

The Danger of USB Drives

Matthew Tischer | University of Illinois at Urbana-Champaign
Zakir Durumeric | University of Michigan
Elie Bursztein | Google
Michael Bailey | University of Illinois at Urbana-Champaign

This study suggests that average users don't recognize the danger of connecting unknown peripherals to a computer, underscoring the continued risk posed by USB drives. Steps organizations can take to safeguard against USB-based attacks are discussed.

The technical community has long suspected that people will plug in USB flash drives they find on the ground. Unfortunately, whether driven by altruistic motives or human curiosity, doing so unknowingly opens their organization to an internal attack—a true Trojan horse. Our community is filled with anecdotes of these attacks. Pentesters even boast that they can hack humans by crafting labels that pique an individual's curiosity:[1]

> 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 these rumors, there's been no formal analysis of whether such attacks are effective or of what motivates users to connect the drives. In this work, we explore whether USB drives still pose a risk and evaluate the classic anecdote that users will plug in drives they find on the ground.

Our Experiment: An Overview

To measure whether users will connect drives they find on the ground, we conducted a large-scale experiment in which we dropped nearly 300 flash drives around the University of Illinois at Urbana-Champaign campus.[2] In the attack, we replaced expected files on the drive with HTML files that contained an embedded image hosted on a central server, allowing us to track when the drive was connected without automatically executing any code. We found that users picked up 98 percent of the drives, and 45 percent of the drives were connected to a computer. Furthermore, the attack was expeditious, with the first drive being connected within six minutes from when it was dropped. Contrary to popular belief, the appearance of a drive didn't increase the likelihood that someone would connect it to their computer. Instead, users connected all types of drives unless there were other means of locating the owner—indicating that many participants were altruistically

 Copublished by the IEEE Computer and Reliability Societies 1540-7993/17/$33.00 © 2017 IEEE

motivated. However, although users initially connected the drive with altruistic intentions, nearly half were overcome with curiosity, first opening intriguing files—such as vacation photos—before trying to find the drive's owner.

To better understand users' motivations, we offered participants the option to complete a short survey when they connected the drive. Most stated that they connected the drive to locate its owner or out of curiosity, although a handful also admitted that they had planned to keep the drive. The students and staff who connected the drives weren't computer illiterate and weren't significantly different from their peers. When prompted, 68 percent of the participants stated that they took no precautions when connecting the drive. For those who did, 16 percent scanned the drive with their antivirus software and 8 percent believed that their OS or security software would protect them. In the end, all but a handful of the participants who took precautions did so ineffectively, and the majority took no precautions at all.

We submitted and received approval from the University of Illinois Institutional Review Board and met with key stakeholders (IT, legal, and public safety departments) while developing the experiment. We didn't automatically execute any code on participants' systems, and we were only able to collect data if participants double-clicked files on the flash drives. Participants were debriefed and provided with an opportunity to withdraw.

Are USB Drives Still a Threat?

Microsoft Windows no longer automatically executes arbitrary code when a USB drive is connected,[3] which defeats many traditional USB-based attacks.[4,5] However, connecting a USB drive still poses significant risk. There are three broad categories of effective USB attacks: social engineering, spoofing, and zero-day.

The simplest type of attack is social engineering, in which the drive doesn't execute any code on connection but instead tricks the end user into opening a file on the USB drive. The files on the drive can contain a Trojan horse or can simply be HTML content that attempts to phish for credentials. These are the easiest type of attack drives to create for two reasons: an attacker can use store-bought drives, and the attack doesn't rely on finding OS vulnerabilities. However, they're also the least reliable and most conspicuous because they rely on the end user to open files without becoming suspicious. Unfortunately, as we describe below, many users will open the files on a drive without any prompting.

A more complex attack disguises a different type of USB device as a flash drive. While USB drives can no longer automatically execute code, USB human interface devices (HIDs)—such as keyboards and mice—don't require user confirmation. This means that if a USB device identifies itself as a keyboard, it can immediately inject malicious keystrokes that compromise the machine. This attack is more difficult to deploy than a simple social engineering one, because it requires configuring a low-level device to emulate an HID, physically disguising the device as a USB drive, and handling OS variations. However, this has been made considerably easier by the recent availability of Arduino-based microcontrollers that facilitate low-level development. Figure 1 shows a disguised Teensy microcontroller that will open a reverse shell in Windows and Mac OS by "typing" out the requisite BASH or PowerShell commands in the background. Off-the-shelf devices of this type are also available, although they cost significantly more than store-bought USB drives. The bar is still higher than a social engineering attack but can be accomplished easily by a determined hacker.[6]



Figure 1. A normal USB drive and a human interaction device (HID)-based attack drive. Traditional OS defenses can by defeated by having a small microcontroller disguised as a USB drive emulate an HID and inject malicious keystrokes.

