The Effect of Breach Notifications on Victims of Previous Data Breaches

Masha Boyarinova
University of Chicago

Ni’Gere Epps
University of Chicago

Santiago Giron
University of Chicago

Alexandra Nisenoff
University of Chicago

Adam Rivkin
University of Chicago

ABSTRACT

In light of the increasing number of data breaches and their toll on individuals’ privacy and security, it is important to design breach notifications that equip affected individuals with the knowledge they need to secure their data in the aftermath of a breach. This paper presents results from a pilot study that investigated the effect of differences in breach notification design on the actions that affected users think they should take take, as well as on their understanding of the breach. As part of our study, we created two breach notifications – one with the accounts involved in breaches and specific details on the types of data at risk, and one with just the accounts involved in breaches. We then sent the notifications to participants, and we later interviewed the participants about the actions they took or were planning to take and about their perception of the notification and general information about their perception of data breaches. Our study found initial evidence that including detailed information about the breached data gives affected users a slightly better understanding of the potential consequences of the breach and makes them more likely to take actions to secure their data. We would need to conduct the study design on a larger scale to reach conclusive results.

1 INTRODUCTION

In this paper we begin to explore users reactions to data breach notifications. Current breach notification designs do not seem to be effective in motivating affected users to take appropriate action in response to a data breach, so more research needs to be done on how to design usable and actionable breach notifications. With the increasing frequency of data breaches and the serious impact they have on their victims, as well as the shortage of research focusing on how users interact with and perceive data breach notifications our research provides a new area of focus for this growing issue.

We seek to address the problem of users who experience confusion and uncertainty over what steps to take after receiving a breach notification. Even when users are notified of breaches, they often do not know what actions they can take to secure their information [19]. Considering the prevalence of recent data breaches, it is particularly important to provide usable breach notifications to impacted users. We hypothesize that more detailed information on what was breached will give users a more concrete idea of what steps they need to take after a breach. If users know what specific information was revealed in a breach, we predict that they will be able to form a more accurate mental model of what risks they face and be better equipped to decide on what actions are necessary.

To explore this issue we created and distributed personalized data breach notifications with varying amounts of information on what was included in the data breach. These breach notifications were followed up with semi structured interviews designed to allow us to assess the users experiences with our notification, experiences with previous breach notifications, and perceptions about data breaches.

Due to the small sample size of our study, we only present preliminary findings in this paper. The study found that informing affected users about the particular types of data that had been compromised by the breach may help ensure they have a better understanding of potential consequences of the breach and, thus, make them better equipped to take appropriate actions to secure compromised data.

2 RELATED WORK

We provide context for our study through an overview of previous research on actions after data breaches. First, we examine the impact of breaches on the companies involved in a breach. We then look at the limited number of studies that address data breaches from a user perspective. Finally, we provide a survey of papers related to effective breach notification design.

A. Data Breaches and Companies

Most prior work about data breaches has focused on the cost of breaches to companies rather than to users. Researchers have investigated the effect of data breaches on the stock market value of affected companies over time, the accuracy of economic models of breaches for small and large organizations, and the per capita cost to a company of each record leaked [5, 6, 14]. Other research applied legal and criminal theories to the subject of data breaches. In 2010, Abraham Shaw advocated for increasing data breach liability for businesses that failed to meet security standards based on those used for credit card companies [21], in 2015 Sen and Borle used criminal theories to predict the risk of breaches within a state [20], and in 2017 Solove and Citron wrote a legal review about whether anxiety due to a data breach was a basis for a lawsuit [22]. Several of these theoretical papers found that a consistent system for understanding the risk and impact of data breaches had yet to be discovered [20, 22].

These papers are just part of a large body of research focused on examining the perspective that industries have on data breaches, their prevention, or the liabilities that companies might face afterwards [2, 11, 7, 10]. Considering the large amount of existing work which takes an industry-level analysis of breaches, we believe that there is a gap in literature that takes the perspective of users. Users and companies likely have different mental models of breaches. Studies of users' views will likely lead to different outcomes than studies of companies, providing new insight into the unexamined harms of breaches. Also, the needs of users put at risk by breaches are distinct from the needs of companies and warrant more examination.

