Users Really Do Plug in USB Drives They Find

Matthew Tischer† Zakir Durumeric‡† Sam Foster† Sunny Duan†
Alec Mori† Elie Bursztein◇ Michael Bailey†

† University of Illinois, Urbana Champaign ‡ University of Michigan ◇ Google, Inc.
{tischer1, sfoster3, syduan2, ajmori2, mdbailey}@illinois.edu
zakir@umich.edu elieb@google.com

***Abstract*— We investigate the anecdotal belief that end users will pick up and plug in USB flash drives they find by completing a controlled experiment in which we drop 297 flash drives on a large university campus. We find that the attack is effective with an estimated success rate of 45–98% and expeditious with the first drive connected in less than six minutes. We analyze the types of drives users connected and survey those users to understand their motivation and security profile. We find that a drive's appearance does not increase attack success. Instead, users connect the drive with the altruistic intention of finding the owner. These individuals are not technically incompetent, but are rather typical community members who appear to take more recreational risks than their peers. We conclude with lessons learned and discussion on how social engineering attacks — while less technical — continue to be an effective attack vector that our community has yet to successfully address.**

I. Introduction

The security community has long held the belief that users can be socially engineered into picking up and plugging in seemingly lost USB flash drives they find. Unfortunately, whether driven by altruistic motives or human curiosity, the user unknowingly opens their organization to an internal attack when they connect the drive — a physical Trojan horse. Our community is filled with anecdotes of these attacks and pentesters have even boasted that they can *hack humans* by crafting labels that will pique an individual's curiosity [19]: "While in the bathroom, I place an envelope in one stall. On the cover of the envelope I put a sticker that says PRIVATE. Inside the 'private' envelope is a USB key with a malicious payload on it. I do this in one stall and also in the hallway by a break room to increase my chances and hope that the person that finds one of them is curious enough to insert it into their computer. Sure enough, this method seems to always work."

However, despite recent attacks that underscore the risk of malicious peripherals [39], [55] and rumors of the attack's efficacy, there has been little formal analysis of whether the attack is effective nor why users connect the drives. In this work, we investigate the classic anecdote by conducting a large scale experiment in which we drop nearly 300 flash drives of different types, in different locations, and at different times on the University of Illinois, Urbana-Champaign campus.

We measure the efficacy and speed of the attack by replacing expected files on the drive with HTML files containing an embedded `img` tag that allows us to track when a file is opened on each drive without automatically executing any code. We find that users pick up and connect an estimated 45%–98% of the drives we dropped. Further, the attack is expeditious with a median time to connection of 6.9 hours and the first connection occurring within six minutes from when the drive was dropped. Contrary to popular belief, the appearance of a drive does not increase the likelihood that someone will connect it to their computer. Instead, users connect all types of drives unless there are other means of locating the owner — suggesting that participants are altruistically motivated. However, while users initially connect the drive with altruistic intentions, nearly half are overcome with curiosity and open intriguing files — such as vacation photos — before trying to find the drive's owner.

To better understand users' motivations and rationale, we offered participants the opportunity to complete a short survey when they opened any of the files and read about the study. In this survey, we ask users why they connected the drive, the precautions they took, demographic information, as well as standard questions to measure their risk profile and computer expertise. We find that attack was effective against all sub-populations at Illinois. The majority of respondents connected a drive to locate its owner (68%) or out of curiosity (18%), although a handful also admitted they planned on keeping the drive for themselves.

The students and staff that connected the drives were not computer nor security illiterate and were not significantly different than their peers at the University of Illinois on Egelman and Peer's Security Behavior Intentions Scale (SeBIS) [12]. While the users that connected the drive engaged in riskier behavior than their peers on the DOSPERT scale [4], they were more risk averse than the general population in every domain except for recreational risk.

When prompted, 68% of users stated that they took no precautions when connecting the drive. For those respondents who considered protective measures, 10 (16%) scanned the drive with their anti-virus software and 5 (8%) believed that their operating system or security software would protect them, e.g., "I trust my macbook to be a good defense against viruses". Surprisingly, another 5 (8%) sacrificed a personal computer or used university resources to protect their personal equipment. In the end, all but a handful of the users who took precautions did so in an ineffective manner and the majority took no precautions at all.

These results — particularly the risk averseness relative to the general population on the DOSPERT scale — suggest that the attack would be effective against most users and that the average person does not understand the danger of connecting an unknown peripheral to their computer. We hope that by bringing these details to light, we remind the security community that

some of the simplest attacks remain realistic threats. There is still much work needed to understand the dynamics of social engineering, develop technical defenses, and learn how to effectively teach users how to protect themselves.

II. Related Work

Our work is based on anecdotal evidence that users will plug in USB flash drives they stumble upon [30], [43], [49], [52] and prior work that has shown that simply connecting a USB drive presents an immediate risk.

Removable Device Attacks. Microsoft Windows no longer automatically executes arbitrary code when connecting a USB drive [36], which defeats many of the traditional attacks [1], [37]. However, despite this precaution, connecting a USB drive still poses significant risk. In 2014, Nohl et al. showed that an attacker can reprogram the firmware in a USB drive to convert it into a USB human interface device that automatically executes malicious code, or into a network interface that intercepts sensitive traffic [33]. Similarly, file previews are automatically generated on connection and vulnerabilities in installed applications can enable an attack. For example, in 2013, a vulnerability in SketchUp allowed code execution during file preview generation [3]. Larimer showed that the same vein of attacks are possible on Linux [25] and work by both Sevinsky [40] and Hudson [20] extended this attack beyond USB to Thunderbolt devices.

USB Drive Engineering. Despite the pervasiveness of the belief that users will plug in USB drives they find, there has been no peer-reviewed research on the topic. Jacobs informally investigated the question: "Are USB flash drives an effective social-engineering vector for cyber attacks targeting commercial and residential computer systems?" in his masters thesis and found that 11 out of 30 flash drives were opened in each of the commercial and residential areas [21]. More recently, CompTIA commissioned a study that dropped 200 flash drives containing text files with email addresses or trackable links in "high traffic public spaces" in four cities. They also fielded a survey but did not survey participants who interacted with the flash drives [9]. We compare our results to both studies throughout the paper.

Social Engineering Attacks. There have been several studies that broadly focus on social engineering. Researchers have used social networks to increase the effectiveness of phishing attacks [22]. Wright left 50 unsecured smartphones in cities to observe their finders' behaviors [53]. Christin et. al investigated the incentive necessary to convince users to run an unknown binary using Mechanical Turk [8]. Greitzer et al. define the Unintentional Insider Threat problem, discuss case studies, and provide recommendations [18].

Social Engineering Susceptibility. There have been several studies that aimed to determine the relationship between demographic factors and cybercrime victims [5], [6], [27], [28], [32], [51], [54]. Beyond specific attacks, there have been several studies that measured what factors affect security hygiene and user behavior [2], [31], [35], [38], [47].

Decision Making. There has been much previous work on human decision making processes. We build on this literature, using the DOSPERT scale [4], [50] to measure participants' risk-taking profile and the SeBIS survey [12] to measure security knowledge and behavior. Our work underscores existing literature on users' attitudes towards security [7], [13], [14], [16], [23], [41], further suggesting that users can generally identify technology risks but do not necessarily understand them.

III. Methodology

To determine whether users pick up and connect USB flash drives they find, we dropped 297 flash drives at the University of Illinois Urbana-Champaign — a large academic institution in the United States — and measured who connected the drives and why.

Each flash drive contained files that are named consistently with the drive's appearance, but are HTML files containing an `img` tag that referenced our centrally managed server and offered the user an opportunity to answer a survey about why they picked up the flash drive. We measured (1) whether users picked up the flash drives (2) whether users later plugged connected the drives and opened files and (3) why users plugged in the flash drives. In this section, we describe our experiment in detail.

