“My religious aunt asked why I was trying to sell her viagra”: Experiences with account hijacking

Richard Shay
Carnegie Mellon University
Pittsburgh, PA, USA
rshay@cmu.edu

Iulia Ion, Robert W. Reeder, & Sunny Consolvo
Google
Mountain View, CA, USA
{iuliaion, rreeder, sconsolvo}
@google.com

ABSTRACT
With so much of our lives digital, online, and not entirely under our control, we risk losing access to our communications, reputation, and data. Recent years have brought a rash of high-profile account compromises, but account hijacking is not limited to high-profile accounts. In this paper, we report results of a survey about people’s experiences with and attitudes toward account hijacking. The problem is widespread; 30% of our 294 participants had an email or social networking account accessed by an unauthorized party. Five themes emerged from our results: (1) compromised accounts are often valuable to victims, (2) attackers are mostly unknown, but sometimes known, to victims, (3) users acknowledge some responsibility for keeping their accounts secure, (4) users’ understanding of important security measures is incomplete, and (5) harm from account hijacking is concrete *and* emotional. We discuss implications for designing security mechanisms to improve chances for user adoption.

Author Keywords
Security; authentication; online accounts; account hijacking; account compromise; attackers; survey; microsurvey; Mechanical Turk; Google Consumer Survey

ACM Classification Keywords
H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous, K.6.5. Security and protection

INTRODUCTION
“In the space of one hour, my entire digital life was destroyed,” wrote Mat Honan, technology writer and editor for Wired magazine [19]. In his widely read 2012 narrative, Honan describes how he lost access to his Google, Twitter, and AppleID accounts, had a year's worth of photos, documents, and emails deleted, and had racist messages posted to his Twitter feed. Honan was *“mad,” “sad,”* and *“shocked.”* Ultimately, he was able to restore access to his accounts and much of the data that had been lost, though at considerable cost, time, and effort on his part [20]. When one of the attackers contacted him, Honan was able to ask why the attacker had done this damage – it was to access Honan's coveted 3-letter Twitter handle, “mat”; the data destruction was just *“collateral damage.”*

Honan's article is gripping not only as a story about his experiences, but also as a cautionary tale. With so much of our lives now digital, online, and not entirely under our control, we can easily imagine losing access to our communications, reputation, and data, with little recourse. Recent years have brought a rash of other stories of high-profile account hijackings. For example, U.S. Vice Presidential candidate Sarah Palin's email account was compromised in 2008 [7], the personal email account of a Twitter executive's wife was compromised in 2009 [34], the group *Anonymous* broke into accounts of executives at a security firm in 2011 [9], and attackers broke into the Twitter accounts of numerous media outlets, including the Associated Press [29], the Financial Times [26], the Guardian [3], and the Onion [27] in 2013.

Account hijacking is hardly limited to high-profile accounts; anecdotal evidence suggests that it is widespread and can be devastating. In response, service providers continue to improve authentication, compromise detection, and account recovery mechanisms. However, the design space for these systems is vast, and they often require user participation, which is notoriously hard to get for security-related tasks [38]. A better understanding of the hijacking problem – and how to motivate users to take action against it – should help improve the design of such systems.

To gain a better understanding of the hijacking problem from the user's perspective, we surveyed 294 people about their experiences with and attitudes toward email and social network account hijacking. We confirm that the problem is, in fact, widespread; 30% of our 294 participants reported that at least one of their email or social networking accounts had been accessed by an unauthorized party.

We also highlight five themes that emerged from our results:

CHI 2014, April 26–May 01, 2014, Toronto, Canada.
ACM 978-1-4503-2473-1/14/04.
http://dx.doi.org/10.1145/2556288.2557330

(1) **Compromised accounts are often valuable to victims:** In our study, most hijacked accounts were for personal communication and used daily.
(2) **Attackers are unknown *and* known to victims:** Guarding against remote, anonymous attackers is most important, but it would be a mistake to ignore attacks from people close to victims.
(3) **Users acknowledge some responsibility:** Users seem to believe that they share responsibility for keeping their accounts secure.
(4) **Users' understanding of important security measures is incomplete:** Users are aware of malware, phishing, and third-party password database breaches as the most prevalent ways accounts are compromised. However, they emphasize password management measures for preventing account compromise and seem less aware of anti-phishing and anti-malware measures.
(5) **Harm from hijacking is concrete *and* emotional:** Concrete harm is usually minimal, though it can sometimes be severe. Even when it is minimal, users experience strong feelings of anger, fear, and embarrassment about the compromise.

We discuss implications for designing security mechanisms into large, modern Web services in ways that improve chances for users to adopt those mechanisms.

RELATED WORK

Our work fits into the space of research about people's experiences with and attitudes toward online security. In this section, we highlight key related work in that space.

One area of research has focused on models of how people think about security. For example, Camp proposed five mental models that were derived from a review of the literature [11]. Her models – *physical security, medical, criminal, warfare,* and *market* – represent a broad view of how people think about privacy and security and how they frame security decisions. Camp points out that people's understandings tend to rely too strongly on their own past experiences. For example, if a person has previously engaged in a risky computer activity without negative consequences, then that person may underestimate the risk of that activity and continue to engage in it.

Wash provides another view of how people think about computer security based on interviews with 33 people [37]. He identified several "folk models" that describe how people think about malware and attackers (e.g., *"viruses cause mischief," "viruses support crime,"* and *"hackers are criminals who target big fish"*). Similar to Camp, Wash points out how shortcomings in these models can lead people to misidentify threats. For example, those who think attackers would not bother going after them personally might not be aware of the threat posed by botnets.