B. Data Breaches and Users

Far less recent research has been done to assess the impact that data breaches have on individuals. The RAND Institute found that 26% of their respondents had received a notification of a data breach in the last 12 months with 51% of them also claiming to have received multiple notifications of data breaches [4]. 45% of people surveyed in a 2017 PwC survey reported that they expected their email or social media accounts to get hacked in 2018 [1], and some studies have shown that the frequency of data breaches has been increasing [9], which indicates that this is a prevalent issue in need of further research.

According to the Ponemon Institute, the most common costs of a data breach, as reported by affected users, are stress, time costs of having to prevent potential consequences of the breach, fraudulent charges to their accounts, and an increased fear of identity theft [3]. When asked, in a study by Ablon et al., to estimate a monetary cost of the breach they experienced, about one-third of the participants said that it had caused them no dollar loss, while the remaining participants reported a median financial loss of $500 [4]. That number was higher if health data, social security numbers, or financial data was involved.

Despite the fear that accompanies a data breach, many people do not seem to spend significant time securing their information. For instance, Harrell showed that most victims spent less than one day resolving associated financial and credit problems after a breach [9]. According to a study by Greene, common actions that people take after a data breach include avoiding using credit cards if financial information had been involved, monitoring account activity more closely for a period of time, running antivirus scans, and changing passwords [17]. However, if users perceive that no important information is connected to the breached account they are less likely to take action [4].

Our research differs from this work because we present users with an accurate breach notification during our study. By showing users new information about their breaches before an interview, we aim to capture their views shortly after seeing a new breach notification. Also, we provide users with information on their own breaches that can be accessed through the website ”Have I Been Pwned,” which is a valuable tool available to most users that has yet to be evaluated extensively in scientific studies.

C. Notification Design

Several legal papers have argued for the creation of a federal breach notification law to standardize companies responsibilities after breaches [16, 15]. However, many of these legal arguments fail to address laws regarding the content or design of a breach notification such that consumers know what steps to take when a data breach occurs. While ensuring that companies actually issue notifications is important, designing notifications that are usable and provide maximum support for users is key to effective breach cleanup.

Proposals by Peters in 2014 and Zou et al. in 2019 address this issue and examine how to improve the effectiveness of notification design [19, 25]. Other proposals have explored the direct application of privacy design principles to breach notification design. Jaap-Henk Hoepman includes data breach notifications as a candidate for design strategies based on data protection legislation [13] and Colesky et al. address notifications from the European Unions General Data Protection Regulation with privacy by design strategies [8]. Additionally

Fer O'Neil uses a heuristic approach to analyze flaws in a breach notification from the 2013 Target data breach [18] and Zou et al. conducted a 2019 analysis of the readability, structure, risk communication, and presentation of 161 previous breach notifications that found that little effective, actionable information was provided to users [23]. Our approach differs from these papers in our incorporation of direct user testing to inform design strategies. We aim to move beyond theoretical frameworks for informative design towards testing these frameworks on actual users in a situations with higher ecological validity.

Maximilian Golla et al. investigated how users respond to two data breach notifications with two survey studies. In the first, users were shown a model password-reuse notification based on notifications sent by real companies [12]. Participants were then surveyed about the feelings elicited by the notification and the actions they may have taken in response. The second study involved showing participants notifications based on the model notifications from the first study but varied in targeted ways. The study found that these variations had a small impact on user behavior, but participants still reported they would take actions that would not adequately protect them against future password-reuse attacks. While Golla et al. explored the effect of breach notifications through user studies, their approach involved presenting participants with a hypothetical breach notification scenario, whereas our study presents participants with notifications of real data breaches that affect them.