A. Drive Selection and Placement

We wanted to measure not only whether users picked up flash drives, but whether external appearance affects users' behavior. In our experiment, we varied the (1) geographic drop location, (2) the physical appearance of the drive (e.g., using an external label), and (3) the time of day and measured their effect:

1) **Geographic Location.** We placed flash drives at 30 unique locations on the campus, ten at each of three sub-campuses (Main Quad, South Quad, and Engineering Quad). On each sub-campus, we placed drives at five location types: parking lots[1], hallways, academic areas (e.g., classrooms or libraries), common areas (e.g., building lobbies or cafeterias), and outside (e.g., sidewalks). We distributed the experiment among the three sub-campuses to reduce the chance of arousing suspicion.
2) **Drive Appearance.** We varied the type of drives dropped at each location to determine whether users picked up the drive for altruistic or selfish reasons.[2] Two types are engineered to trigger altruistic tendencies: drives with a return address or with keys attached; two are intended to trigger selfish tendencies: drives with the label "confidential" or "final exam solutions"; one is our control group: drives with no label. We show an example of each in Figure 1.
3) **Time of Day.** We dropped drives during the morning (6– 10am) and afternoon (1– 5pm). By varying drop time, we hoped to target faculty, staff, and students both coming to and leaving campus.

We dropped each of the five drive types at two times of day at 30 locations for a total $5 \times 2 \times 30 = 300$ drives.

[1]Five of the six parking lots are designated for faculty/staff only.

[2]Prior work by Forbes et al. have argued that participants who return keys do so for altruistic reasons [15].

(a) Unlabeled drive (b) Drive with keys (c) Drive with return label (d) Confidential drive (e) Exam solutions drive

Fig. 1: **Drive Appearances**—We dropped five different types of drives. We chose two appearances (keys and return label) to motivate altruism and two appearances (confidential and exam solutions) to motivate self-interest, as well as an unlabeled control.

B. Drive Content

Each drive contained files consistent with external appearance, as depicted in Figure 2. The only difference was that all of the files on the drives were HTML documents, which contained an `img` tag for an image located on a centrally controlled server. This embedded image allowed us to detect when a file was opened from an Internet-connected computer, but did not execute any code on the machine. The HTML file also explained the study, allowed recipients to withdraw from the experiment, and included a link to a follow-up survey. We emphasize that we do not automatically run *any* code on participants' machines. As such, we may under count responses if a user connected the drive, but did not open any of the HTML files.

C. Survey

To understand why users picked up the flash drives and to measure users' risk attitudes, we offered users who picked up flash drives the opportunity to complete an anonymous survey on their risk attitudes for $10 compensation. In this survey, we asked participants a range of questions using SurveyMonkey [44] that broadly measured a user's risk-taking profile, computer security expertise, and rationale for plugging in the flash drive. We specifically asked about:

1) **Demographics.** We asked demographic questions from SurveyMonkey's question bank (e.g., age, sex, and level of education) [17].
2) **Affiliation.** We asked a participant their affiliation with the University of Illinois (e.g., faculty, staff, or student).
3) **Previous Knowledge.** We asked if the participant had previously heard about the study. We later discarded responses where the user had pre-existing knowledge.
4) **Motivation.** We asked the participant why they picked up the flash drive and if external appearance or any other factor affected their decision.
5) **Computer Expertise and Behaviors.** We asked questions from the SeBIS Survey [12] to measure the participants' computer and computer security behaviors and three questions from another study [27] to measure their computer expertise.
6) **Risk Attitude.** We presented questions from the DOSPERT Survey [4], a standardized survey for measuring how likely a participant is to take part in risky behavior.
7) **Internet Usage.** We asked how much time the user spent online on a weekly basis. We asked this because previous studies have found that time spent on the Internet and visits to certain types of websites correlate with cybercrime victimization or malware encounters [6], [27], [32], [51], [54].

We also added six confirmation questions that instructed participants to chose a specific answer in order to check whether they were still paying attention to the survey. Once the participant finished the survey, they were offered the choice of a $10 Amazon gift card or to meet a researcher in person and collect $10 in cash compensation.

To collect baseline values for the University of Illinois, we emailed a random 600 members of the Illinois community in December 2015, in which we asked users to complete a version of the survey with the USB-related questions removed. The surveys were otherwise identical and participants were compensated with either a $5 Amazon gift card or $5 in cash compensation.

D. Ethical Considerations

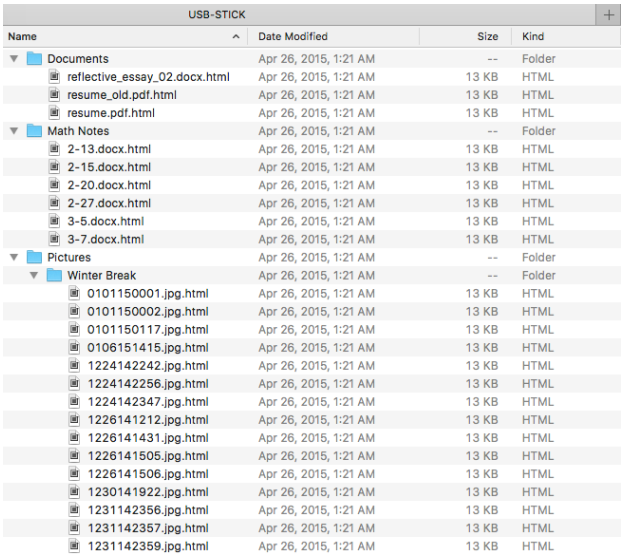
We submitted and received IRB approval for both the experiment and base line survey. We explicitly note that our experiment employed a degree of deception: we misrepresented the purpose of and content on the flash drives. Throughout the experiment, we provided participants with contact information for both our team and the University of Illinois IRB. We allowed participants to exclude themselves from the experiment when they clicked on any of the HTML files on the flash drives. We received no negative feedback from participants and as we discuss in Section IV; several participants expressed their appreciation for the research and asked about our results.

To minimize the risk to participants' computers, we did not automatically run any code on participants' systems and the HTML files contained no scripts. We purchased the USB drives from a reputable vendor and tested the drives to ensure they did not present any unusual warnings on our test systems.

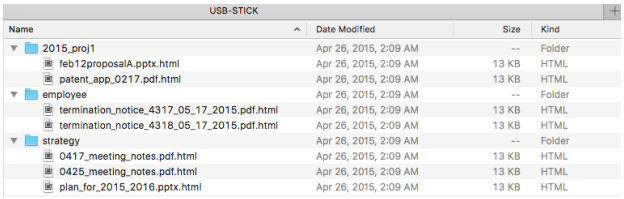
E. Execution

We dropped 297 flash drives during the week of April 27, 2015, a typical week on the campus.[3] Our team dropped 143 drives on 4/27, 145 drives on 4/28, and 9 drives on 4/29.

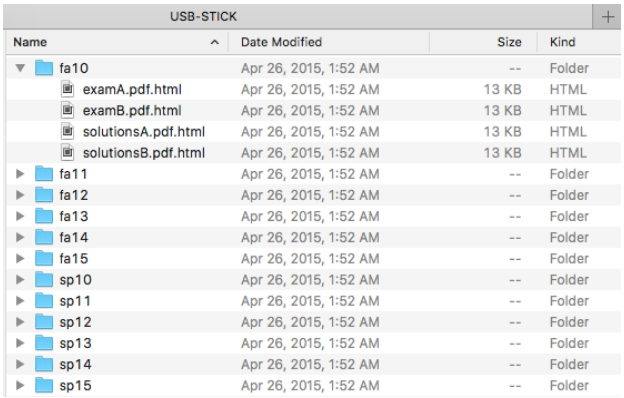
[3]We intended to drop 300 drives. One drive was lost during the experiment, and a researcher could not physically access one location to drop two drives.