Other researchers have explored how people make specific security-related decisions. For example, Mazurek et al. interviewed 33 people about how they made data sharing and trust decisions with devices in their homes [23]. The researchers found that interviewees often applied their own understandings of real-world physical security when making access-control decisions.

Another line of research has explored how people react to security incidents or changes in security policies. For example, in a survey of 301 undergraduate students, Rader, Wash, and Brooks investigated how stories that people tell about security incidents that they or others have experienced resonate with people and, in turn, are translated into security-related beliefs [30]. The researchers found that respondents encapsulated and transmitted security lessons in the form of stories and that these stories can affect behavior and understanding. In another example, Shay et al. surveyed 470 people on a university campus that had recently transitioned to a stricter password policy [35]. The researchers found that while respondents tended to be annoyed, they also felt more secure and were neutral about reverting to the previous policy. And finally, Harbach et al. investigated why users were slow to adopt a new German ID system with added security features [18].

This related work suggests that by identifying shortcomings in users' understanding, designers might be able to correct misunderstandings and encourage users to practice better security-related behaviors. The work presented in this paper fits into this space by helping to describe how users experience and perceive account hijacking so that we and others can figure out how to encourage users to make decisions and practice behaviors that help prevent their accounts from being compromised. To the best of our knowledge, this is the first such study on this topic.

METHODOLOGY

In July 2013, we conducted an online survey of people in the U.S. who use a personal email or social networking account at least once per month. In this section, we describe the survey – including supplemental data that we collected from an additional microsurvey, the participants' demographics, and how we analyzed the qualitative data.

The Survey

The online survey had two main branches: one branch was administered to people who had experienced the compromise of a personal email or social networking account (N=89) and the other was administered to people who had not (N=205). We recruited participants from the Amazon Mechanical Turk crowdsourcing service (MTurk). When we recruited, we did not mention that our survey was about account hijacking; rather, our posting proposed, "Answer a survey about your email or social networking account." Participants were assigned to one of the branches based on their response to the question: "As far as you know, has anyone ever broken into any of your personal email or online social networking accounts?" Those who answered "Yes, only once" or "Yes, more than once" continued with the branch for people who had experienced

an account compromise, and those who responded "No" or "I don't know" continued with the other branch. Both branches included open- and close-ended questions.

We collected data over three hours on the evening of Friday, July 26, 2013. Each participant could only take the survey once and received $1 as compensation.

Those who had experienced a compromise (N=89)

Participants who had experienced the compromise of an email or social networking account were asked about their experience (N=89). If participants indicated having experienced more than one such compromise, they were instructed to answer the questions about "the most upsetting" episode. We asked about their account, how the compromise happened, who they thought did it, its consequences, and whose responsibility it was to prevent their accounts from being compromised.

Those who had not experienced a compromise (N=205)

Participants who had not experienced the compromise of an email or social networking account were instructed to think about either their primary personal email (N=111) or social networking (N=94) account throughout the survey. Those having only one or the other were asked about that one; otherwise we asked about one at random. We asked about whom participants were concerned about breaking into their accounts, how they thought accounts were compromised, what they thought an attacker would do if he or she broke into the participants' accounts, and whose responsibility it was to prevent their accounts from being compromised.

Survey Development

To develop the survey, we conducted five semi-structured interviews with a convenience sample of friends and family of our extended research team who had experienced an account compromise. Results from the interviews provided us with insight for creating the survey. After drafting the survey, it was reviewed by experts from our institution, revised, and then piloted with a convenience sample of six people from our institution who were not from our research team. After subsequent improvements, we launched a pilot on MTurk with 20 people. After we made minor adjustments from that pilot, we launched the final survey. We do not report data collected from these pilot studies.

We received 300 completed surveys and discarded six that were duplicates or did not meet our criteria for participation, such as if a participant did not have a personal email or social networking account that was checked at least once per month.

Mechanical Turk as a Recruiting Platform

MTurk, which has been used in prior usable security research (e.g., [6,14]), allowed us to collect data from a large number of diverse participants. MTurk has also been used by Kittur, Chi, and Suh to investigate how well "Turkers" (i.e., the people who complete tasks on MTurk) assessed the quality of Wikipedia articles [21]. The researchers were impressed with how well the Turkers' ratings compared to those of experts. Buhrmester et al. found that the MTurk population was more diverse than that found on a typical college campus and that using MTurk could result in high-quality data [10]. Paolacci et al. conducted a survey on the demographics of U.S. Turkers [28]. They found Turkers to be more female than male, and average 36 years with more education than the general U.S. populace. They also found evidence of MTurk resulting in data comparable in quality to surveying on a university campus.

Mechanical Turk Quality Control

Although MTurk has been shown to be a trustworthy platform for past user studies, it is possible to get low-quality responses. As with any online survey, participants on MTurk can cheat to receive incentives by answering all required questions as quickly as possible and providing junk data in the process. We took three measures to guard against such junk data in our results. First, we required that the Turkers who responded to our survey have a task approval rate of 95% or better, and have completed at least 100 tasks, so we expected to have a relatively high-quality pool of participants. Second, one member of the research team reviewed all responses to the open-ended questions to ensure that responses were on topic and determined that they all were. Finally, we had three trap responses to our multiple-choice questions – responses that were obviously wrong, and we expected no participant who was paying attention would choose. We found that six participants did choose trap responses. However, no participant chose more than one, and those participants did provide valid responses to open-ended questions. Thus, we assume the few trap responses we received were errors due to misreading or misclicking rather than cheating, and we include these participants' data in our analysis.