In another study involving users perceptions of a data breach, Yixin Zou et al. conducted interviews with 24 participants about the Equifax data breach in 2017. The study aimed to better understand participants mental models of the breach [24]. Zou et al. found that while most participants demonstrated an understanding of the potential risks of the breach, a majority did not assume they would be affected. In contrast, our study directly presents participants with evidence of their exposure to a data breach, and explores their perception of the risks with this knowledge in mind.

3 DESIGN ITERATIONS

Our study design evolved through several iterations, illustrating some of the many difficulties in studies of data breaches. Our initial design involved encouraging participants to think-aloud as we presented them with mock breach notifications and then conducting a follow-up interview. However, this study seemed similar to prior work by Golla et al. and had insufficient ecological validity because participants saw hypothetical breach scenarios instead of information they considered personally valuable [12].

Our next iteration involved a deception study where participants provided data to a study unrelated to breaches and then received a personalized notification that this data had been breached. While this study would closely mirror a real situation, it also could cause psychological harm to participants who believed that their privacy has been violated. Although a deception study on data breaches could lead to highly beneficial and valid results, the ethical intricacies involved led us to avoid this type of study for the scope of this assignment.

Our third approach was to collect real data and emails leaked in pastes on Pastebin.com and send notifications to potential participants, who would enroll to take a survey. Unlike the previous design, the third study did not involve deception because our notifications were based on real breaches that had already transpired. However, the ethical issue of sending a breach notification before asking for consent to be part of a study, the differences between involvement in data breaches and in pastes, and the low response rate from participants whose email was found through Pastebin resulted in us abandoning this methodology.

Our final design incorporated many of the ideas from our design process. Similarly to the first design, we interviewed participants shortly after they see a breach notification. However, by presenting participants with information involving their actual, personal leaks from "Have I Been Pwned," we hoped to collect ecologically valid responses like in our second and third designs. Throughout the design process, we realized that studying breach notifications involves a difficult balancing act of realistically simulating the risk from exposure of private information with the need to protect participants from actual harm and psychological distress. Our study aims to avoid causing undue concern to participants while remaining ecologically valid.

4 METHODOLOGY

For this study participants were emailed personalized data breach notifications based on data breaches that they had been a part of in the past. These notifications had varying amounts of information on what information was included in the data breach. These notifications were followed up with a semi structured interview to assess how they reacted to the breach notification, their experiences with previous breach notifications, their trust in our notification, and their risk and value assessment of the breached accounts listed in the notification.

Recruitment and Breach Notifications

To increase the likelihood of getting responses we individually reached out to friends of friends to see if they would be interested in being a part of our study. We particularly tried to reach out to people that were older than 35 since they would be more likely to have previously been a part of a data breach. If the person we reached out to expressed an interest in being a part of the study we asked for an email (if that is not how they were originally contacted) such that we could send them the consent form. Our consent form explained the purpose of our study, what would be involved for them in the study, the possible risks associated with the study, how they would be compensated for their time, and asked them to confirm that they were not a part of a vulnerable population. The consent form can be found in the Appendix. In the same email that included the consent form we also requested a list of current emails and the subjects availability over the following few days for the interview.

Once we received the list of emails from the participants and had a time arranged for the interview we ran all of their emails through Have I Been Pwned, a website that checks if an email has been associated with any of the breaches they have in their database and also lists the types of information associated with each breach (passwords, emails addresses, etc). Have I been Pwned also lists ”pastes” and breaches of companies that people might not actually have accounts set up with such as advertising companies. We attempted to not include these items in our notifications. All of the breaches that we encountered for the participants we interviewed were seemingly benign so none of the accounts were removed from a breach notification due to the subject matter of the account.

If none of the emails the subject provided were associated with any breaches in the Have I Been Pwned database, we emailed them back asking if there were any other emails that they frequently used. If there were no other emails that they used or if none of the other emails they provided us were connected to any data breaches we would have informed them of this and sent them a modified version of the debrief email explaining that none of their emails had been a part of any of the breaches we had access to. That being said, sending a modified debrief was not necessary for any of the people that we reached out to as they were a part of at least 2 breaches with a max of 7 breaches and an average of 4. The number of breaches included in the data breach notifications is shown in Figure 1.