(a) **Personal Contents**—Unlabeled, keys, and return label drives contain these files.



(b) **Business Contents**—Confidential drives contain these files.



(c) **Exam Contents**—Exam drives contain these files. Note that only one folder is expanded for brevity; all other folders contain the same file names.

Fig. 2: **Drive Contents**—We show the folder structures for each drive type. Contents were chosen to match the flash drives' appearances and provide participants with multiple file options.

A team of eight students dropped drives in plain sight. Our protocol was similar to the one defined by Lastdrager et al., in which students would walk around and pretend to tie their shoelaces, look around to see if anybody noticed them, and then drop the USB key before walking away [26].

After dropping the drives, the researchers recorded the location of the drive on a smartphone. Throughout the day, the researchers would check on the location and record whether the drive had been moved or removed. Researchers were instructed not to touch or move the drives and not to interact with any subjects. Drives were checked once per drop period (6–10 am, 1–5 pm) until they were taken or until the end of 5/1.

IV. Results

We analyzed the drives that were picked up, the drives connected to a computer, and the files opened on each drive. We present the details of this analysis in this section.

Participants opened one or more files on 135 of the 297 flash drives (45%) and 290 of the drives (98%) were removed from their drop locations by the end of our observation period. It is not clear if users plugged in the remaining 155 drives—a participant might have plugged in a drive without opening a file or simply might not have had connected the drive. However, these two numbers allow us to bound the attack's success rate to be between 45–98%. Of the 135 users who plugged a drive into their computer, 77 (57%) did not explicitly opt-in to providing detailed data. We include them in the raw number of users who plugged in a drive, but exclude them from any further analysis in this study.[4]

A. Affecting Success Rate

When we dropped drives, we varied (1) geographic location, (2) time of day, and (3) drive appearance. We applied the test of equal proportions and find that geographic location, time of day, and day of week have no affect on whether a user plugs in the drive (Table I). While none of the different drive types had a *higher* success rate, the drives with return labels had a lower success rate: only 17 of 59 (29%) of drives with return address labels were plugged in compared to 27 of 60 (45%) of unlabeled drives ($p = 0.10$). We suspect that this is because altruistic participants had another means of locating the drive owner. We present the exact values for each category in Table I.

B. Opened Files

We analyzed the files that users opened to determine whether users are acting altruistically or selfishly. While the fact that fewer participants connected drives with return address labels suggests that users are acting altruistically, the order of file operations paints a slightly different picture. The unlabeled drives, as well as the drives with keys and/or return address

[4]In two cases, consent was recorded, but no files were opened. We suspect that users opened the HTML files in a text editor or opened the files on a machine without Internet access.

[5]Significantly fewer drives that were dropped on Tuesday were opened, but all return label drives were dropped on that day and when they are removed from the data set, the difference is no longer significant.

Category	Drives Opened		p
Drive Type			
Confidential	29/58	(50%)	0.72
Exams	30/60	(50%)	0.71
Keys	32/60	(53%)	0.47
Return Label	17/59	(29%)	0.10
None	27/60	(45%)	–
Location Type			
Academic Room	25/58	(43%)	0.35
Common Room	26/60	(43%)	0.36
Hallway	24/59	(41%)	0.23
Outside	28/60	(47%)	0.58
Parking Lot	32/60	(53%)	–
Location Geography			
North	49/100	(49%)	0.26
South	46/97	(47%)	0.36
Main	40/100	(40%)	–
Time of Day			
Morning	71/149	(48%)	0.52
Afternoon	64/148	(43%)	–
Day of Week			
Tuesday	58/147	(39%)	0.05
Tuesday (no Return Label)	41/88	(47%)	0.57
Monday	77/150	(51%)	–

TABLE I: **Flash Drive Open Data**—We show the number of flash drives whose files were opened, divided among a number of different categories that we believed could affect the attack's effectiveness. We are unable to significantly improve our success rate, and can only decrease it by including drives that contain return labels.[5]

label contained a file labeled as the owner's résumé, which would be a logical place to find the owner's contact information. However, as shown in Table II, nearly half of the users first opened one of the winter break photos, which wouldn't reasonably help locate the owner. We suspect that participants who pick up the drive do so with altruistic intentions, but their curiosity surpasses their altruism.

C. Lag Time

We measured the time differences between when the flash drive was dropped, when it was found missing, and when a file was opened on the drive. We find that 87.5% of drives were picked up before the next drop round and all of the drives were taken were missing by the 8th round of checks.[6]

Drives were plugged into a computer in a median 6.9 hours (average, 38.5 hours), as depicted in Figure 3.[7] The drives that we dropped in the afternoon were connected significantly faster (two-sample Kolmogorov-Smirnov test, $p = 0.017$). However, in both cases, the attack is effective and users pick up the drives quickly.

[6]This excludes one drive we found moved, four drives we found unchanged, one drive that was given a status of "other", and one drive whose status was not updated.

[7]During this analysis, we noticed two inconsistencies. In the first, one drive was connected before it was recorded as being dropped. In the second, the drive was marked missing significantly after a file had been opened on it. Both of these were due to recording error and we do not believe they significantly affect our analysis.

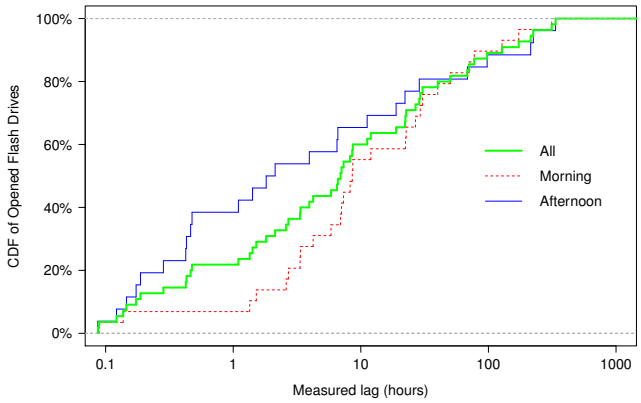


Fig. 3: **Empirical CDF of Measured Lag**—We show the empirical cumulative distribution function for the time difference between when a drive was dropped and when a file was opened on that drive. Afternoon drives were picked up more quickly than morning ones, but both were generally picked up quickly.

D. Browser and Operating System

We find no significant difference between the web browsers used by the users that picked up drives and the statistics published by W3Counter [48] for the general population (Table IV).[8] We do however find a higher proportion of Mac ($p = 0.0022$) and lower proportion of Windows users ($p = 0.026$), as shown in Table III.

E. Comparison to Previous Studies

The file open fraction we observe in this study is less than the open fraction found in three prior anecdotes [30], [43], [52] (75%, 59%, 68% and $p = 0.020, 0.085, 0.005$, respectively). It does not significantly differ from Jacobs [21] (37%, $p = 0.268$), but is significantly greater than CompTIA (17%, $p = 9.8 \times 10^{-11}$). We suspect that demographic differences are partially responsible for this discrepancy.

F. Summary

We find the attack is both effective with 45%–98% of drives plugged into participants' computers and timely with a median 6.9 hours for a drive to be connected. It is not clear whether users are acting altruistically: while users are less likely to plug in drives with a return label, users frequently open vacation pictures prior to the résumé on the drive, which would more likely contain contact information. We suspect that users are initially acting altruistically, but their curiosity eclipses their altruism as they try to find contact information. We further explore reported motivations in the next section.