Confirming the rate of account compromises

We ran a separate one-question survey (or "microsurvey") with a different survey service (Google Consumer Surveys (GCS) [16]), and thus a different population, to confirm our finding about the rate of account compromises. Web users respond to microsurveys from GCS in order to access premium Web content [24,36]. We used GCS's "multiple choice, single answer" microsurvey format to ask, "As far as you know, has anyone ever broken into any of your personal email or online social networking accounts?" (i.e., the same question and set of response options that we used to branch participants in the main MTurk survey). We set the "audience sample" feature to target the general population in the U.S., and we collected data from 1,501 participants from Tuesday, July 30 through Thursday, August 1, 2013.

Participant Demographics (N=294)

Participants in our MTurk survey skewed slightly male and young: 58.8% male, 40.5% female, and 0.7% preferred not to answer; 34.4% were between the ages of 18-24, 40.5% were 25-34, 11.9% were 35-44, 6.1% were 45-54, 5.1% were 55-64, 1.7% were 65 or over, and one preferred not to

answer. As to their highest level of education, just over a third had Bachelor's degrees and another third had some college. The remaining third was spread over a broad range of from some high school (1.7%) to having a Master's or doctorate (8.8%).

Just over 70% of the participants were employed full- or part-time or were self-employed (37.1% full-time, 19.6% part-time, and 13.6% self-employed). 19.7% were students, some of whom were also employed, and 16.3% were unemployed or looking for work. Participants represented a broad range of occupations, including customer service representative, sign fabricator, human resources assistant, retired teacher, piano mover, biologist, lawyer, day trader, youth development professional, video editor, filmmaker, administrative assistant, web developer, construction worker, homemaker, writer, and lead programmer.

Data Analysis Approach

To mitigate priming and learn from participants in their own words, we asked open-ended questions. Participants who had experienced the compromise of an email or social networking account were asked five open-ended questions, and the other participants were asked one. For each question, we created a codebook to interpret responses. Coding categories were developed from our review of the responses and related work.

Two coders independently categorized each response using the codebooks. We validated the codebooks through pre- and post-discussion coding, measuring agreement with Cohen's Kappa [22]. Prior to discussion, the Kappa values show agreement ranging from "Fair" (0.373) to "Almost Perfect" (0.857). After discussion, the coders were in "Almost Perfect" agreement on responses from every question (with Kappa values ranging from 0.927 to 1) [22].

RESULTS

In this section, we review details of the compromises that participants experienced as well as who participants think is responsible for keeping their accounts safe and the role they think passwords have in account protection and recovery. We refer to participants who experienced an account hijacking as H1, … , H89 and participants who did not as NH1, … , NH205.

Compromise rates, account importance, & attackers

At the beginning of the survey, all participants were asked, "As far as you know, has anyone ever broken into any of your personal email or online social networking accounts?" Of our 294 participants, 89 (30.3%) answered that one or more such accounts had been compromised.

In our supplemental GCS microsurvey (N=1501), 15.6% of participants indicated that they had experienced one or more account compromises. Though less than our MTurk sample, it still represents a meaningful portion of the Web population experiencing account compromises. Moreover, GCS participants were more likely than MTurk participants to answer "I don't know" (18.7% versus 4.1%, respectively) rather than simply "No," for which the proportions were almost the same (65.8% and 65.6%, respectively). While we cannot account precisely for the difference in MTurk and GCS responses, we note that the motivations for completing surveys may be different; Turkers set out to complete a survey, while GCS participants are trying to get to premium Web content. Differences in the responses may be due to this motivational difference or to other demographic differences, but we note that account compromises are reported at high levels and seem to be a common experience. Our findings are consistent with a 2013 study from the Pew Research Center, which found that 21% of Internet users have had an email or social networking account compromised [31].

How important were the hijacked accounts?

Of the 89 participants who reported experiencing an account compromise, 73 (82.0%) used their accounts at least once a week, and 53 (59.5%) used their accounts daily. When we asked participants for the main reasons they used their accounts, 69 (77.5%) indicated "Personal communication," which we take to be an important use, compared with options such as "Receiving deals or coupons" or "Receiving updates or newsletters."

Who broke into the accounts?

We asked the 89 participants who had experienced a compromise, "Who do you think was behind the break-in?" and offered three response options:

- Someone you didn't know at the time of the break-in,
- Someone you knew but didn't live with at the time of the break-in, and
- Someone you lived with at the time of the break-in.

We followed that by asking for participants' confidence level about who broke in. Just over half (46; 51.7%) indicated they were "Not at all" confident about who broke in, but of the 35 who were at least moderately confident, 30 (85.7%) indicated it was someone they did not know. Of the remainder who expressed at least moderate confidence, three were extremely confident it was someone they knew but did not live with, and two indicated it was someone they lived with. Of those who expressed they were "Slightly" or "Not at all" confident, 51 (96.2%) indicated it was someone they did not know, and only two (3.8%) indicated it was someone they knew but did not live with.

What harm came from the compromise?

In this section, we provide a summary of the harms reported by participants as a result of the compromise.

Hundreds of my emails had been deleted

Most of the compromises reported by the 89 participants did not result in very harmful consequences. Many participants (33; 37.1%) reported having spam emails sent from their accounts to their contacts (e.g., H80 explained, *"I had spam emails sent to people on my contact list."*).