The most complex type of USB-based attack is one in which the USB device exploits a known vulnerability in the host OS or hardware. Such "zero-day" attacks are difficult to find and expensive to purchase, and frequently require time-consuming implementation, which makes them unlikely to be used in most settings. However, if an attacker can acquire a zero-day, such an attack is incredibly difficult to protect against: OS policies can be bypassed, and there's little protection that administrators can take beyond disabling USB ports altogether.

Each of the three attacks has its set of advantages and disadvantages. Social engineering attacks are trivial to implement but rely on user curiosity. On the other extreme, zero-day attacks are difficult to acquire but nearly impossible to centrally protect against. HID spoofing devices achieve a reasonable compromise: they can be built using readily available materials and don't require user interaction after the device has been plugged in.

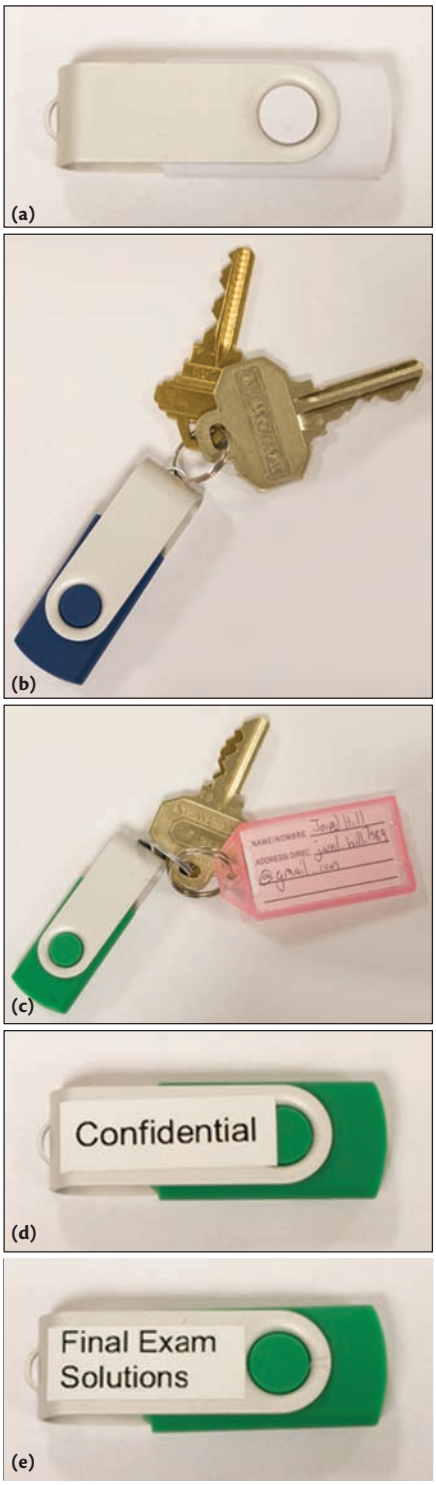

Figure 2. Appearance of study drives. We dropped five different types of drives: (a) an unlabeled control; (b) and (c) two drives to motivate altruism: one with attached keys and one with a return label; and (d) and (e) two drives to motivate self-interest: one marked "confidential" and one marked "final exam solutions."

Do Users Pick Up Drives?

To determine whether users will plug in drives they find on the ground, we dropped nearly 300 drives around the University of Illinois at Urbana-Champaign campus in April 2015, and measured how many were picked up and connected. To safely track when drives were plugged in, we populated each drive with files that were named consistently with the drive's appearance but were HTML files containing an IMG tag referencing our centrally managed server. This methodology was limited because we couldn't detect situations in which users didn't open a file on the drive. However, we believe it provided a safe balance, given that we didn't want to execute code on users' machines.