V. Survey Results

When users opened a file on the flash drive, we offered $10 in compensation for answering a short survey. We received

[8]The W3Counter survey data was normalized to remove Android and Apple iOS users.

File Name	Frequency	
Confidential	13/58	(22%)
`2015_proj1/feb12proposalA.pptx`	4/13	(31%)
`2015_proj1/patent_app_0217.pdf`	3/13	(23%)
`employee/termination_notice_*.pdf`	3/13	(23%)
`strategy/plan_for_2015_2016.pptx`	2/13	(15%)
`strategy/0425_meeting_notes.pdf`	1/13	(8%)
Exams	12/58	(21%)
`sp15/examA.pdf`	6/12	(50%)
`fa10/examA.pdf`	3/12	(25%)
`fa10/solutionsA.pdf`	1/12	(8%)
`fa13/examB.pdf`	1/12	(8%)
`sp10/examA.pdf`	1/12	(8%)
Keys	11/58	(19%)
`Pictures/Winter Break/*.jpg`	5/11	(45%)
`Documents/resume.pdf`	4/11	(36%)
`Documents/reflective_essay_02.docx`	2/11	(18%)
Return Label	7/58	(12%)
`Pictures/Winter Break/*.jpg`	3/7	(43%)
`Documents/resume.pdf`	2/7	(29%)
`Math Notes/2-13.docx`	1/7	(14%)
No file recorded	1/7	(14%)
None	15/58	(26%)
`Documents/resume.pdf`	8/15	(53%)
`Pictures/Winter Break/*.jpg`	5/15	(33%)
`Math Notes/2-13.docx`	1/15	(7%)
No file recorded	1/15	(7%)

TABLE II: **File Operations**—We include matching files on each type of USB drive. However, each file is an HTML with an embedded image that allows us to track when users open files. We find that participants displayed evidence consistent with both altruistic motivations (`resume.pdf.html`) and self-interest (winter break pictures).

Operating System	Flash Drive		W3Counter	p
Linux	4/58	(7%)	3%	0.26
Mac	16/58	(28%)	8%	0.0022
Windows	36/58	(62%)	79%	0.026
None	2/58	(3%)	–	–

TABLE III: **OS Data**—We collect browser information from consenting participants using their user-agent strings. P-values are computed using Fisher's Exact Test. Our sample contains a smaller portion of Windows machines and a larger proportion of Macs than a general Internet population.

Browser	Flash Drive		W3Counter	p
Chrome	26/58	(45%)	43%	0.87
Firefox	12/58	(21%)	15%	0.39
IE	8/58	(14%)	17%	0.66
Other	6/58	(10%)	–	–
Safari	4/58	(7%)	15%	0.20
None	2/58	(3%)	–	–
Opera	0/58	(0%)	3%	0.30

TABLE IV: **Browser Data**—We collect browser information from consenting participants using their user-agent strings. P-values are computed using Fisher's Exact Test. Our sample's browser population does not significantly differ from a general Internet population.

Code	Respondents	
Return drive	42	(68%)
Curious	11	(18%)
Listed location as response	5	(8%)
Keep drive	2	(3%)
Given drive by someone else	2	(3%)

TABLE V: **Participant Motivation**—We show the primary reasons given as responses to the question "Why did you pick up the flash drive and insert it into your computer?". Most respondents expressed a desire to return the flash drive, although many respondents also expressed curiosity.

Code	Respondents	
Specific Precautions		
Scanned files with anti-virus	10	(16%)
Mentioned OS security features	5	(8%)
Sacrificed a computer	5	(8%)
Opened a file in a text editor	4	(6%)
Sandboxed a file	3	(5%)
Contacted/Web searched researcher	2	(3%)
Specific Words		
No	42	(68%)
Yes	8	(13%)

TABLE VI: **Participant Precautions**—We show coded responses to the question "Did you take any precautions before opening the file on the flash drive (e.g., scanning it for viruses)?". Most respondents did not take formal protection measures, although those that did employed a variety of methods.

62 valid responses to the survey[9], which we compare to the 31 valid responses[10] collected through our email survey sent to random members of our university community (our baseline).

A. Motivation

We asked users why they picked up and connected the flash drive, as well as whether the drive's appearance affected their decision. We analyzed the responses by developing a code book for each question and having two researchers independently analyze the responses.[11] As shown in Figure V, the majority of respondents answered that they wanted to return the drive (68%) or expressed curiosity (18%).

Several users indicated that the attached keys encouraged them to find the owner, e.g., "It placed more urgency to return it to its owner. Someone could be locked out of their apartment/house or something, so I would rather return it faster." A smaller number mentioned curiosity, which appears

[9]We received 80 raw responses, but discarded 18: 6 incomplete, 1 from an underage participant, 1 from a participant who had prior knowledge of the experiment, and 1 user who submitted the survey 11 times (we discarded the 10 subsequent submissions). We received four more responses than consents. However, we did not discard the responses because it was not immediately clear that the responses were cases of abuse.

[10]We received 43 raw responses, but discarded 12: 7 incomplete and 5 from participants who failed more than one attention-check question.

[11]Cohen's kappa [24] for these questions ranged from 0.50 (moderate) to 0.92 (almost perfect).

to dominate any sense of suspicion: "I was wondering why a jpeg picture had an html address". In two cases, participants admitted picking up the drive because they personally needed a flash drive. However, it is important to note that users were likely inclined to over-report altruistic tendencies and under-report self-interested ones.

B. Precautions

The majority of respondents (68%) explicitly stated that they did not take any precautions for plugging in the drive or opening any of the files. For those who did take precautions, 10 mentioned scanning the files with anti-virus software, 5 believed their operating system would protect them, 5 sacrificed a computer, and 9 mentioned another form of protection (Table VI).

During this process we also noted the following trends:

- Users underestimate the risk of visiting malicious websites. Several even perceived the files on the flash drive as being safer because of the `.html` extension.
- Users intentionally use institutional resources for unsafe activity to avoid infecting their personal computers. For example, when questioned over safety concerns, one respondent answered "I sacrificed a university computer."
- Users trust their OS and security software to protect them, e.g., "I trust my macbook to be a good defense against viruses".
- A few users took reasonable precautions, including opening the HTML file in a text editor and connecting the drive to an offline computer.

C. Demographics

We asked participants standard SurveyMonkey demographic questions as well as the respondent's university affiliation. Of the 62 responses to the USB survey, 41 identified as undergraduate students, 13 as graduate students, and 7 as staff, which does not differ from the school's population [46] (test of equal proportions, Fisher's Exact Test); however we note that no respondents were faculty members.

Participants identified as 65% male and 35% female, which is not significantly different than the general University population (55% male, 45% female) [11]. This result is consistent with prior work that found that gender does not affect infection risk [2], [27], [32]. However, this is also simultaneously inconsistent with results that showed that women are more likely to fall for targeted phishing attacks [22] and men are more likely to adopt both adaptive and risky online behaviors [31]. We find no significant demographic differences between the emailed campus survey (baseline) and Illinois' published statistics, which suggests that the baseline survey was not skewed towards any particular demographic (Table VII).

D. Risk Attitude

We asked participants to complete the risk taking portion of the English DOSPERT questionnaire to measure risk attitudes.

[12]We excluded the seven staff in our study from this comparison and compared statistics for the student populations.

Category	Flash Drive		University	p
Age[12]				
18-20	20/55	(36%)	38%	0.90
21-29	32/55	(58%)	55%	0.75
30-39	1/55	(2%)	6%	0.37*
40+	2/55	(4%)	1%	0.12*
Affiliation				
Undergraduate	41/62	(66%)	59%	0.34
Graduate	13/62	(21%)	20%	0.99
Staff	7/62	(11%)	15%	0.50
Faculty	0/62	(0%)	5%	0.08*
Prefer not to answer	1/62	2%	–	–

TABLE VII: **Demographics** — We collect demographic information about participants who plugged in the flash drives and find that they do not significantly differ from the University population.
* Comparison performed using Fisher's Exact Test instead of the test of equal proportions.