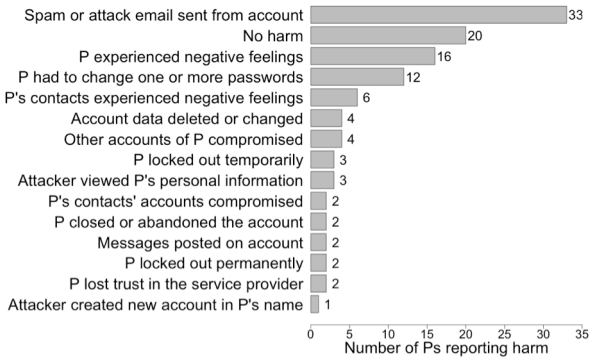

Figure 1. Categories of harm that participants (Ps) experienced as a result of their account compromises (from an open-ended question). Responses were coded into the categories shown; the data show the number of participants who reported each harm (N=89).

Twenty-two participants (24.7%) downplayed the harm (e.g., *"No harm, except for…"*); and 20 (22.5%) indicated that no harm at all resulted from the compromise. Sixteen participants (18.0%) reported experiencing a negative feeling, such as *"It was frustrating, but not harmful"* (H73).

However, for some, the harm was more substantial. Five participants reported being locked out of their accounts, two of whom never regained access. We note that in a later multiple-choice question, 25 (28.1%) of the 89 participants reported that they were locked out of their accounts at least temporarily; however, only five mentioned it as a harm in the earlier open-ended question. Four participants reported having other accounts hijacked as a result of the compromise, one of which was financially related: "*my amazon account [was] hacked and purchases were made*" (H47). Four reported that data in their account was altered or deleted (e.g., "*my personal information was changed"* (H20) and *"hundreds of my emails had been deleted"* (H83)). Two participants believed that accounts belonging to their contacts were compromised as a result, two others closed their accounts after the compromise, and two more lost trust in their service provider (e.g., H36 wrote *"Well, my friends no longer trust my email account and neither do I. We had to find another form of communication."*). See Figure 1 for a breakdown of the open-ended responses.

The harm was mental

Although most participants reported no substantial harm, when asked *how they felt* when they learned their account had been compromised, all but seven expressed strong negative feelings, such as "*I was mad," "violated,"* or "*angry*." For example, though H50 reported, *"No harm came from it. It was just a nuisance,"* he nevertheless reported feeling *"angry"* and *"upset."* The most prominent feelings, each reported by over a quarter of participants, were anger (e.g., *"angry," "mad,"* or *"enraged")* and fear (e.g., *"afraid"* or *"paranoid"*). H48 explained: *"It also made me afraid as I realize how vulnerable electronic information is."* The next dominant emotion was annoyance. Furthermore, some participants felt "*violated," "frustrated,"* or *"vulnerable."*

For some, the emotional damage persisted because they could not fully gauge the consequences. H5 explained,

> *"The harm was mental because I was afraid that the email hacking may have also allowed a computer bug to infiltrate [the] system."*

H72 continues to worry about potential future fraud: *"So far I have [not] noticed any thing* [sic] *like credit fraud yet, but I'm still nervous."*

It made a bad impression of me

Participants didn't just feel annoyed or afraid; a few were also *"embarrassed."* H19 reported,

> *"A lot of my friends and colleagues had received spam emails from [me] and it made a bad impression of me to them."*

Overall, six participants indicated that the compromise caused bad feelings for their contacts, making their contacts *"annoyed"* with the spam or *"a little upset."* H48 expressed the harm in terms of damage to his reputation: *"Rumors were spread, and people might look at me differently because of it."* The embarrassment sometimes was caused by the inappropriate content of the spam messages. For example, H52 explained, *"My religious aunt asked why I was trying to sell her viagra* [sic]."

However, the social implications were not all negative. When asked what good came of the compromise, H62 stated, *"I knew my friends cared! They warned me and asked if I was alright."*

Lock you out of your account

To understand what the 205 participants who had not experienced an account compromise believed might happen in a compromise, we asked, "If someone you don't know broke into your account, how likely is he or she to do the following?" Response options, which participants ranked from "Not at all likely" to "Extremely likely," were:

- Break into your other accounts,
- Send spam to your contacts,
- Find things to blackmail you with,
- Find things to blackmail your contacts with,
- Try to trick your contacts into sending him or her money,
- Lock you out of your account,
- Delete your account,
- Delete stuff in your account, and
- Impersonate you (i.e., identity theft).

Popular responses were that the attacker would impersonate the victim, send spam to the victim's contacts, or lock the victim out of the account. However, these participants were

Who is Responsible	Had a break-in (N=89)	Had no break-in (N=205)
User	**37.1%**	**38.0%**
Service Provider	13.5%	5.9%
Both, User & SP equally	**40.4%**	**40.0%**
Both, User more than SP	4.5%	11.2%
Both, SP more than User	0.0%	3.4%
Didn't mention User or SP	4.5%	1.5%

Table 1. Participants tended to split responsibility for preventing break-ins between the user and the service provider. Each participant is represented exactly once.

not very concerned about their accounts being hijacked. More than 70% were only slightly to not at all concerned (41.5% and 30.7%, respectively), while fewer than 8% were very or extremely concerned (3.4% and 4.4%).

Who is responsible?

In an open-ended question, we asked all 294 participants "Whose responsibility is it to prevent your account from being broken into?" Below, we discuss the responsibilities that participants mentioned for different stakeholders.