When dropping the drives, we varied the following factors to see whether they increased the likelihood that a drive would be connected:

- *Drive appearance.* We varied the type of drives dropped at each location to see whether users were motivated by altruism or self-interest. Drives with a return label or with keys attached were engineered to trigger altruistic tendencies; drives with the label "confidential" or "final exam solutions" were intended to trigger selfish tendencies; and drives with no label were our control group. Figure 2 shows an example of each.
- *Geographic location.* We placed flash drives at 30 unique locations on the campus across five location types: parking lots, hallways, academic areas (such as classrooms and libraries), common areas (such as building lobbies and cafeterias), and outside (such as sidewalks).
- *Time of day.* We dropped drives during the morning (6 am to 10 am) and the afternoon (1 pm to 5 pm).

Surprisingly, we found that users opened one or more files on 135 of the 297 flash drives (45 percent), and 290 of the drives (98 percent) were removed from their drop locations. Because we didn't execute any code when a drive was connected, it's not clear whether users plugged in the remaining 155 drives. However, the first two numbers allow us to bound the attack's success rate to between 45 and 98 percent.

Drive Appearance

While drives marked "confidential" or "final exam solutions" or containing keys didn't have a different success rate than unlabeled drives, drives with return labels had a lower success rate. We suspect that this is because altruistic participants were presented with a means of locating the drive owner: the email address on the label.

Some participants explicitly consented to provide us with more detailed data about their usage, including

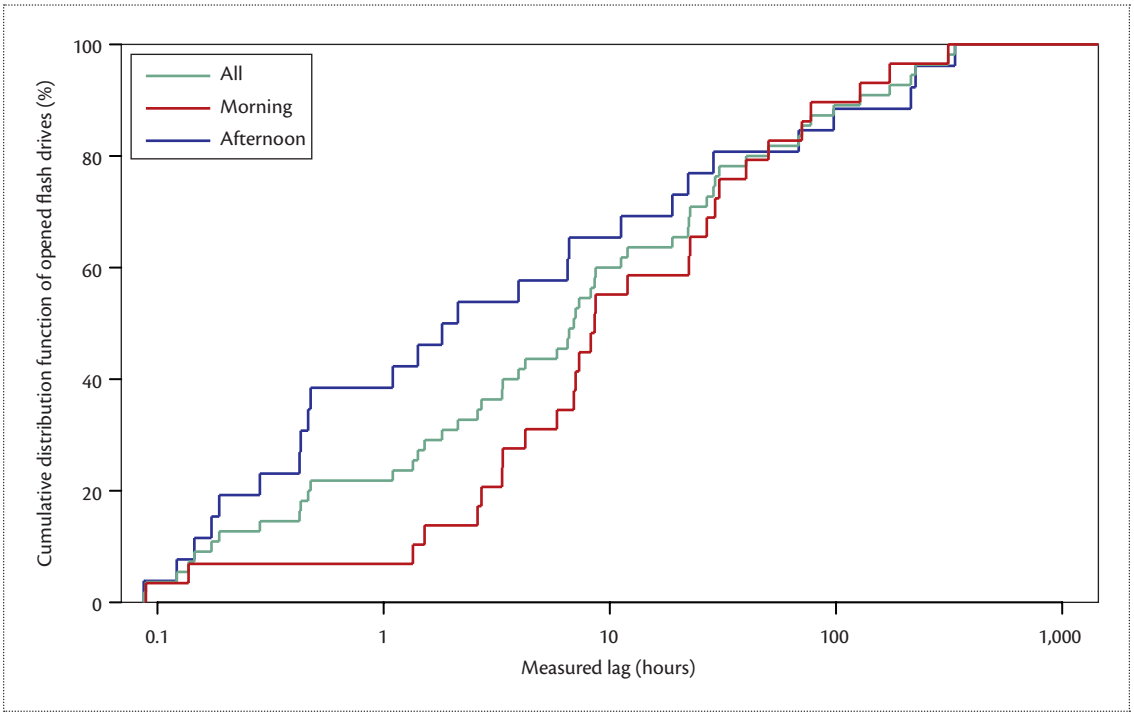

Figure 3. Measured lag time between when we dropped drives and when they were connected to a computer.

what files they opened and when. We investigated what files participants opened first to see if the filenames provided any information about their motivations.

Although the fact that fewer participants connected drives with return labels suggests that they were 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 label contained a file labeled as the owner's resume, which would be a logical place to find the owner's contact information. However, nearly half of the participants who provided data opened one of the vacation photos first, which wouldn't reasonably help locate the owner. We suspect that the participants who picked up drives did so with altruistic intentions, but their curiosity sometimes surpassed their altruism.