We compared these values to the general population in the original study [4], along with a sample of the University of Illinois population using the Welch two-sample unpaired t-test.[13]

Our email survey found that the University of Illinois population is more risk averse than the general population measured by Blais and Weber in every domain. The users that connected a USB drive are more willing to take more risk in the health/safety, recreational, and social domains (Table VIII) than the University of Illinois population; their appetite for recreational risk was even greater than the (demographically-"riskier") Blais and Weber population. This suggests that recreational risk taking can be used to detect susceptibility to this class of attack.

E. Computer and Security Knowledge

We asked participants if they had "installed or re-installed an operating system on a computer", "configured a home network", or "created a web page" — three questions from Lévesque et al. [27] — to measure general computer expertise. We find that there is no significant difference between the users who plug in a flash drive and the general population (18/62 = 29% vs 9/50 = 18%, test of equal proportions, $p = 0.25$).

We also included questions from Egelman and Peer's Security Behavior Intentions Scale (SeBIS) [12], a set of questions that measure how well end users follow well known security advice. We show the SeBIS items with $p < 0.1$ in

[13]We generated and compared normally-distributed data with the given statistics using R's `mvrnorm` function given that Blais and Weber only reported summary statistics for their study. Cronbach's alpha [10], a measure of a scale's internal consistency, was generally less in our study (0.57 in the USB survey and 0.62 in the emailed surveys vs. 0.75 in Blais and Weber for ethical, 0.67 vs. 0.84 vs. 0.83 for financial, 0.65 vs. 0.65 vs. 0.71 for health/safety, 0.87 vs. 0.66 vs. 0.86 for recreational, and 0.54 vs. 0.74 vs. 0.79 for social). We note that many of these subscale values are below the 0.70 cutoff given by Nunnally and Bernstein [34].

Risk Domain	Blais and Weber μ	Blais and Weber σ	USB μ	USB σ	t	df	p
Ethical	17.97	7.16	12.82	4.96	6.02	138.29	1.48E-08
Financial	20.67	8.51	15.32	5.22	0.67	157.94	7.43E-08
Health/Safety	21.80	7.84	19.11	7.02	2.44	105.90	1.65E-02
Recreational	23.01	9.40	25.56	10.07	-1.69	90.54	9.54E-02
Social	32.42	6.44	29.77	5.62	2.97	108.63	3.67E-03
Risk Domain	School μ	School σ	USB μ	USB σ	t	df	p
Ethical	11.97	4.15	12.82	4.96	-0.85	66.05	4.00E-01
Financial	13.90	6.15	15.32	5.22	-1.06	48.97	2.93E-01
Health/Safety	16.14	6.28	19.11	7.02	-1.99	62.31	5.11E-02
Recreational	18.21	6.44	25.56	10.07	-4.11	79.49	9.70E-05
Social	27.34	6.61	29.77	5.62	-1.69	49.07	9.71E-02

TABLE VIII: **DOSPERT Results**—We compare the responses to the DOSPERT in both Blais and Weber's paper [4] and our study. Greater numbers indicate a greater willingness to try risky behaviors. College students as a whole tolerate far less ethical and financial risk, but greater levels of recreational risk-taking are associated with compromise via USB; this subscale could be used to identify at-risk populations.

Table XI; the full results can be found in Appendix B.[14] We find that USB survey participants differ from the Amazon Mechanical Turk population in Egelman and Peer [12] in most items but only differ from the Illinois baseline for two items involving computer locking and applying manual updates.

These results suggest that the users who picked up flash drives had similar security behaviors to their peers and that the attack is effective against the University of Illinois population, rather than a non-technically-oriented subgroup.

F. Summary

Our survey results suggest that altruism and curiosity motivated users to pick up and connect the USB drives they found. Those users had security hygiene that was not noticeably different than their peers, but tolerated more recreational risk than both their peers and the general adult population. We believe that participants' risk-averseness compared to the general population and typically-equivalent security knowledge compared to their peers suggests that the attack would be effective against most users. That said, participants could be less willing to take risks and/or more willing to report security behaviors after they were explicitly told that they had fallen victim to an attack.

VI. Returns and Reactions

In this section, we describe the users who returned drives to us, users who contacted the email addresses on the drives with return labels, and the social media response to the experiment.

[14]We generated normally-distributed data using `mvrnorm` in order to compare with Egelman and Peer using their summary statistics. The USB survey was less reliable in the device securement (Cronbach's alpha of 0.732 in the USB survey vs. 0.759 in the emailed survey vs. 0.764 in Egelman and Peer [12]), password generation (0.497 vs. 0.598 vs. 0.728), and updating (0.520 vs. 0.683 vs. 0.719) subscales. The USB survey was more reliable in the proactive awareness (0.691 vs. 0.589 vs. 0.668) subscale and overall (0.802 vs. 0.699 vs. 0.801). We note that the password generation and updating scores violate McKinley et al.'s [29] criterion as given in Egelman and Peer [12]: "a multicomponent scale is reliable if $\alpha > 0.6$ for all sub-scales and $\alpha > 0.7$ for a majority of sub-scales."

[15]Items denoted with ^{r} are reverse-scored and recoded.

A. Drive Returns

Despite instructing users that they could keep the flash drives they found, 54 (18%) of participants returned the drive to us (Table X). Of those, 36 (67%) of the drives were never connected to a computer. A significant fraction (17/54 = 32%) of the returned drives had keys attached. 11 of the remaining drives had return address labels, 9 of which had not been plugged into a computer. Most of the users who returned drives to us were administrative personnel that acted as the lost and found contact for their department (59%) or IT staff (33%).

B. Received Email

The drives with return labels contained ten fictitious names; half of the names were women's, half were men's. These names were generated from the 100 most popular first and last names from the state and U.S. censuses in 1993 and 2000, respectively [42], [45]. We then generated unique Gmail accounts of the form `first.last.N@gmail.com`, where n represents a four-digit random number, and we wrote each corresponding name and email on six drives.

On average, each recipient received 4.8 emails from 4.4 senders (out of a total of six drives each) after a week, all of which stated that they drive had been found. There was no significant difference between male and female names.

C. Social Media Response

During the experiment, we monitored social media sites (e.g., Facebook and Reddit) for any descriptions of the experiment. At 11 am on the second day, a student posted a picture of one of the flash drives with attached keys to Facebook. Later that day, at 1 pm, a user posted on the university sub-Reddit about finding multiple drives on campus and stated that they reported the incident to an IT group. Commenters confirmed the presence (and non-maliciousness) of the flash drives and speculated about the purpose of the study. Two users warned

[16]We used the test of equal proportions.