Participants acknowledge some responsibility

Most participants indicated that they alone were responsible for preventing break-ins (e.g., H52 explained, *"It is my responsibility to prevent my account from being broken into"*), or that they share responsibility with the service provider. Table 1 summarizes the results. Only 11 (3.7%) mentioned an entity other than the user or service provider, of which five (1.7%) indicated the attacker. We found no significant difference in responses between participants who had or had not experienced a compromise.

Some participants (10; 3.4%) indicated that the responsibility depends on the type of compromise. As NH116 explained: "*It depends, if someone breaks into Facebook and steals my password from them it's their fault. Otherwise its* [sic] *mine."* Furthermore, several participants stated clear responsibilities for users and service providers, such as users being responsible for following good password practices and service providers being responsible for providing a secure website or system.

I need to have a strong password that isn't easy to crack

Seventy-six participants (25.9%) indicated specific responsibilities for users, of which 61 (20.7% of the 294) mentioned something about password management. Responses varied, with most mentioning the need for strong passwords (38; 12.9%). For example, NH107 said, *"I need to have a strong password that isn't easy to crack."* Others mentioned that it is their responsibility to keep passwords secret (15; 5.1%), change passwords frequently (10; 3.4%), and not reuse passwords (9; 3.1%). For example, NH86 explained, *"it's my job to use secure passwords and not use the same password for multiple accounts."* Other user responsibilities included using only trusted websites (6; 2%), avoiding malware (5; 2%), using anti-virus software (4; 1%), logging out of their accounts when done (3; 1%), avoiding unsecured networks (3; 1%), keeping software up-to-date (1; 0.3%), and generally *"being cautious"* (5; 2%).

The provider needs to maintain a secure website

When asked who is responsible for preventing account compromises, 173 (59% of 294), said the service provider is at least partially responsible. Of these 173, 26 (8.8% of 294) indicated that the service provider was responsible for general security. For example, H73 said, *"It is the provider's responsibility to make sure the system is as hack-proof as possible."* Furthermore, 22 (7.5%) mentioned that providers need to keep their systems secure. For example, NH185 wrote, *"The provider needs to maintain a secure website and keep up to date on security threats,"* whereas NH6 mentioned that providers are responsible for *"keeping password databases secure."*

They should be able to tell if an account has been hacked

A few participants stated that the service provider has a duty to prevent the attacker from breaking in, detect suspicious activity, inform the user of the compromise, and help the user get back into the account. NH121 explained, *"They should be able to tell if an account has been hacked, and have a way to contact me."* H31 reported how being notified about the compromise by the service provider increased her trust in them, "*I trusted gmail* [sic] *because they notified me immediately"* (H31).

In a check-all-that-apply question, we asked the 89 participants who had experienced an account compromise, "How did you discover that your account was broken into?" Participants chose from:

- I got locked out because my password didn't work,
- Someone told me about something suspicious from my account (e.g., a strange email or post),
- I was notified by the service provider (e.g., Facebook, Google, LinkedIn),
- I noticed things happening in my account that I didn't do, and
- Other (with a write-in response).

Twenty-six (29.2%) were informed by their account's service provider. However, the most common response was that someone told them about something suspicious from their account (45; 50.6%). Twenty-seven (30.3%) noticed things happening in their account that they didn't do, and fifteen (16.9%) couldn't log in to their account.

The role of passwords in account protection & recovery

Participants not only reported that passwords played a role in their responsibility for preventing account compromises, but they also thought that passwords played an important role in keeping accounts secure in general.

Using a strong password

We asked all 294 participants the check-all-that-apply question, "Which of the following would help prevent your account from being broken into?" Participants chose from:

- Changing passwords often,
- Changing your computer wallpaper,
- Upgrading your web browser,
- Using two-factor authentication (e.g., 2-Step Verification),
- Deleting your web browser cookies,
- Using a strong password,
- Installing photo editing software,
- Avoiding logging in on public computers (such as a library or hotel),
- Avoiding using the same password on different accounts,
- Locking your computer or device screen,
- Signing out when you're done checking your account,
- Using your username as your password,
- None of these, and
- Other (with a write-in response).

The most common responses were password-related: "Using a strong password" (266; 90.5%); "Changing passwords often" (259; 88.1%); and "Avoiding using the same password on different accounts" (239; 81.3%).

Someone, somehow, found out my password

We asked the 89 participants who had experienced a compromise the open-ended question, "How do you think your account was broken into?" Many (28 of 89; 31.5%) believed that passwords were the source of the attack. Passwords were either brute-forced (6 participants), weak (5), guessed (5), reused (5), simply *"found out"* (4), shared (1), shoulder-surfed (1), or reset (1). H67 explained, *"I used the same username and password for everything,"* whereas H37 did not know how her password was stolen, "*Someone, somehow, found out my password. Which seems humanly impossible. Maybe they used a 'password cracking' machine."*

Besides compromised passwords, there was no other popular explanation for how participants thought the compromise occurred. Thirty participants (33.7%) indicated not knowing or being unsure about how their accounts were compromised; nine (10.1%) attributed it to phishing or a malicious link; seven (7.9%) blamed it on viruses or other malware; and five (5.6%) thought the compromise was a result of the service provider being hacked.

How are accounts broken into?

We asked the 205 participants who had not experienced a compromise the check-all-that-apply question, "Which of the following do you think are the most common ways that someone might try to break into your account?" The most popular option (166 of 205; 81%) was "Installing a virus or other program on your computer." Other popular choices were "Tricking you into typing your password on a website that's impersonating another site" (135; 65.9%), and "Stealing your password from another website where you used the same password" (113; 55.1%). Finally, 77 (37.6%) selected "Stealing your computer or device," and 79 (38.5%) chose "Stealing your web browser cookies."