Timeliness

We found that 87.5 percent of the drives were picked up by the first time we returned to check on them; that is, the afternoon of the same day for drives dropped in the morning, and the morning of the next day for drives dropped in the afternoon. We also measured the time between when we dropped drives and when they were plugged in. Drives were connected to a computer within a median 6.9 hours, as depicted in Figure 3. The drives that we dropped in the afternoon were connected significantly faster. However, in both cases, the attack was effective and participants picked up the drives quickly. Most impressive, more than 20 percent of the drives were connected within an hour of being dropped. Because an attacker might only need a single connection to stage an attack, this attack could cause harm within a very short period of time.

Why Do Users Plug in Drives?

To understand why participants picked up the drives and the precautions they took, we offered individuals who picked up flash drives the opportunity to complete an anonymous survey by including a link to the survey in the HTML files on the drive. To collect baseline survey values for the University of Illinois, we also emailed 600 random members of the University of Illinois at Urbana-Champaign community in December 2015. We asked users about the following:

- *Demographics*. We asked demographic questions from SurveyMonkey's question bank (including age, sex, and level of education),[7] along with participants' affiliation with the University of Illinois (faculty, staff, or student).
- *Previous knowledge.* We asked whether participants had previously heard about the study. We later discarded responses in which the user had preexisting knowledge.
- *Motivation.* We asked the participants why they picked up the flash drive and whether external appearance or any other factor affected their decision to do so.
- *Computer expertise and behaviors.* We asked questions

Table 1. Participant motivation in picking up a drive.

	Respondents (n = 62)	
Reason	**No.**	**%**
To return drive to owner	42	68
Curiosity	11	18
Listed a location instead of why he or she picked up the drive	5	8
To keep drive	2	3
Was given drive by someone else	2	3

from the Security Behavior Intentions Scale (SeBIS) to measure participants' computer and computer security behaviors[8] as well as three questions from another study to measure their computer expertise.[9]

- *Risk attitude.* We presented questions from the Domain-Specific Risk-Taking (DOSPERT) scale, a standardized survey for measuring how likely a person is to participate in risky behavior.[10]

We received 62 valid responses to the survey, which we compared to the 31 valid responses collected through our email survey sent to random members of the university community.

Motivation

When asked why they plugged in the drive, most responded that they wanted to return the drive (68 percent) or were curious (18 percent). Several participants indicated that the attached keys encouraged them to find the owner; for example: "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 appeared 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's important to note that users were likely inclined to overreport altruistic tendencies and underreport self-interested ones. Table 1 reports these results.

Precautions

The majority of users (68 percent) explicitly stated that they didn't take any precautions when plugging in the drive. For those who did take precautions, 10 scanned the files with antivirus software, five believed that their OS would protect them, five sacrificed a computer, and nine mentioned another form of protection (see Table 2).

We noted the following trends:

- Participants underestimated the risk of visiting malicious websites. Several even perceived the files on the flash drive as being safer because of the .html extension.
- Participants intentionally used 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."
- Participants trusted their OS and security software to protect them; for example: "I trust my MacBook to be a good defense against viruses."
- A few participants took reasonable precautions, including opening the HTML file in a text editor and connecting the drive to an offline computer.

Demographics

Of the 62 responses to the USB survey, 41 identified as undergraduate students, 13 as graduate students, and seven as staff, which doesn't differ from the school's population;[11] however, we note that no respondents were faculty members. Participants identified as 65 percent male and 35 percent female, which isn't significantly different from the general university population. Similarly, the student age distribution didn't significantly differ from that of the larger university population. We found no significant demographic differences between the emailed campus survey (baseline) and the University of Illinois' published statistics, which suggests that the baseline survey wasn't skewed toward any particular demographic.

Risk Attitude

Our survey included questions from the risk-taking portion of the DOSPERT, which measures how likely participants are to participate in risky behaviors across five different domains. We compared responses from the participants who plugged in the found drives with those from the original DOSPERT study[10] and the baseline survey emailed to the University of Illinois sample. The participants who connected a USB drive were more

Table 2. Precautions participants took before connecting a drive.

Precaution	Respondents (n = 62)	
	No.	%
Scanned files with antivirus	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 or searched for a member of the research group to verify that the experiment was legitimate	2	3
The following specific words were used in participants' responses in the shown proportions:		
No	42	68
Yes	8	13

willing to take more risks in the health/safety, recreational, and social domains than the University of Illinois population; their appetite for recreational risk was even greater than the otherwise demographically "riskier" DOSPERT population[10] (see Table 3). This suggests that recreational risk taking can be used to detect susceptibility to flash drive attacks.