Question[15]	Egelman and Peer μ	Egelman and Peer σ	USB μ	USB σ	t	df	p
I set my computer screen to automatically lock if I don't use it for a prolonged period of time.	3.20	1.559	3.95	1.419	-3.790	75.510	2.98E-04
I use a password/passcode to unlock my laptop or tablet.	3.78	1.525	4.19	1.420	-2.060	74.700	4.26E-02
I manually lock my computer screen when I step away from it.	2.63	1.343	3.32	1.514	-3.360	69.210	1.27E-03
I use a PIN or passcode to unlock my mobile phone.	3.21	1.733	3.75	1.677	-2.310	73.400	2.36E-02
I do not change my passwords, unless I have to^r.	2.65	1.091	1.88	1.001	5.520	75.210	4.59E-07
I use different passwords for different accounts that I have.	3.75	1.037	3.19	1.152	3.590	69.550	6.11E-04
I do not include special characters in my password if it's not required^r.	3.30	1.292	2.85	1.472	2.260	68.960	2.69E-02
When someone sends me a link, I open it without first verifying where it goes^r.	4.01	1.014	2.95	1.209	6.470	67.970	1.24E-08
I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon)^r.	3.69	1.102	3.31	1.149	2.440	71.190	1.70E-02
When browsing websites, I mouseover links to see where they go, before clicking them.	3.69	1.027	3.25	1.359	2.380	66.040	2.00E-02
If I discover a security problem, I continue what I was doing because I assume someone else will fix it^r.	4.08	0.976	3.71	1.115	2.430	68.900	1.78E-02
When I'm prompted about a software update, I install it right away.	3.07	1.035	2.81	1.008	1.840	73.190	6.94E-02
I try to make sure that the programs I use are up-to-date.	3.78	0.890	3.53	0.935	1.990	70.970	5.07E-02
Question	School μ	School σ	USB μ	USB σ	t	df	p
I set my computer screen to automatically lock if I don't use it for a prolonged period of time.	3.36	1.471	3.95	1.419	1.770	51.450	8.21E-02
When I'm prompted about a software update, I install it right away.	3.36	1.026	2.81	1.008	-2.320	52.290	2.42E-02

TABLE IX: **SeBIS Results**—We compare items with different ($p < 0.1$) responses to items in the SeBIS in both Egelman and Peer's study [12] and the USB experiment and between the school survey and the USB experiment. College students appear to have different security knowledge profiles than a general population.

Drive Type	Opened		p	Returned		p[16]
Confidential	29/58	(50%)	0.72	8/58	(14%)	0.73
Exams	29/60	(48%)	0.71	11/60	(18%)	0.30
Keys	29/60	(48%)	0.47	17/60	(28%)	0.02
Return Label	14/59	(24%)	0.10	11/59	(19%)	0.28
None	27/60	(45%)	–	6/60	(10%)	–

TABLE X: **Returned Drive Data**—We compare the fractions of drives returned to us by type versus our unlabeled control. We also include drive opens by type for reference. Keys drives were returned more frequently than our unlabeled control.

readers to avoid plugging the devices into their computers. The next day, a purported IT worker posted about the "Final Exam Answers" and encouraged users not to plug in the drives.

We note that while news of the experiment spread quickly and despite IT workers recommending against connecting the drives, the attack was still largely successful.

D. Altruistic Experiences

Twice during the experiment, users returned flash drives to the researchers who were attempting to drop them. We consider these incidents an effective display of altruism that underscores the conclusions of this paper.

VII. Conclusion

In this paper, we showed that the anecdote that users will pick up and plug in flash drives they find is true. In a controlled experiment at the University of Illinois, we find that the attack both effective with an estimated 45%–98% of dropped drives connected and expeditious with the first drive connected in under six minutes.

Users pick up the drives with altruistic intentions based on the types of the drives that were connected, the files that were opened, and the number of unconnected drives that were returned to us. However, we simultaneously note that nearly half of users are overtaken by curiosity, first opening vacation photos instead of the prominently placed résumé (which would have reasonably included contact information). Contrary to previous belief, intriguing drive labels do not increase the attack's success rate, but we do find that by attaching keys to the drive, more users return the drives and that by providing a return label, users contact the owner directly instead of connecting it.

The users who connect the drives do not belong to a unique subpopulation—they are neither technically incompetent relative to their peers nor particularly risk loving compared to the general population. Surprisingly, they are more risk averse than the general population in all but one DOSPERT category—recreational risk. Instead, we find that many of the users believe their computers will protect them and they are either not aware of or are more tolerant of the *actual* risks of plugging in a USB drive.

This evidence is a reminder to the security community that less technical attacks remain a real-world threat and that we have yet to understand how to successfully defend against them. We need to better understand the dynamics of social engineering attacks, develop better technical defenses against them, and learn how to effectively teach end users about these risks.

Acknowledgements

The authors thank the University of Illinois Technology Services, especially Wayland Morgan, as well as the members of the University of Illinois Police Department and the Office of

University Counsel, who were all fundamental in executing the study at Illinois. We thank Troy Chmieleski for his contributions towards building the experiment infrastrcture, as well as Brian Meier, David Wang, Katie Sreenan, Lawrence Humphrey, and Yoojin Hong for assisting in dropping the drives. Finally, we thank Serge Egelman, Alex Halderman, Iulia Ion, and Vern Paxson.

This work is supported by the National Science Foundation under grants CNS 1518888, CNS 1409758, CNS 1111699, CNS 1518741, and by a Google Ph.D. Fellowship in Computer Security.

REFERENCES

[1] M. Al-Zarouni. The reality of risks from consented use of USB devices. In *Proceedings of the 4th Australian Information Security Conference*. School of Computer and Information Science, Edith Cowan University, Perth, Western Australia, 2006.

[2] Z. Benenson, A. Girard, N. Hintz, and A. Luder. Susceptibility to URL-based Internet attacks: Facebook vs. email. In *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2014 IEEE International Conference on*, pages 604–609. IEEE, Mar. 2014.

[3] Binamuse Inc. Sketchup BMP Material RLE4 Heap Overflow, 2013. http://www.binamuse.com/advisories/BINA-20130521B.txt.

[4] A.-R. Blais and E. U. Weber. A domain-specific risk-taking (DOSPERT) scale for adult populations. *Judgment and Decision Making*, 1(1), 2006.

[5] A. M. Bossler and T. J. Holt. On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, 3(1):400–420, 2009.

[6] D. Canali, L. Bilge, and D. Balzarotti. On the Effectiveness of Risk Prediction Based on Users Browsing Behavior. In *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security*, ASIA CCS '14, pages 171–182, New York, NY, USA, 2014. ACM.

[7] E. Chin, A. P. Felt, V. Sekar, and D. Wagner. Measuring User Confidence in Smartphone Security and Privacy. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, New York, NY, USA, 2012. ACM.

[8] N. Christin, S. Egelman, T. Vidas, and J. Grossklags. It's All about the Benjamins: An Empirical Study on Incentivizing Users to Ignore Security Advice. In *Financial Cryptography and Data Security*, volume 7035 of *Lecture Notes in Computer Science*, pages 16–30. Springer Berlin Heidelberg, 2012.

[9] White paper: Cyber secure: A look at employee cybersecurity habits in the workplace. Technical report, CompTIA, 2015.

[10] L. Cronbach. Coefficient alpha and the internal structure of tests. *Psychometrika*, 16(3):297–334, Sept. 1951.

[11] Division of Management Information. On-campus fall 2014 statistical abstract of ten-day enrollment, 2014. http://www.dmi.illinois.edu/stuenr/abstracts/fa14_ten.htm.

[12] S. Egelman and E. Peer. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). In *SIGCHI Conference on Human Factors in Computing Systems (CHI '15)*. ACM, 2015.

[13] A. P. Felt, S. Egelman, and D. Wagner. I've Got 99 Problems, but Vibration Ain't One: A Survey of Smartphone Users' Concerns. In *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, SPSM '12, pages 33–44, New York, NY, USA, 2012. ACM.

[14] S. Flinn and J. Lumsden. User Perceptions of Privacy and Security on the Web. In *Proceedings of 3rd Annual Conference on Privacy, Security and Trust (PST)*, pages 15–26, 2005.

[15] G. B. Forbes, TeVault, and H. F. Gromoll. Regional differences in willingness to help strangers: A field experiment with a new unobtrusive measure. *Social Science Research*, 1(4):415–419, Dec. 1972.