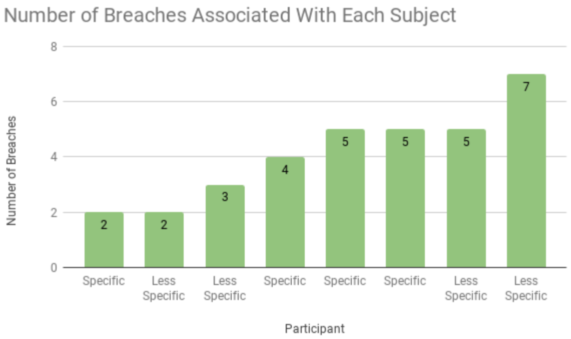


Figure 1: Number of breached accounts for each participant

Participants were then randomly sorted into two groups. Each group got either a ”specific” or ”less specific” notification. In our study, we ended up with four participants in each condition. For the specific data breach notifications, accounts and details about the types of information revealed in the breach were included. For the less specific breach notification, the details about the types of information revealed in the breach were omitted from the notification. Aside from this one difference, the two notifications used the same wording and format. Examples of both the specific and less specific data breach notifications are included in the Appendix. While designing the notifications we kept the NEAT and SPRUCE guidelines in mind, with the exception of providing the user with an actionable set of choices to make as this would have biased their responses during the interview phase of our study. All data breach notifications and subsequent emails were sent from BreachNotifications@uchicago.edu an alias on one of the researcher’s student email accounts and designed to emphasize that the notification was coming from researchers at the University of Chicago. There was then a delay before the interview to allow participants to take action in response to the notification.

Interview procedure

We performed semi-structured interviews with our participants to evaluate the effects of our notification design. The interviewer was never the same person who had reached out to that participant as a friend of a friend. Although the design was varied between subjects, the interview questions were the same for participants receiving either design. We asked our respondents about their experiences with previous breaches, how they reacted to our breach notification, and their risk and value assessments of the breached accounts listed in the notification. We also asked about participants experiences with previous breach notifications, their trust in our notification, and the details of the notification that stood out to them. Finally, we asked participants what they believed they should do in response to a breach, and if they planned on taking any future steps. The full interview script can be found in the Appendix.

All of our interviews were conducted using the video conferencing service appear.in. This allowed us to connect with our participants over video chat without requiring them to install new software or create accounts. We decided to use web conferencing software so that multiple researchers could join a call remotely, allowing one of us to take notes while the other conducted the interview. We planned to use the screen-sharing capabilities of appear.in to display a respondents breach notification if they had not seen it prior to the interview. The duration of the interviews varied significantly, with some only taking only 6 to 7 minutes and longer interviews lasting approximately 15. After the interviews, we took additional time to answer participants questions.

Many of our participants were alarmed by our breach notification and had questions for us at the start of the interview. Some participants wanted to know how we obtained data about their breaches, or whether these breaches had actually occurred. They were often unfamiliar with the names of breaches appearing in their notification and were dismayed that unknown entities had compromised their information. We did not address most of participants questions and concerns during the interview to avoid biasing their responses.

Debriefing

After the interview we conducted a verbal debriefing to allay participants concerns. We took questions from participants regarding their breached information and provided advice for handling data breaches. We also answered any questions participants had about our research methods and its objectives. We explained how we used Have I Been Pwned to obtain their breach information, and instructed them on how they could use it themselves to check the security of their accounts and passwords.

In addition to the verbal debriefing after the interviews, we sent participants a debriefing email along with their compensation for participating. The emails included a breach notification with the more specific information design for all participants. The debriefings provided links to Have I Been Pwned and educational resources on handling data breaches. They also included links to articles from The University of Chicago IT Services, which provide useful advice on information security measures that could prevent data breaches.

Qualitative Coding

After conducting our interviews we performed qualitative coding to identify common themes in the responses. We worked through an anonymized transcription of our interviews and performed the coding as a group. For each question, we determined a set of themes for the responses. We then tallied the number of responses fitting each theme. Finally, we compared the number of occurrences of each theme between participants who received more specific and less specific breach notifications.