Computer and Security Knowledge

To measure general computer expertise, we used three questions from another study, which asked participants whether they'd "installed or re-installed an operating system on a computer," "configured a home network," or "created a webpage."[9] Participants were classified as experts if they answered "yes" to all questions. There was no significant difference in the fraction of experts between our participants (29 percent; 18 out of 62) and those in the other study (18 percent; 9 out of 50).[9]

We also included questions from the SeBIS, which measures how well end users follow well-known security advice, such as "I use different passwords for different accounts that I have," and "If I discover a security problem, I continue what I was doing because I assume someone else will fix it."[8] Our survey participants differed from the Amazon Mechanical Turk population in Egelman and Peer[8] in most items but differed from the University of Illinois group for only two: "I set my computer screen to automatically lock if I don't use it for a prolonged period of time," and "When I'm prompted about a software update, I install it right away." These results suggest that the participants who picked up flash drives had similar security behaviors as their peers and that the attack was effective against the University of Illinois population, rather than a nontechnically oriented subgroup.

Returns and Reactions

We also tracked participants' attempts to return found drives, as detailed below.

Returned Drives

Although we instructed participants that they could keep the flash drives that they found, 54 (18 percent) returned the drives. Of those returned drives, 36 (67 percent) were never connected to a computer. A significant fraction (17 out of 54; 32 percent) of the returned drives had keys attached. Eleven of the remaining drives had return labels; nine of these drives hadn't been plugged into a computer. Most participants who returned drives to us were administrative or IT staff.

Email

The drives with return labels contained 10 fictitious names generated from the 100 most popular names in the 1993 and 2000 US censuses. We then generated unique Gmail accounts of the form first.last.n@gmail.com, where n represented a four-digit random number; we wrote each name and its corresponding email on six drives. On average, each recipient received 4.8 emails from 4.4 senders after a week. There was no significant difference in number of emails and number of unique email addresses for male and female names.

Social Media

We monitored social media sites (Facebook and Reddit) for any descriptions of the experiment. At 11 am on the second day, a student posted a picture to Facebook of one of the flash drives with attached keys. Later that day (at 1 pm), a participant posted on the university sub-Reddit about finding multiple drives

Table 3. Relative risk attitude of participants who picked up drives in our study compared to a University of Illinois baseline sample and the original Domain-Specific Risk-Taking (DOSPERT) study.[10]

Our participants versus ...	Risk attitude				
	Ethical	Financial	Health/safety	Recreational	Social
DOSPERT study	Less	Less	Less	More	Less
University of Illinois	Not significant	Not significant	More	More	More

on campus and stated that they had reported the incident to an IT group. Commenters confirmed the presence (and nonmaliciousness) of the flash drives and speculated about the study's purpose. Two commenters warned readers to avoid plugging the devices into their computers. The next day, a purported IT worker posted about the "final exam answers" and encouraged readers not to plug in the drives. Despite the news of the experiment and IT workers recommending against connecting the drives, the attack was still largely successful.

Altruistic Experiences

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

Recommendations

Organizations can take several steps to protect themselves against this sort of attack.

Educate Users

We found no significant demographic differences between the general population at the University of Illinois and the participants who picked up the flash drives. Participants also had similar risk tolerances and security behaviors. Educational campaigns should include everyone in an organization, not just participants who are stereotypically vulnerable to this type of attack (that is, the less technically skilled). Although we found a potential link between recreational risk tolerance and compromise via USB, we don't suggest relying on this correlation.

Be Vigilant

During the experiment, one of the University of Illinois IT departments was notified by department personnel after they found multiple drives in their building. Similarly, we were contacted by administrative representatives from multiple departments that had eventually collected a significant number of drives that were dropped near them. Our droppers also returned to locations at multiple times of day and participants even noticed them dropping drives; however, participants returned drives to them instead of noticing their suspicious behavior. Organizations should advise employees to notice suspicious behavior and symptoms of an attack and should provide channels for staff to report concerns quickly.

Harden Computing Resources

Whenever participants took precautions, they tended to depend on the computer's existing configuration. Participants mentioned using virus scanners, relying on the OS's security features, and even sacrificing shared computers before mentioning methods like opening the files in a text editor. We recommend hardening machines to reduce the potential consequences of inadvertent user actions.

Have a Plan

Participants plugged in drives quickly; more than 20 percent were plugged in within an hour after being dropped. As such, discovery of an attack might occur soon before (or even after) the organization's compromise. Warnings should be centralized to help ensure that employees receive notice about attacks.