[16] B. Friedman, D. Hurley, D. C. Howe, E. Felten, and H. Nissenbaum. Users' Conceptions of Web Security: A Comparative Study. In *CHI '02 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '02, pages 746–747, New York, NY, USA, 2002. ACM.

[17] L. Gauthier. How Question Bank Was Built, 2011. https://www.surveymonkey.com/blog/en/blog/2011/07/27/how-question-bank-was-built/.

[18] F. L. Greitzer, J. R. Strozer, S. Cohen, A. P. Moore, D. Mundie, and J. Cowley. Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits. In *Security and Privacy Workshops (SPW), 2014 IEEE*, pages 236–250. IEEE, May 2014.

[19] C. Hadnagy. *Social engineering: The art of human hacking*. John Wiley & Sons, 2010.

[20] T. Hudson. Thunderstrike, 2014. https://trmm.net/Thunderstrike.

[21] J. R. Jacobs. Measuring the effectiveness of the USB flash drive as a vector for social engineering attacks on commercial and residential computer systems. Master's thesis, Embry-Riddle Aeronautical University, 2011.

[22] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer. Social Phishing. *Commun. ACM*, 50(10):94–100, Oct. 2007.

[23] L. Koved, S. Trewin, C. Swart, K. Singh, P.-C. Cheng, and S. Chari. Perceived security risks in mobile interaction. In *Symposium on Usable Privacy and Security (SOUPS)*, 2013.

[24] J. R. Landis and G. G. Koch. The measurement of observer agreement for categorical data. *Biometrics*, 33(1):159–174, Mar. 1977.

[25] J. Larimer. USB autorun attacks against linux. In *Hackito Ergo Sum 2011*, 2011.

[26] E. Lastdrager, L. Montoya, P. Hartel, and M. Junger. Applying the Lost-Letter Technique to Assess IT Risk Behaviour. In *Socio-Technical Aspects in Security and Trust (STAST), 2013 Third Workshop on*, pages 2–9. IEEE, June 2013.

[27] F. L. Levesque, J. Nsiempba, J. M. Fernandez, S. Chiasson, and A. Somayaji. A Clinical Study of Risk Factors Related to Malware Infections. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, CCS '13, pages 97–108, New York, NY, USA, 2013. ACM.

[28] G. Maier, A. Feldmann, V. Paxson, R. Sommer, and M. Vallentin. An Assessment of Overt Malicious Activity Manifest in Residential Networks. In *Detection of Intrusions and Malware, and Vulnerability Assessment*, volume 6739 of *Lecture Notes in Computer Science*, pages 144–163. Springer Berlin Heidelberg, 2011.

[29] R. K. McKinley, T. Manku-Scott, A. M. Hastings, D. P. French, and R. Baker. Reliability and validity of a new measure of patient satisfaction with out of hours primary medical care in the United Kingdom: development of a patient questionnaire. *BMJ (Clinical research ed.)*, 314(7075):193–198, Jan. 1997.

[30] M. McQueen. Software and human vulnerabilities. In *ARC World Industry Forum 2010*, Feb. 2010.

[31] G. R. Milne, L. I. Labrecque, and C. Cromer. Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices. *Journal of Consumer Affairs*, 43(3):449–473, Sept. 2009.

[32] F. T. Ngo and R. Paternoster. Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, 5(1):773–793, 2011.

[33] K. Nohl, S. Krissler, and J. Lell. BadUSB–on accessories that turn evil. In *Black Hat USA*, 2014.

[34] J. Nunally and I. Bernstein. *Psychometric theory, 3rd edition*. McGraw-Hill, 1994.

[35] K. Onarlioglu, U. O. Yilmaz, E. Kirda, and D. Balzarotti. Insights into User Behavior in Dealing with Internet Attacks. In *Network and Distributed Systems Security Symposium (NDSS)*, Feb. 2012.

[36] C. Paoli. Microsoft releases security update for autorun vulnerability, 2011. https://redmondmag.com/articles/2011/02/10/update-for-autorun-vulnerability.aspx.

[37] D. V. Pham, A. Syed, A. Mohammad, and M. N. Halgamuge. Threat analysis of portable hack tools from USB storage devices and protection solutions. In *Information and Emerging Technologies (ICIET), 2010 International Conference on*, pages 1–5. IEEE, June 2010.

[38] H.-S. Rhee, C. Kim, and Y. U. Ryu. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, 28(8):816–826, Nov. 2009.

[39] Security Research Labs. Turning USB peripherals into BadUSB. Technical report, 2014.

[40] R. Sevinsky. Funderbolt: Adventures in thunderbolt DMA attacks. In *Black Hat USA*, 2013.

[41] R. Shay, I. Ion, R. W. Reeder, and S. Consolvo. "My Religious Aunt Asked Why I Was Trying to Sell Her Viagra": Experiences with Account Hijacking. In *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems*, CHI '14, pages 2657–2666, New York, NY, USA, 2014. ACM.

[42] Social Security Administration. Popular names by state, 2015. http://www.ssa.gov/cgi-bin/namesbystate.cgi.

[43] S. Stasiukonis. Social engineering, the USB way, 2006. http://www.darkreading.com/attacks-breaches/social-engineering-the-usb-way/d/d-id/1128081?

[44] SurveyMonkey, 2015. https://www.surveymonkey.com/.

[45] United States Census Bureau. Frequently occurring surnames from the census 2000, 2014. http://www.census.gov/topics/population/genealogy/data/2000_surnames.html.

[46] University of Illinois, Urbana-Champaign. Illinois facts, 2015. http://illinois.edu/about/facts.html.

[47] A. Vance, B. B. Anderson, C. B. Kirwan, and D. Eargle. Using Measures of Risk Perception to Predict Information Security Behavior: Insights from Electroencephalography (EEG). *Journal of the Association for Information Systems*, 15(10), 2014.

[48] W3Counter. February 2015 market share. Technical report, Feb. 2015. http://www.w3counter.com/globalstats.php?year=2015&month=02.

[49] D. Wagenaar, D. Pavlov, and S. Yannick. USB baiting. *Universite van Amserdam*, 2011.

[50] E. U. Weber, A.-R. Blais, and N. E. Betz. A domain-specific risk-attitude scale: measuring risk perceptions and risk behaviors. *J. Behav. Decis. Making*, 15(4):263–290, Oct. 2002.

[51] A. Welsh and J. A. Lavoie. Risky eBusiness: An examination of risk-taking, online disclosiveness, and cyberstalking victimization. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 2012.

[52] S. Wright. Honey stick project - phase 1 results. Technical report, Streetwise Security Zone, 2012. http://www.streetwise-security-zone.com/members/streetwise/adminpages/HSP-Phase1-Results.

[53] S. Wright. Report: The Symantec smartphone honey stick project, 2012.

[54] T. F. Yen, V. Heorhiadi, A. Oprea, M. K. Reiter, and A. Juels. An Epidemiological Study of Malware Encounters in a Large Enterprise. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, pages 1117–1130, New York, NY, USA, 2014. ACM.

[55] K. Zetter. An unprecedented look at Stuxnet, the world's first digital weapon. *Wired*, 2014. http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

APPENDIX A
SURVEY

This is the survey that was asked to respondents who picked up USB flash drives. Items denoted with ^{r} are reverse-scored.