Pilot Study

In order to evaluate and refine our study design, we performed a pilot test of our procedure with the first two respondents to our study. We found that some of our interview questions elicited the same information from participants, so we merged these questions to eliminate the redundancy. One question asked if participants took action after receiving the breach notification and the next asked whether they planned on taking any long term steps going forward. In response to the first question, participants often explained that they had yet to take any action, but that they planned to take specific steps going forward. As a result, participants often provided the same answer to the next question.

Both of the participants in our pilot study were unfamiliar with the names of some of the breaches in their notifications. These were often data breaches of third parties with which participants had no direct interaction, but which nonetheless possessed some of their personal information. We considered omitting these breaches from our notifications since our participants would not know which account or service these breaches had affected. We ultimately decided to keep these types of breaches as part of our notification design because we felt that their inclusion could still prompt users to take general precautions.

Limitations

The method and sample population we used have several limitations. We had a small sample size chosen for likelihood to respond and likelihood to be victims of previous breaches, and not for generalizability. This means that our findings cannot be used to extrapolate to the population at large. Participants were also not strangers to us. This may have lead to subjects being more likely to participate in the study or to be more trusting of the notification. The personal connection to the people running the study and the prior knowledge that they were a part of a study on data breaches may have also increased probability of the participants to delay taking action to deal with the breach in favor of waiting to ask the interviewer for advice. Also, due to the nature of our data breach notification, we notified the participants of multiple data breaches in the same notification rather than a single one which is more common in actual data breaches. Our notification was also designed to show that it was coming from the University of Chicago rather than the companies that were breached as is more typical of data breaches. Since our notifications included all of the breaches (in the Have I Been Pwned database) for each participant the accounts, age of the breaches, as well as the number of accounts varied for each subject. Many of the breaches included on Have I Been Pwned may not have been accounts that the subjects had directly signed up for.

There was also quite a bit of variance in the time between when the participant received the breach notification and when they were interviewed, this was due to the times the participants were available to be interviewed. The same issue of scheduling also meant that the interviewer was not consistent across all of the subjects. Additionally, some potential participants expressed an initial interest in participating in the study but did not follow-up after the consent form to schedule an interview time.

5 ETHICS

As this was just a pilot study with very few participants we did not go through our institution's IRB. We received consent from the participants before we sent them a breach notification or looked into possible data breaches they may have been involved in. We also only looked into breaches on emails that they voluntarily shared with us. By using Have I Been Pwned we also were not given access to any of the information that was breached. Instead, we just saw that their email was associated with the breaches that came up and general information on the breach. As was mentioned earlier, we also debriefed all of our subjects following the interview both verbally and in a follow-up email. All of the data collected from our subjects was stored securely online and all data that connected a specific person to a set of responses was deleted.

6 RESULTS

Since the sample size of the study was quite small, the results we present are not generalizable, and instead we report recurrent themes we identified in the interviews by qualitatively coding the participants responses. Many of these themes could be a direct result of our notification design choices, while some may be due to the limitations inherent in our study design. We discuss these themes in detail below.

Knowledge of Breach

One participant recalled receiving a breach notification regarding an account we informed them about, which claimed that their account was likely unaffected. Meanwhile, all other participants reported they were not aware at all the accounts in question had been breached. This may be due to the participants forgetting that the breach had occurred, as some of the breaches we informed them of happened up to 11 years before the study. Additionally, half of the participants were not aware they even had some of the accounts listed in the breach notification. These accounts were either set up through a third party, such as another company a participant had an account with, or opened without their knowledge by somebody they knew.

Trust in Notification

All participants perceived the breach notification as trustworthy because it was sent from a university domain and because they were aware that they were part of a research study about security.

Retained Details

Five of the participants were able to recall that the breach notification contained a list of their accounts that had been breached. Three participants found the number of accounts listed in the notification particularly striking, and half of the participants were surprised to find accounts they did not recognize on that list. Half of the participants who received a specific notification also remembered that the notification contained information about the types of data that was associated with the breaches, but did not specify if they could recall that information.