I started using more secure passwords

We asked the 89 participants who had experienced a break-in, "What good, if any, came as a result of the break-in?" More than two thirds reported something positive from the experience, most often a heightened awareness or improved security-related behavior. For example, H74 said that the compromise *"gave me a wake up call about my password security."* The most popular response (reported by 34 participants; 38%) was changing the account password or improving password management. For example, H60 said,

> *"It made me realize that I need a more secure password and now I have the hardest password in the world."*

H72 also *"started using more secure passwords."* Overall, 23 participants (25.8%) reported changing the password for their account, with nearly half expressing that they had created a stronger password than before. Ten (11.2%) mentioned better password behavior not only for the account that was broken into, but also for other accounts. In contrast, having to change their account's password was mentioned as a harmful outcome by 12 participants (13.5%), as H79 explained, *"I had to change my password that I've used for a long time."* Furthermore, 13 participants (14.6%) provided a general statement about being more mindful or better about online security. H86 explained,

> *"I developed smarter habits. I change my passwords often. I also am careful about clicking on things I'm not sure about."*

Other participants reported a change in their account-related behavior. Five (5.6%) mentioned switching to another email provider as a positive, and three (3.4%) listed deleting or abandoning the account as a positive outcome.

DISCUSSION

Modern Web services that host millions of accounts can take a wide variety of measures to prevent account compromises. For system designers who are responsible for the security of these services, the set of design possibilities and tradeoffs is vast and often difficult to navigate. For example, password-based authentication can potentially be made more secure in a variety of ways: perhaps with a policy that prohibits easily guessed passwords; by serving content securely over HTTPS rather than over HTTP; or by using two-factor authentication (i.e., using a password plus another factor, such as a single-use code obtained from the user's mobile phone). Each candidate solution has costs and risks. Costs may include a learning curve for users and implementation and operational costs for the service provider. Potential risks include increased user lockout,

increased friction for users, and low adoption rates. A system designer might ask which solutions are worth pursuing. Even after a service implements a solution, the designer is faced with choices about how to educate users about the new solution and how to motivate adoption.

Our results bring some data to bear on the difficult design tradeoffs that designers face. We discuss our results with an eye toward their implications for the secure design of large, modern Web services. With this perspective, we see five important themes emerging from our results:

(1) Compromised accounts are often valuable to victims;
(2) Attackers are unknown *and* known to victims;
(3) Users acknowledge some responsibility;
(4) Understanding of security measures is incomplete;
(5) Harm from hijacking is concrete *and* emotional.

Compromised accounts are often valuable to victims

Users place different values on their various digital accounts [16,33]. Some may be unimportant, such as accounts users set up merely to try out a new service that they soon abandon; others may be very important, such as a daily-use email or social-networking account. Our results suggest that most of our participants' compromised accounts were frequently used, and a primary use of those accounts was personal communication. Designers should acknowledge that many of today's vulnerable accounts are important, and that users might be willing to invest more effort into protecting them *if* users better understood the risks and outcomes of having their accounts compromised.

Attackers are both unknown *and* known to their victims

Different security mechanisms have strengths and weaknesses in protecting against different kinds of attacks, so it is valuable for system designers to understand the common forms of attack. Over 90% of the 89 participants who experienced a compromise believed their attackers to be unknown to them. Still, attacks by people close to the account holder occur and should not be ignored. If designers must make resource tradeoffs, our results suggest focusing on unknown attackers, but that known attackers should also be considered.

These results can help inform the cost-benefit tradeoff of using authentication systems like social authentication [32], which may provide some security against people unknown to the account holder, but may leave them vulnerable to people known to the account holder.

These results also suggest that two simple password memorability techniques that can help users use unique passwords for their different accounts – (1) writing passwords down at home; and (2) using a password manager on a home computer – are likely to be secure against the most common attackers. Password managers on a home computer also have the added benefit of being secure against phishing, since they provide passwords only to the correct domains. System designers might update advice and training to include recommendations for using these simple password memorability techniques.

Users acknowledge some responsibility

Given the literature indicating limited patience and cooperation of users for security measures [2,4,38], we were surprised that a large majority of participants indicated that they alone were responsible for keeping their accounts safe, or that they shared that responsibility with the service provider – 82% and 89% of compromised and non-compromised participants, respectively. These high rates at which participants acknowledged some responsibility suggest – though they do not guarantee – that users may be open to additional security features, such as two-factor authentication or social-based account recovery, that provide greater security at the cost of somewhat increased friction. Certainly, there are numerous barriers to adoption for such features [12], but our data suggest that at least one barrier – user attitudes – may be overcome.

Understanding of security measures is incomplete

When asked about the common ways accounts are compromised, participants selected malware ("Installing a virus or other program on your computer"), phishing ("Tricking you into typing your password on a website that's impersonating another site"), and third-party password database breaches ("Stealing your password from another website where you used the same password") as the top ways. This indicated a surprising (to us) awareness of the most common ways accounts are compromised.[1]

Nevertheless, when asked what they did or would do if their account were compromised, more participants mentioned password-related measures, such as using stronger passwords or unique passwords for each service, than anti-malware or anti-phishing measures. In particular, 90.5% of our participants selected "Using a strong password" as a way to prevent their account from being broken into, and in open-ended responses, participants emphasized the importance of "secure" and "strong" passwords. We note that "secure" or "strong" passwords are commonly interpreted to mean passwords with a variety of characters or with random-looking patterns. However, such passwords only mitigate some instances of one class of attack – password cracking. Even "Avoiding using the same password on different accounts," a response selected by 81.3% of our participants, only mitigates against third-party breaches and other reuse attacks, but not against phishing and malware. Guarding against phishing and malware attacks requires users to put other preventive measures in place. As others have argued, service providers might wish

[1] Though we are unaware of any published precise data on account compromise methods, evidence such as breach reports [27,31,34] and existence of phishing sites, malware, and database breaches [1,5,8,13,15,25] point to these as the top methods.

to focus efforts on encouraging users to take steps to guard against the most prevalent forms of attack [15,17].

