their workstations. 110 (50%) subjects were observed in each of the two experimental phases. Among the 220 subjects, 148

(67.3%) subjects left their laptops unattended while only 72 (32.7%) took their laptops with them during their absence.

In terms of demographics and other control variables, the following observations were made: 185 (84%) subjects' estimated age was between 23 and 25 years. 152 (69%) were male subjects while only 68 (31%) were females. The subjects surrounded by the number of other people followed a rough normal distribution, with 46 (21%) subjects seated beside low number of people, 147 (67%) subjects seated beside medium number of people, and 27 (12%) seated beside high number of people. Table 1 summarizes the results. However, none of the socio-demographic variables had any relationship with the decision of a subject to leave the laptop unattended (outcome variable). Therefore, these variables were not included in further analysis.

Variable	Value	Samples (N)	Total (N)
Estimated age	23-25 years	185	220
	Other	35	
Apparent gender	Male	152	220
	Female	68	
Number of people in surrounding area	Low	46	220
	Medium	147	
	High	27	
Location of laptop in study hall	Side	128	220
	Center	92	

Table 1: Distribution of control variables' values

Behavioral changes among subjects were observed during the two experimental phases. In the control group, i.e. Phase 1, 83 (75.5%) subjects left their laptops unattended, while only 27 (24.5%) took their laptops with them. Moreover, among the subjects who left their laptops unattended, a little over half (46) left the laptops in a secure state while the rest 37 (44.5%) left them in an insecure state. After the warning banner was placed, the frequency of subjects leaving their laptops unattended reduced significantly -- only 65 (59.1%) subjects, which was previously 83 (75.5%), left their laptops unattended. Among the subjects who still left their laptops unattended this time around, 35 (53.8%) left them securely, while 30 (46.2%) left them insecurely, which does not show much variation in percentage compared to the control group.

In summary, there is an increase of 16.4% in the subjects who take their laptops along with them in the experimental group. These differences are statistically significant as can be seen in Table 2*. However, the difference between the state of the laptop when it was left unattended among the control and experimental group is not significant, which is shown in Table 3**.

	Control group	Experimental group	Difference experimental group in comparison with control
Laptop left unattended	75.5%	59.1%	- 16.4%
Took laptop along	24.5%	40.9%	16.4%
Total samples (N)	110	110	
Pearson Chi Square = 6.689, p = 0.0097*			

Table 2: All subjects, with attended and unattended laptops, in %

	Control group	Experimental group	Difference experimental group in comparison with control
Unattended and Secure	55.4%	53.8%	1.6%
Unattended and Insecure	44.6%	46.2%	-1.6%
Total samples (N)	83	65	
Pearson Chi Square = 0.036, p = 0.848**			

Table 3: State of the laptop for subjects who left their laptops unattended, in %

Lastly, a qualitative analysis was performed on the answers received from 17 interviews. The interviewees were randomly selected subjects from the experimental group who still left their laptops unattended after the banner was placed (65 subjects). Most of the interviewees (10) had noticed the warning sign and mentioned that it had a positive effect on the awareness of people. However, their own behavior was opposite to what they said, indicating a discrepancy in their beliefs and actions. When asked why the subjects thought other people did not follow warning signs, seven suggested that it might be because of convenience – extra effort is required to carry the laptop along. Four interviewees stated that it might be to keep their spot occupied, while other four mentioned that people might consider the study hall (and faculty building) as a safe environment. Meanwhile, the Kensington study puts educational institutes as one of top organizations prone to laptop thefts. This implies that in addition to the discrepancy in the subjects’ beliefs and actions, they also have a false sense of security or high faith in the security mechanisms at the faculty.

5. DISCUSSION

To summarize, the aim of the present empirical study was to investigate the effectiveness of a warning banner to encourage laptop users not to leave their laptop unattended in a university study hall. In line with the principles of situational crime prevention (Cornish & Clarke, 1987; Cornish et al., 2008; Wortley, 1996), we expected that a warning banner would increase the efforts and risk for a potential offender by increasing the guardianship of the laptop. We studied the behavior of 220 subjects in a study hall of a university. Subjects were mostly males, corroborating the findings of (Lörz, Schindler, & Walter, 2011) regarding gender gap in technical studies.