Call to Action

None of the participants took appropriate actions to secure their data by the time of the interview. Half of the participants did not take any action at all and were waiting to ask their interviewer for advice as they were unsure what steps to take. Two participants tried to log into their accounts to see if there was any suspicious activity, but did not change their account credentials. Five of the participants thought they should eventually change their passwords for the breached accounts, and two thought they should use more secure passwords for the affected accounts going forward. Even though half of the participants reported that they had reused their password for at least one of the breached accounts, none mentioned that they should change their password on the accounts that shared the breached password.

Concerns

All of the participants were particularly concerned about their financial (bank account or credit card) information being compromised. Additionally, half of the participants were worried about the attackers gaining access to their personal information (name, home address, etc.). The participants tended to be less concerned about the breach if it involved an account they had not used for a long time, as they thought the information it contained was probably outdated. Most of the participants who received specific notifications seemed aware of the particular types of their information (as listed in the breach notification) that was now at risk. Meanwhile, the participants who received unspecific notifications only had a vague idea of which of their information was compromised (e.g., ”personal information” or ”account information”).

Breached Accounts

The following table presents the distribution of the participants accounts that had been breached. We found that the most commonly breached among the participants was their account with LinkedIn (five participants were a part of this breach), while Houzz, MyFitnessPal, and ShareThis breaches shared the second place (each affected three of the participants).

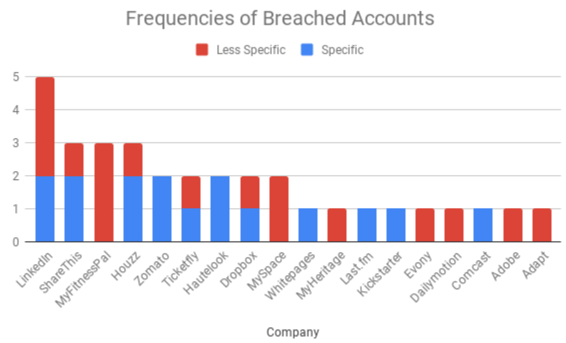


Figure 2: Frequencies of accounts involved in breaches

7 DISCUSSION

Our findings suggest the importance of breach notification design in ensuring that users are properly informed of the data breach, the information that was compromised, and what protective actions should be taken next. As this was just a pilot study we did not collect enough data to definitively draw a conclusion about our hypothesis. Listing what accounts were breached and the vulnerable information that compromised seemed to lead to a slightly improved understanding of the potential consequences of the data breach. The most prominent difference we saw between the participants in the two groups was that the participants who received more informative notifications were aware of which of their information was at risk while the participants who received less specific notifications tended to focus on general categories of information that covered a broader range of topics.

We found that in designing the notification, it is important that the users receive it from a credible source. Many of our participants stated that they only read or responded to the breach notification because it came from the university or because they knew they were a part of a study. Thus, it is important to establish credibility when sending breach notifications or the users may be more likely to not take any action as a result of the notification. Also, we saw evidence that it is important to include what steps to take next after a data breach because many of the participants did not know what to do or waited for us to give them directions on how to protect their accounts and information. Without clear instructions, participants tended to wait for directions from a trusted authority, suggesting that the inclusion of a clear process in a notification is key to effective user action. The primary steps the participants were planning to take were consistent with what we expected based on previous research [4], but there was a lot of variation in the additional steps the participants considered.

Lastly, it is especially crucial for companies that deal with financial information to send informative breach notifications with the next steps to take. Participants primarily expressed concern about financial companies and put less value on other sorts of breached information. Financial breaches appeared to be the main cause for worry and perceived risk for participants.