Users may emphasize password management measures because they are a commonly communicated message in many account set-up processes, security training, and in the press; or because users may view password management as a relatively easy, actionable step they can take. Either way, it seems security mechanisms that focus on easily messaged and easily actionable steps are likely to have a chance at user acceptance. In fact, there are simple steps users can take against malware and phishing, such as updating their browser to the latest version, ensuring that automatic updates are enabled, and using a password manager. Simple steps like these could be more widely and clearly communicated through advice and training.

Harm from hijacking is both concrete *and* emotional

Our results suggest that the concrete harm that users experience from an account compromise is often minimal, though it can sometimes be severe. But even when concrete harm is minimal, users experience strong negative feelings such as anger, fear, and embarrassment. Designers who are trying to motivate users to adopt enhanced security mechanisms might try emotional appeals about the harms of compromised accounts to gain users' attention and interest. As one idea on this theme, designers might try using stories about the potential effects of account compromise. In fact, Rader, Wash, and Brooks found that stories are a prevalent and effective way for users to learn about security [30].

LIMITATIONS

This exploratory study has limitations with the population that we surveyed as well as with the methodology that we employed. We used MTurk as our recruiting platform and limited our population to Turkers in the U.S. who were over 18 years of age. As described above, MTurk has known biases, but allowed us to conduct this research quickly and in a reasonably cost-effective manner; we discussed several quality control mechanisms that we used to mitigate the biases. We used the GCS platform to compare our MTurk population to a more broad Web population, but the GCS platform comes with its own limitations.

As to our method, we relied on self-report data collected online. Such data is unconfirmed, and can be impacted by biases such as recall, social desirability, and lack of understanding. For example, participants may have been more likely to recall or even notice the compromise of an important account; therefore, such accounts may be disproportionately reported as compromised. Further, our survey of participants who had not experienced an account compromise often asked them to speculate.

Future work should validate and expand on our results, for example, by considering the experiences of and attitudes toward account hijacking in other countries, for other types of accounts, with different age groups, and by using other methods to investigate these issues.

CONCLUSION

In this paper, we presented results of a survey about people's experiences with and attitudes toward the compromise of a personal email or social networking account. We confirm that the problem is widespread; 30% of our 294 participants reported that at least one of their email or social networking accounts had been compromised. We highlighted five themes that emerged from our results: (1) compromised accounts are often valuable to victims, (2) attackers are unknown *and* known to their victims, (3) users acknowledge some responsibility for keeping their accounts safe, (4) users' understanding of security measures is incomplete, and (5) harm from account hijacking is concrete *and* emotional. We discussed implications for designing security mechanisms into large, modern Web services in ways that we hope will improve chances for user adoption.

ACKNOWLEDGMENTS

Our sincere thanks go out to Adrienne Porter Felt, Allison Woodruff, Anna Avrekh, Antonio Fuentes, Borbala Benko, Cindy Yepez, Diana Smetters, Ed Chi, Eddie Chung, Elie Bersztein, Jay Nancarrow, Kathy Baxter, Martin Ortlieb, Mayank Upadhay, Nadja Blagojevic, Noam Bernstein, Roberto Ortiz, Steve Gribble, Susan Gentile, Tadek Pietraszek, and the many other family, friends, colleagues, participants, and reviewers who have contributed to this work.

REFERENCES

1. Aaron, G. & Rasmussen, R., "Global Phishing Survey: Trends and Domain Name Use in 2H2012," *Anti-Phishing Working Group*, (2013).
2. Adams, A., & Sasse, M.A., "Users are not the enemy, *Communications of the ACM, 42(12),* (Dec 1999), 40-6.
3. The Associated Press, "Twitter feeds of UK's Guardian newspaper hacked," (Apr 29, 2013).
4. Beautement, A., Sasse, M.A., & Wonham, M., "The compliance budget: managing security behaviour in organisations." *Proceedings of the Workshop on New Security Paradigms*, (2008).
5. Bonneau, J., "The Gawker hack: how a million passwords were lost," *Light Blue Touchpaper Blog,* (Dec 15, 2010).
6. Bravo-Lillo, C., Cranor, L.F., Downs, J., Komanduri, S., & Sleeper, M., "Improving Computer Security Dialogs," *Proceedings of INTERACT '11*, (2011), 18-35.
7. Bridis, T., "Hacker impersonated Palin, stole e-mail password," *Associated Press*, (Sep 18, 2008).
8. Bright, P., " 'Military Meltdown Monday': 90K military usernames, hashes released," *arstechnica*, (Jul 12, 2011).
9. Bright, P., "Anonymous speaks: the inside story of the HBGary hack," (Feb 15, 2011).
10. Buhrmester, M., Kwang, T., & Gosling, S.D., "Amazon's Mechanical Turk A New Source of Inexpensive, Yet High-Quality, Data?," *Perspectives on Psychological Science*, *6(1)*, (2011), 3-5.