The first research question aimed to identify how often subjects at the EEMCS faculty left their laptops unattended. The results showed that in the control group, most of the subjects (75.5%) left their laptops unattended, which proves that the problem of unattended laptops is highly relevant. Furthermore, it also raises questions regarding students' level of security awareness within university premises. After all, even if the faculty is considered safe, personal precautionary measures are most important to prevent misuse and/or data breaches (Dimkov et al., 2010).

For the second research question, we investigated whether a warning sign is effective in reducing the frequency of subjects leaving their laptops unattended. The warning banner used in present study was designed keeping in mind the effectiveness of the use of graphical aid in warning signs (Laughery, Young, Vaubel, & Brelford, 1993; Young & Wogalter, 1990), and the known problems with warning signs, such as removing a picture of 'watchful eyes' which seemed to lead to crime displacement (Nettle et al., 2012). Our findings showed that merely putting the banner for three weeks was sufficient to see significant positive behavioral changes among the subjects. The number of subjects who took their laptops along, when temporarily leaving their workstations,

increased from 25% to 41% after the warning banner was placed. This is in line with much of the previous research that showed that warnings can be effective in influencing behavior, as demonstrated by Argo & Main (2004), Laughery & Wogalter (2006) and Neuschatz, Benoit, & Payne (2003).

However, some studies found limited effectiveness of warnings. For instance, Nettle et al. (2012)'s warning was effective but they found crime displacement because of watchful eyes in warnings about bicycle theft; Snyder & Blood (1992) found that warnings against alcohol and smoking have reverse effect on young adults. Taken together these findings suggest that warning's effectiveness is context-dependent and sometimes dependent on the product or the group for whom it is meant.

Overall, the present study shows that simple and inexpensive interventions are effective in changing behavior. This is a highly desirable outcome for security professionals as it hits the sweet spot between budget allocation and security achieved. It also shows the necessity to test intervention before implementing them at a broader scale.

Among those who left their laptops unattended (secure or insecure), there was no apparent change in behavior. The subjects who left their laptops behind in both cases did not seem to care about the state of the laptop either as secure or insecure. There could be two possible reasons behind this observed behavior: 1) As shown from the interview results, some subjects had trust in the safety of the faculty so if no one was going to steal their laptop, no one would have interacted with it either, hence the state did not matter; 2) Since the warning banner only reminded subjects to not to leave their belongings 'unattended', as opposed to 'safe', the subjects might have been unaware of the implications of leaving their laptop in an insecure state. After all, the purpose of the banner

was to remind subjects about safety precautions, but it left out an important aspect of safety -- protecting their cyber assets. Therefore, further investigation is required to identify which of the two reasons are responsible for the absence of change in behavior among the subjects.

5.1. Limitations and Future work

The watchful eyes were removed from the warning banner, but not from the experiment itself. During the field experiment, when a subject spotted the researchers looking at them, they often either left their laptops in a secure state before leaving or took their laptops with them. This suggests that if individuals believe that they are being monitored, they are more likely to behave in a prudent fashion. This observation is in line with a study conducted by (Beaman et al., 1979), who showed the effect of watchful eyes on children when left unattended to take only a limited 'allowed' number of sweets from a bowl. The study showed that the children behaved better when they felt they were being monitored, even if the watchful eyes were their own in a mirror reflection. This proves that humans are very sensitive to monitoring, and the researchers should have taken it into account while conducting the experiment.

The level of prudent behavior and the extent to which students left their laptops unattended seemed related to the distance between them and their laptop and how long they are going away for. Most subjects felt comfortable leaving their laptops insecure if their destination was inside the study hall, for example, if they were going to throw something in the dustbin or talk to a friend. Similar results were observed when they were leaving to run a small errand, such as refilling their water bottle. For these tasks, although they had to go outside the study hall, but it only took a few minutes. This pattern was observed many times by the researchers and suggests that there is a

correlation between distance/interval and the decision of the laptop owners. This observation also suggests that while it might seem careless on the subjects' part for leaving their laptops unattended, their behavior might have been more rational and careful. Hence, further research in this domain is warranted.

The secure and insecure states only catered for the situations present in definitions stated in Section 3.4. Other factors such as the proximity of others to the device, positioning of the device, having a guardian close by, and so on, were not included in the assessment of the device's state. These factors might explain a subject's behavior towards leaving their laptop unattended. However, since the other control variables that were included in our study initially were not significantly related to the outcome variable, it seems unlikely to be the case.