Our study results suggest that such an attack method would be effective against most users and that average individuals don't understand the danger of connecting an unknown peripheral to their computer. When combined with the technical risks associated with connecting a drive, we find that the attack still poses a danger to many organizations. We hope that by bringing these details to light, we remind administrators that sometimes the simplest attacks are the most realistic threats. To address this risk, organizations need to educate users, harden computing resources against USB-based attacks, and prepare a response plan in case of an attack. ■

Acknowledgments

We thank the University of Illinois Technology Services, Police, and Office of University Counsel, who were all fundamental in executing the study. We thank Sam Foster, Sunny Duan, Alec Mori, and Troy Chmieleski for their assistance in designing, executing, and analyzing data in the

original experiment. We thank Brian Meier, David Wang, Katie Sreenan, Lawrence Humphrey, and Yoojin Hong for assisting in dropping the drives. Finally, we thank Serge Egelman, J. Alex Halderman, Iulia Ion, and Vern Paxson. This work is supported by the National Science Foundation under grants CNS 1518888, CNS 1409758, CNS 1111699, and CNS 1518741, and by a Google PhD Fellowship in Computer Security.

References

1. C. Hadnagy, *Social Engineering: The Art of Human Hacking*, John Wiley & Sons, 2010.
2. M. Tischer et al., "Users Really Do Plug in USB Drives They Find," *Proc. IEEE Symp. Security and Privacy* (SP 16), 2016; doi.org/10.1109/SP.2016.26.
3. C. Paoli, "Microsoft Releases Security Update for Autorun Vulnerability," *Redmond*, 10 Feb. 2011; redmondmag.com/articles/2011/02/10/update-for-autorun-vulnerability.aspx.
4. M. Al-Zarouni, "The Reality of Risks from Consented Use of USB Devices," *Proc. 4th Australian Information Security Conf.* (ISM 06), 2006; ro.ecu.edu.au/ism/70.
5. D.V. Pham et al., "Threat Analysis of Portable Hack Tools from USB Storage Devices and Protection Solutions," *Proc. Int'l Conf. Information and Emerging Technologies* (ICIET 10), 2010; doi.org/10.1109/ICIET.2010.5625728.
6. E. Bursztein, "What Are Malicious USB Keys and How to Create a Realistic One?," Elie, Aug. 2016; www.elie.net/blog/security/what-are-malicious-usb-keys-and-how-to-create-a-realistic-one.
7. L. Gauthier, "How Question Bank Was Built," blog, SurveyMonkey, 27 Jul. 2011; www.surveymonkey.com/blog/2011/07/27/how-question-bank-was-built.
8. S. Egelman and E. Peer, "Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS)," *Proc. ACM Conf. Human Factors in Computing Systems* (CHI 15), 2015, pp. 2873–2882.
9. F.L. Levesque et al., "A Clinical Study of Risk Factors Related to Malware Infections," *Proc. ACM SIGSAC Conf. Computer & Communications Security* (CCS 13), 2013, pp. 97–108.
10. A.-R. Blais and E.U. Weber, "A Domain-Specific Risk-Taking (DOSPERT) Scale for Adult Populations," *Judgment and Decision Making*, vol. 1, no. 1, 2006, pp. 33–47.
11. "Illinois Facts," University of Illinois at Urbana-Champaign, 2015; illinois.edu/about/facts.html.

Matthew Tischer is a former graduate student at the University of Illinois at Urbana-Champaign. His research interests include usable security and social engineering. Tischer received an MS in electrical and computer engineering from the University of Illinois at Urbana-Champaign. He's a member of IEEE. Contact him at tischer1@illinois.edu.

Zakir Durumeric is a PhD candidate and Google Research Fellow at the University of Michigan. His research interests include computer security and privacy. Contact him at zakir@umich.edu.

Elie Bursztein leads the antiabuse research team at Google. His research interests include security, privacy, and abuse prevention. Bursztein received a PhD in computer science from the Ecole Normale Superieure de Cachan. Contact him at elieb@google.com.

Michael Bailey is an associate professor at the University of Illinois at Urbana-Champaign. His research interests include the security and availability of complex distributed systems. Bailey received a PhD in computer science from the University of Michigan. He's a Senior Member of IEEE and ACM. Contact him at mdbailey@illinois.edu.



Want to know more about the Internet?

This magazine covers all aspects of Internet computing, from programming and standards to security and networking.

www.computer.org/internet