11. Camp, L.J., "Mental Models of Privacy and Security," *IEEE Technology & Society*, (2006).
12. Cranor, L.F., "A Framework for Reasoning About the Human in the Loop," *Proceedings of the Conference on Usability, Psychology, & Security: UPSEC '08*, (2008).
13. Doyle, K., "Second LulzSec hacker sentenced," *ITWeb*, (Aug 12, 2013).
14. Egelman, S., Sotirakopoulos, A., Muslukhov, I., Beznosov, K., & Herley, C., "Does My Password Go up to Eleven? The Impact of Password Meters on Password Selection," *Proceedings of the Conference on Human Factors in Computing Systems: CHI '13*, (2013), 2379-88.
15. Florencio, D. & Herley, C., "Where do security policies come from?" *Proceedings of the Symposium on Usable Privacy & Security: SOUPS '10*, (2010).
16. Google Consumer Surveys, http://www.google.com/insights/consumersurveys/how.
17. Grosse, E. & Upadhay, M., "Authentication at Scale." *IEEE Security and Privacy,* vol. 11, (Jan/Feb 2013), 15-22.
18. Harbach, M., Fahl, S., Rieger, M., & Smith, M., "On the Acceptance of Privacy-Preserving Authentication Technology: The Curious Case of National Identity Cards," *Privacy Enhancing Technologies, volume 7981 of Lecture Notes in Computer Science*, Springer Berlin Heidelberg, (2013), 245-64.
19. Honan, M., "How Apple and Amazon Security Flaws Led to my Epic Hacking," *Wired*, (Aug 6, 2012).
20. Honan, M., "Mat Honan: How I Resurrected My Digital Life After an Epic Hacking," *Wired*, (Aug 17, 2012).
21. Kittur, A., Chi, E.H., & Suh, B., "Crowdsourcing User Studies With Mechanical Turk," *Proceedings of the Conference on Human Factors in Computing Systems: CHI '08*, (2008), 453-6.
22. Landis, J.R. & Koch, G.G., "The measurement of observer agreement for categorical data," *Biometrics 33*, (1977), 159-74.
23. Mazurek, M.L., Arsenault, J.P., Bresee, J., Gupta, N., Ion, I., Johns, C., Lee, D., Liang, Y., Olsen, J., Salmon, B., Shay, R., Vaniea, K., Bauer, L., Cranor, L.F., Ganger, G.R., & Reiter, M.K., "Access control for home data sharing: Attitudes, needs and practices," *Proceedings of the Conference on Human Factors in Computing Systems: CHI '10,* (Apr 2010), 645-54.
24. McDonald, P., Mohebbi, M., & Slatkin, B., "Comparing Google Consumer Surveys to Existing Probability and Non-Probability Based Internet Surveys," Google Whitepaper, Retrieved from http://www.google.com/insights/consumersurveys/static/consumer_surveys_whitepaper.pdf.
25. Microsoft, *Microsoft Security Intelligence Report*, Vol. 14, (2012), Retrieved from http://www.microsoft.com/security/sir/default.aspx.
26. O'Mahony, J., "Financial Times hacked by Syrian Electronic Army," (May 17, 2013).
27. Onion Inc.'s Tech Team. "How the Syrian Electronic Army Hacked The Onion," (May 8, 2013).
28. Paolacci, G., Chandler, J., & Ipeirotis, P., "Running experiments on Amazon Mechanical Turk," *Judgment & Decision Making*, *5*(5), (2010), 411-9.
29. Perlroth, N. & Shear, M.D., "In Hacking, A.P. Twitter Feed Sends False Report of Explosions," *The New York Times: The Caucus*, (Apr 23, 2013).
30. Rader, E., Wash, R., & Brooks, B., "Stories as Informal Lessons about Security," *Proceedings of the Symposium on Usable Privacy and Security: SOUPS '12*, (2012).
31. Rainie, L., Kiesler, S., Kang, R., & Madden, M., "Anonymity, Privacy, and Security Online," *Pew Research Center*, (Sep 2013).
32. Schechter, S., Egelman, S., and Reeder, R.W., "It's Not What You Know, but Who You Know: A Social Approach to Last-Resort Authentication," *Proceedings of the Conference on Human Factors in Computing Systems: CHI '09*, (2009).
33. Schechter, S., & Reeder, R.W., "1 + 1 = You: Measuring the Comprehensibility of Metaphors for Configuring Backup Authentication," *Proceedings of the Symposium on Usable Privacy & Security: SOUPS '09,* (2009).
34. Schonfeld, E., "Twitter's @Ev Confirms Hacker Targeted Personal Accounts; Attack Was 'Highly Distressing,'" (Jul 14, 2009).
35. Shay, R., Komanduri, S., Kelley, P.G., Leon, P.G., Mazurek, M.L., Bauer, L., Christin, N., & Cranor, L.F., "Encountering stronger password requirements: user attitudes and behaviors." *Proceedings of the Symposium on Usable Privacy & Security: SOUPS '10*, (2010).
36. Sosik, V.S., Bursztein, E., Consolvo, S., Huffaker, D., Kossinets, G., Liao, K., McDonald, P., & Sedley, A., "Online Microsurveys for User Experience Research," *CHI '14 Extended Abstracts on Human Factors in Computing Systems*, (2014—to appear).
37. Wash, R., "Folk Models of Home Computer Security," *Proceedings of the Symposium on Usable Privacy & Security: SOUPS '10*, (2010).
38. Whitten, A. & Tygar, J.D. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," *Proceedings of the USENIX Security Symposium,* (1999).