There is a possibility that subjects who were leaving with their laptops were only doing so because they were leaving the study hall for good. In order to prevent these results from contaminating the experiment, measurements were noted only for subjects who left some of their belongings behind so there was a reasonable expectation that they would be coming back. However, this observation sheds some light on the relevance of the subject's relative long-term intentions, which were not considered when performing the present study. In the future, the effect of these additional variables can be studied in detail.

The interview questions were framed in a way that the subjects were not explicitly asked for the reasons of their actions but rather their point of view towards the actions of others in a similar situation. As mentioned in the experimental setup (Section 3.1), this was done because we did not want to prime the subjects' answers. However, this might also have shifted the pressure from the

subjects to others, not giving the insight that the researchers were looking for. Consequently, the answers of the interviews might not have reflected their own motivations, which was the intended purpose of the interviews to begin with. Therefore, additional studies need to be conducted exploring this aspect of human interactions.

We were unable to observe whether there was some form of displacement, and whether the increased prudent behavior of students who took their laptop with them when they temporarily left their place in the hall was transferred to other situations or not. Previous research mentioned that situational crime prevention can lead to displacement of crime but also to diffusion of benefits (Guerette & Bowers, 2009). However, in this case, neither of the two phenomena could be observed. The design of the warning banner was such that it reminded subjects to never leave without their belongings but did not warn them about the implications of assets left in an insecure state. While this might explain the lack of diffusion of benefits in the results, further research in this domain is warranted to be able to conclude this.

Lastly, the duration of the experiment was quite short and behavioral changes take time (Prochaska, Norcross, & DiClemente, 1994). The banners were only up for three weeks. It is possible that the subjects who still left their laptops unattended either did not notice the banners or did not take them seriously. In the future, a more extensive experiment will be conducted with more time for each phase to measure behavioral changes.

6. CONCLUSIONS

Laptops are cyber-physical assets that often contain highly sensitive information, such as credentials and confidential documents. As a result, the value of the laptop is an accumulation of

the value of both, the physical device itself and the cyber assets it contains. Laptops are one of the most commonly stolen objects from universities and research labs. However, for this to be the general conclusion, opportunity for the offender plays an important role. In this paper, we present our findings from an empirical study conducted at a study hall of a university to find the prevalence of students and staff leaving their laptops unattended. We found that 148 out of 220 subjects left their laptops unattended during our study which lasted for three weeks. Moreover, as an application of situational crime prevention, we evaluated the effectiveness of a simple warning sign as an intervention to correct the behavior of individuals and to reduce the opportunity for potential attackers. In just a short period, the percentage of subjects leaving their laptops unattended reduced significantly from 75.5% to 59.1%. Lastly, we also conducted a qualitative analysis on the responses of interviews from subjects who left their laptops unattended even after the warning banners were placed. The results show an interesting mix of convenience, and a blind trust on the safety of the faculty.

ACKNOWLEDGEMENTS

The authors would like to thank William Freeborn (University of Technology, Sydney, Australia) and Nils Bijlsma (Delft University of Technology, The Netherlands) for their contributions in the design and execution of the experiment.

FUNDING

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

DECLARATIONS OF INTEREST: None

AUTHOR CONTRIBUTION: The field experiment was the brainchild of Azqa Nadeem and she is also the main author of this article. Marianne Junger provided extensive guidance in the preparation of the article and the literature that was cited.

REFERENCES

Argo, J. J., & Main, K. J. (2004). Meta-Analyses of the Effectiveness of Warning Labels.

Journal of Public Policy & Marketing, 23(2), 193–208.

Baheti, R., & Gill, H. (2011). Cyber-physical systems. *The Impact of Control Technology*, 12, 161–166.

Beaman, A. L., Klentz, B., Diener, E., & Svanum, S. (1979). Self-awareness and transgression in children: Two field studies. *Journal of Personality and Social Psychology*, 37(10), 1835–1846.

Best universities in the Netherlands. (2017, September 5). Retrieved May 26, 2018, from <https://www.timeshighereducation.com/student/best-universities/best-universities-netherlands>

Bhattacharjee, A. (2012). *Social Science Research: Principles, Methods, and Practices*. CreateSpace.

Center for Problem-Oriented Policing | 25 Techniques. (n.d.). Retrieved May 26, 2018, from <http://www.popcenter.org/25techniques/>

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 30(8), 719–731.

Clarke, R. V. G. (1997). *Situational crime prevention*. Criminal Justice Press Monsey, NY.