While we found initial evidence supporting our hypothesis, we had too small a sample size to draw any strong conclusions. While this study provided a valuable pilot for future research, it cannot reach a conclusion on its own. Future work on this subject could include a replication of this study with a larger and more diverse participant pool as well as a more consistent delay between participants agreeing to be a part of the study, the personalized notification, and the actual interview. Variations on the study could have the notifications appear to be coming from the breached company or focusing on a single data breach to improve the ecological validity of the study. Instead of focusing on varying the amount of information displayed in the data breach notification, a possible adaptation could be to see how variations in the suggested steps that are recommended to data breach victims in notifications affect the steps that they take and the steps that they think that they need to take following a data breach.

References

[1] How consumers see cybersecurity and privacy risks:pwc. https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/cybersecurity-protect-me.html.

[2] 2011 data breach investigations report. *Verizon RISK Team, Available: www.verizonbusiness.com/resources/reports/rp_databreach-investigationsreport-2011_en_xg. pdf*, pages 1–72, 2011.

[3] The aftermath of a data breach: Consumer sentiment. *Ponemon Institute LLC*, jan 2012.

[4] Lillian Ablon, Paul Heaton, Diana Catherine Lavery, and Sasha Romanosky. Consumer attitudes toward data breach notifications and loss of personal information. 2016. Santa Monica, CA: Rand Corporation.

[5] Alessandro Acquisti, Allan Friedman, and Rahul Telang. Is there a cost to privacy breaches? an event study. *ICIS 2006 Proceedings*, page 94, 2006.

[6] Abdullah M. Algarni and Yashwant K. Malaiya. A consolidated approach for estimation of data security breach costs. *2016 2nd International Conference on Information Management (ICIM)*, 2016.

[7] Long Cheng, Fang Liu, and Danfeng Daphne Yao. Enterprise data breach: causes, challenges, prevention, and future directions. 2018.

[8] Michael Colesky, Jaap-Henk Hoepman, and Christiaan Hillen. A critical analysis of privacy design strategies. *2016 IEEE Security and Privacy Workshops (SPW)*, 2016. doi:10.1109/spw.2016.23.

[9] Harrell E. Victims of identity theft, 2014. *Bureau of Justice Statistics Bulletin*, 2017. https://www.bjs.gov/content/pub/pdf/vit14.pdf.

[10] Warren Ross Federgreen. System and method for automated data breach compliance. U.S. Patent Application No. 13/435,126.

[11] John A. Fisher. Secure my data or pay the price: Consumer remedy for the negligent enablement of data breach. *Wm. & Mary Bus. L. Rev. 4*, page 215, 2012.

[12] Maximilian Golla, Miranda Wei, Juliette Hainline, Lydia Filipe, Markus Drmuth, Elissa Redmiles, and Blase Ur. What was that site doing with my facebook password? *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security - CCS 18*, 2018. doi:10.1145/3243734.3243767.

[13] Jaap-Henk Hoepman. In ict systems security and privacy protection. *29th IFIP TC 11 International Conference, SEC 2014*, page 446459, jun 2014. Marrakech, Morocco.

[14] Ponemon Institute. 2018 cost of a data breach study: Global overview. *Ponemon Institute LLC*, 2018.

[15] Jill Joerling. Data breach notification laws: An argument for a comprehensive federal law to protect consumer data. *Washington University Journal of Law and Policy vol. 32, no. 1*, pages 467–488, 2010. HeinOnline, https://heinonline.org/HOL/P?h=hein.journals/wajlp32&i=469.

[16] Dana J Lesemann. One more unto the breach: An analysis of legal, technological, and policy issues involving data breach notification statutes. *Akron Intellectual Property Journal vol. 4, no. 2*, pages 203–238, 2010. HeinOnline, https://heinonline.org/HOL/P?h=hein.journals/akrintel4&i=207.

[17] Federal Reserve Bank of Boston. Consumer reactions to data breaches. may 2017.

[18] F. ONeil. Target data breach: applying user-centered design principles to data breach notifications. *In Proceedings of the 33rd Annual International Conference on the Design of Communication*, page 47, 2015. ACM.

[19] Rachael M Peters. So you've been notified, now what: The problem with current data-breach notification laws. *Arizona Law Review vol. 56, no. 4*, pages 1171–1202, 2014. HeinOnline, https://heinonline.org/HOL/P?h=hein.journals/arz56&i=1197.