A. SeBIS

[Never (1), Rarely (2), Sometimes (3), Often (4), Always (5), Prefer not to answer]

1) I set my computer screen to automatically lock if I don't use it for a prolonged period of time.
2) I use a password/passcode to unlock my laptop or tablet.
3) I manually lock my computer screen when I step away from it.
4) I use a PIN or passcode to unlock my mobile phone.
5) I do not change my passwords, unless I have to.^{r}
6) Please choose often for this item to show you are paying attention.
7) I use different passwords for different accounts that I have.
8) When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.
9) I do not include special characters in my password if it's not required.^{r}
10) When someone sends me a link, I open it without first verifying where it goes.^{r}
11) I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar.^{r}
12) I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon).^{r}
13) When browsing websites, I mouseover links to see where they go, before clicking them.
14) If I discover a security problem, I continue what I was doing because I assume someone else will fix it.^{r}
15) When I'm prompted about a software update, I install it right away.
16) I try to make sure that the programs I use are up-to-date.
17) Select always as the answer to this question.
18) I verify that my anti-virus software has been regularly updating itself.

B. DOSPERT

For each of the following statements, please indicate the likelihood that you would engage in the described activity or behavior if you were to find yourself in that situation. Provide a rating from Extremely Unlikely to Extremely Likely, using the following scale: [Extremely Unlikely (1), Moderately Unlikely (2), Somewhat Unlikely (3), Not Sure (4), Somewhat Likely (5), Moderately Likely (6), Extremely Likely (7), Prefer not to answer]

1) Admitting that your tastes are different from those of a friend.
2) Going camping in the wilderness.
3) Betting a day's income at the horse races.
4) Investing 10% of your annual income in a moderate growth diversified fund.
5) Select the third bubble from the left for this item.
6) Drinking heavily at a social function.
7) Taking some questionable deductions on your income tax return.
8) Disagreeing with an authority figure on a major issue.
9) Betting a day's income at a high-stake poker game.
10) Having an affair with a married man/woman.
11) If 2+2 = 5, please choose extremely likely. Otherwise, choose extremely unlikely.
12) Passing off somebody else's work as your own.
13) Going down a ski run that is beyond your ability.
14) Investing 5% of your annual income in a very speculative stock.
15) Going whitewater rafting at high water in the spring.
16) Betting a day's income on the outcome of a sporting event.
17) Engaging in unprotected sex.
18) Revealing a friend's secret to someone else.
19) Driving a car without wearing a seat belt.
20) Investing 10% of your annual income in a new business venture.
21) Taking a skydiving class.
22) Purchasing a banana for $1000. Choose extremely unlikely if you wouldn't.
23) Riding a motorcycle without a helmet.
24) Choosing a career that you truly enjoy over a more secure one.
25) Speaking your mind about an unpopular issue in a meeting at work.
26) Select not sure as the answer to this question.

27) Sunbathing without sunscreen.
28) Bungee jumping off a tall bridge.
29) Piloting a small plane.
30) Walking home alone at night in an unsafe area of town.
31) Moving to a city far away from your extended family.
32) Starting a new career in your mid-thirties.
33) Leaving your young children alone at home while running an errand.
34) Not returning a wallet you found that contains $200.

C. USB Questions

1) Why did you pick up the flash drive and insert it into your computer? [Open-ended]
2) Why did you open a file on the flash drive? [Open-ended]
3) Did you happen to notice any of the following things about the flash drive you picked up? [It had a label attached to it, It had items (such as keys) attached to it, Other (please specify), Prefer not to answer]
4) Did any labels attached to the flash drive significantly impact your decision to pick it up and place it into your computer? [Yes, No, I did not notice any labels attached to the flash drive, Prefer not to answer]
5) (If yes to 4) How did any labels attached to the flash drive influence you to pick it up and insert it into your computer? [Open-ended]
6) Did any items (such as keys) attached to the flash drive significantly impact your decision to pick it up and place it into your computer? [Yes, No, I did not notice any items attached to the flash drive, Prefer not to answer]
7) (If yes to 6) How did items (such as keys) attached to the flash drive influence you to pick it up and insert it into your computer? [Open-ended]
8) Did you have any concerns about picking up the flash drive and inserting it into your computer? If so, please explain. [Open-ended]
9) Did you have any concerns about opening the file on the flash drive? [Open-ended]
10) Did you take any precautions before opening the file on the flash drive (e.g., scanning it for viruses)? [Open-ended]
11) Had you heard any information about this research study in the past? [Yes, No, Prefer not to answer]
12) Please select your affiliation with the University, if any. [Faculty, Staff, Graduate Student, Undergraduate Student, No affiliation, Prefer not to answer]

D. Demographics

1) Are you male or female? [Female, Male, Prefer not to answer]
2) What is your age? [17 or younger, 18-20, 21-29, 30-39, 40-49, 50-59, 60 or older, Prefer not to answer]
3) What is the highest level of school you have completed or the highest degree you have received? [Less than high school degree, High school degree or equivalent (e.g., GED), Some college but no degree, Associate degree, Bachelor degree, Graduate degree, Prefer not to answer]
4) Which of the following categories best describes your employment status? [Employed, working full-time; Employed, working part-time; Not employed, looking for work; Not employed, NOT looking for work; Retired; Disabled, not able to work; Prefer not to answer]

E. Other questions

1) On average, how much time did you spend on the Internet per week (e.g., searching for information, checking email, streaming videos)? [Less than 10 hours, More than 10 but less than 30 hours, More than 30 but less than 50 hours, More than 50 but less than 80 hours, More than 80 hours, Prefer not to answer]
2) Select the task(s) that you have previously accomplished; if none of these tasks applies to your situation, then please select “None of the above”: [I have installed or re-installed an operating system on a computer, I have configured a home network, I have created a web page, None of the above, Prefer not to answer]

APPENDIX B
SEBIS ITEM RESULTS

Question	Egelman and Peer μ	Egelman and Peer σ	USB μ	USB σ	t	df	p
I set my computer screen to automatically lock if I don't use it for a prolonged period of time.	3.20	1.559	3.95	1.419	-3.790	75.510	2.98E-04
I use a password/passcode to unlock my laptop or tablet.	3.78	1.525	4.19	1.420	-2.060	74.700	4.26E-02
I manually lock my computer screen when I step away from it.	2.63	1.343	3.32	1.514	-3.360	69.210	1.27E-03
I use a PIN or passcode to unlock my mobile phone.	3.21	1.733	3.75	1.677	-2.310	73.400	2.36E-02
I do not change my passwords, unless I have to.^{r}	2.65	1.091	1.88	1.001	5.520	75.210	4.59E-07
I use different passwords for different accounts that I have.	3.75	1.037	3.19	1.152	3.590	69.550	6.11E-04
When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.	3.31	1.096	3.42	1.192	-0.700	70.070	4.87E-01
I do not include special characters in my password if it's not required.^{r}	3.30	1.292	2.85	1.472	2.260	68.960	2.69E-02
When someone sends me a link, I open it without first verifying where it goes.^{r}	4.01	1.014	2.95	1.209	6.470	67.970	1.24E-08
I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar.^{r}	3.17	1.077	3.05	1.007	0.850	74.550	3.96E-01
I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon).^{r}	3.69	1.102	3.31	1.149	2.440	71.190	1.70E-02
When browsing websites, I mouseover links to see where they go, before clicking them.	3.69	1.027	3.25	1.359	2.380	66.040	2.00E-02
If I discover a security problem, I continue what I was doing because I assume someone else will fix it.^{r}	4.08	0.976	3.71	1.115	2.430	68.900	1.78E-02
When I'm prompted about a software update, I install it right away.	3.07	1.035	2.81	1.008	1.840	73.190	6.94E-02
I try to make sure that the programs I use are up-to-date.	3.78	0.890	3.53	0.935	1.990	70.970	5.07E-02
I verify that my anti-virus software has been regularly updating itself.	3.55	1.228	3.29	1.390	1.380	69.100	1.71E-01

TABLE XI: **SeBIS Results**—We show all responses to items in the SeBIS in both Egelman and Peer's study [12] and the USB experiment. Items denoted with ^{r} are reverse-scored and recoded.