Coleman, J. S. (1958). *Relational Analysis: The Study of Social Organizations with Survey*

- Methods. *Human Organization*, 17(4), 28–36.
- Cornish, D. B., & Clarke, R. V. (1987). UNDERSTANDING CRIME DISPLACEMENT: AN APPLICATION OF RATIONAL CHOICE THEORY. *Criminology; an Interdisciplinary Journal*, 25(4), 933–948.
- Cornish, D. B., Clarke, R. V., Wortley, R., & Mazerolle, L. (2008). Environmental criminology and crime analysis. *Willan Publishing, Devon*.
- Crime displacement - Securipedia. (n.d.). Retrieved May 26, 2018, from https://securipedia.eu/mediawiki/index.php/Crime_displacement
- Dimkov, T., Pieters, W., & Hartel, P. (2010). Laptop theft. In *Proceedings of the 17th ACM conference on Computer and communications security - CCS '10*. <https://doi.org/10.1145/1866307.1866391>
- Felson, M., & Eckert, M. A. (2017). *Introductory Criminology: The Study of Risky Situations*. Routledge.
- Filkins, B., & Hardy, G. M. (2016). IT security spending trends. A SANS Survey. SANS Institute.
- Ghernouti-Hélie, S., Tashi, I., & Simms, D. (2010). A Multi-stage Methodology for Ensuring Appropriate Security Culture and Governance. In 2010 International Conference on Availability, Reliability and Security (pp. 353–360).
- Gigerenzer, G., & Goldstein, D. G. (1996). Reasoning the fast and frugal way: models of bounded rationality. *Psychological Review*, 103(4), 650–669.
- Guerette, R. T., & Bowers, K. J. (2009). Assessing the extent of crime displacement and diffusion of benefits: A review of situational crime prevention evaluations. *Criminology; an Interdisciplinary Journal*, 47(4), 1331–1368.
- How Does the Color Blue Make You Feel? (n.d.). Retrieved May 26, 2018, from

<https://www.verywellmind.com/the-color-psychology-of-blue-2795815>

Keane, J. (2016, January 13). Why stolen laptops still cause data breaches, and what's being done to stop them. Retrieved May 26, 2018, from <http://www.pcworld.com/article/3021316/security/why-stolen-laptops-still-cause-data-breaches-and-whats-being-done-to-stop-them.html>

Knowles, E. S., & Linn, J. A. (2004). The promise and future of resistance and persuasion. *Resistance and Persuasion*, 301–310.

Laptops hold more sensitive data, but they're less protected than smartphones | Enforce Encryption on Third-Party Devices – Laptop Encryption as a Service – AlertSec. (n.d.-a). Retrieved May 26, 2018, from <https://www.alertsec.com/new-data-reveals-that-the-machine-that-holds-the-most-sensitive-data-is-frequently-not-encrypted-raising-security-risks/>

Laptops hold more sensitive data, but they're less protected than smartphones | Enforce Encryption on Third-Party Devices – Laptop Encryption as a Service – AlertSec. (n.d.-b). Retrieved May 26, 2018, from <https://www.alertsec.com/new-data-reveals-that-the-machine-that-holds-the-most-sensitive-data-is-frequently-not-encrypted-raising-security-risks/>

Laughery, K. R., & Wogalter, M. S. (2006). Designing Effective Warnings. *Reviews of Human Factors and Ergonomics*, 2(1), 241–271.

Laughery, K. R., Young, S. L., Vaubel, K. P., & Brelsford, J. W. (1993). The Noticeability of Warnings on Alcoholic Beverage Containers. *Journal of Public Policy & Marketing*, 12(1), 38–56.

Lörz, M., Schindler, S., & Walter, J. G. (2011). Gender inequalities in higher education: extent, development and mechanisms of gender differences in enrolment and field of study choice. *Irish Educational Studies*, 30(2), 179–198.

Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive data.

Network Security, 2012(12), 5–8.

Nettle, D., Nott, K., & Bateson, M. (2012). “Cycle Thieves, We Are Watching You”: Impact of a Simple Signage Intervention against Bicycle Theft. *PloS One*, 7(12), e51738.

Neuschatz, J. S., Benoit, G. E., & Payne, D. G. (2003). Effective warnings in the Deese-Roediger-McDermott false-memory paradigm: the role of identifiability. *Journal of Experimental Psychology. Learning, Memory, and Cognition*, 29(1), 35–41.

News & Press Center - Kensington - Kensington - A Mobile Device is Stolen Every Minute; Most Thieves Strike in the Office or During a Meeting. (n.d.). Retrieved May 26, 2018, from <https://www.kensington.com/us/in/n/3699/763/a-mobile-device-is-stolen-every-minute-most-thieves-strike-in-the-office-or-during-a-meeting>

Ponemon, L. (2012). The cost of a lost laptop. White Paper, Ponemon Institute, Apr. 2009.

Prochaska, J. O., Norcross, J. C., & DiClemente, C. C. (1994). *Changing for good*. Avon Books New York.

Simon, H. A. (1955). A Behavioral Model of Rational Choice. *The Quarterly Journal of Economics*, 69(1), 99–118.

Snyder, L. B., & Blood, D. J. (1992). Caution: Alcohol advertising and the surgeon general’s alcohol warnings may have adverse effects on young adults. *Journal of Applied Communication Research: JACR*, 20(1), 37–53.

Strom, D., Curry, D., Sponsors, R., Andersen, J., & Church, G. (2012, February 14).

[Infographic] The Cost of Stolen Laptops - ReadWrite. Retrieved July 29, 2017, from <https://readwrite.com/2012/02/14/infographic-the-cost-of-stolen/>

The Importance of Having a Laptop | Techwalla.com. (n.d.). Retrieved May 26, 2018, from <https://www.techwalla.com/articles/the-importance-of-having-a-laptop>

Wikipedia contributors. (2018, May 25). Utilitarianism. Retrieved May 26, 2018, from

<https://en.wikipedia.org/w/index.php?title=Utilitarianism&oldid=842865400>

Wogalter, M. S., Laughery, K. R., & Mayhorn, C. B. (2012). Warnings and hazard communications. *Handbook of Human Factors and Ergonomics, Fourth Edition*, 868–894.

Wood, W. (n.d.). LAPTOP THEFT: A GROWING CONCERN FOR ORGANIZATIONS.

Retrieved from http://iacis.org/iis/2007/Behling_Wood.pdf

Wortley, R. K. (1996). Guilt, shame and situational crime prevention. In *The politics and practice of situational crime prevention* (Vol. 5, pp. 115–132).

Young, S. L., & Wogalter, M. S. (1990). Comprehension and Memory of Instruction Manual Warnings: Conspicuous Print and Pictorial Icons. *Human Factors*, 32(6), 637–649.

Consent to Participate in a Research Study
IMPACT OF WARNING SIGNS ON STUDENT BEHAVIOR - INTERVIEW

You are invited to be part of a short interview about whether warning banners affect student sensitivity to cyber security. The study is being conducted by Azqa Nadeem, William Freeborn, and Nils Bijlsma of TU Delft. The purpose of the research is to study the impact of warning signs placed around different locations at TU Delft and the awareness of students about such warning signs. The results may be used for future studies, and to assist decision-makers make more informed decisions at both TU Delft and other universities.

If you agree to be part of the study, you will be asked to answer some questions, which could take a maximum of **5 minutes**. Participating in this study is completely voluntary. Even if you decide to participate now, you may change your mind and stop at any time. You may choose not to answer questions for any reason.

If you have questions about this research study, you can contact the researcher, William Freeborn, TU Delft, wfreeborn@student.tudelft.nl.

The ethical committee at TU Delft has approved this study.

I agree to participate in the study.

Signature

Date

Appendix B: Interview Questions

Hi,

We are students of Computer science at TU Delft. We are taking an interesting course in which we are studying the impact of warning signs around campus on students' behavior. We were wondering if you could spare a few minutes of your time to talk to us regarding that?

[Subject says no]:

No problem. Have a nice day!

[Subject says yes]:

Great! Thank you very much!

There is a recently placed warning sign in the study area that reminds people about being responsible with their own belongings. Have you noticed that?

[Subject says no]:

Do you normally look out for warning signs?

[Note answer]

In your opinion, why do you think you miss warning signs? Are they placed obscurely or are they unnoticeable?

[Note answer]

[Subject says yes]:

Do you think such warning signs motivate you to change anything in your behavior or to be more aware of your surroundings?

[Note answer]

We noticed that many people see the warning signs but still leave their belongings unattended, and we are wondering why that might be the case. What is your take on it?

[Note answer]

That is all. Thank you for your time and have a nice day!