[20] Ravi Sen and Sharad Borle. Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems, vol. 32, no. 2*, page 314341, 2015.

[21] Abraham Shaw. Data breach: From notification to prevention using pci dss. *Columbia Journal of Law and Social Problems vol. 43, no. 4*, pages 517–562, 2010. HeinOnline, https://heinonline.org/HOL/P?h=hein.journals/collsp43&i=525.

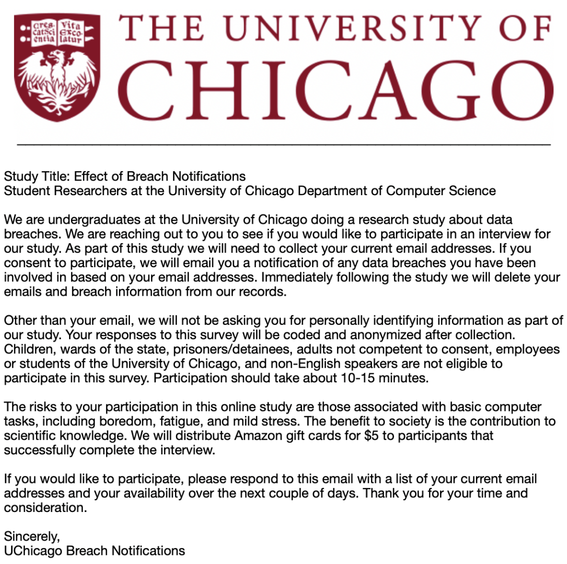
[22] Daniel J. Solove and Danielle Keats Citron. Risk and anxiety: A theory of data breach harms. *SSRN Electronic Journal*, 2016.

[23] Zou Yixin, Shawn Danino, Kaiwen Sun, and Florian Schaub. You might be affected: An empirical analysis of readability and usability issues in data breach notifications. *In Proceedings of CHI Conference on Human Factors in Computing Systems (CHI '19)*, may 2019. Glasgow, Scotland UK. ACM, New York, NY, USA.

[24] Yixin Zou, Abraham H Mhaidli, Austin McCall, and Florian Schaub. I've got nothing to lose: Consumers' risk perceptions and protective actions after the equifax data breach. *SOUPS*, 2018. In Proc.

[25] Yixin Zou and Florian Schaub. Beyond mandatory: Making data breach notifications useful for consumers. *IEEE Security & Privacy 17.2*, pages 67–72, 2019. https://ieeexplore.ieee.org/abstract/document/8677354.

APPENDIX



THE UNIVERSITY OF CHICAGO

Study Title: Effect of Breach Notifications
Student Researchers at the University of Chicago Department of Computer Science

We are undergraduates at the University of Chicago doing a research study about data breaches. We are reaching out to you to see if you would like to participate in an interview for our study. As part of this study we will need to collect your current email addresses. If you consent to participate, we will email you a notification of any data breaches you have been involved in based on your email addresses. Immediately following the study we will delete your emails and breach information from our records.

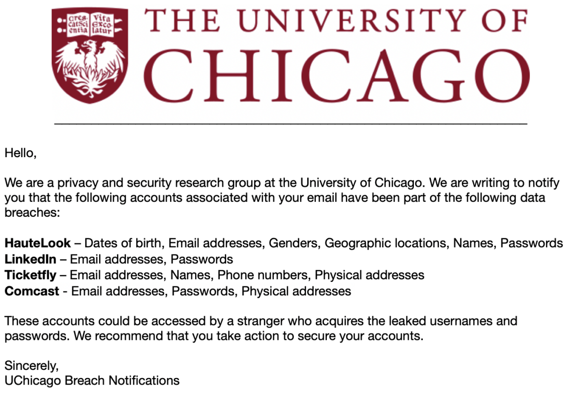
Other than your email, we will not be asking you for personally identifying information as part of our study. Your responses to this survey will be coded and anonymized after collection. Children, wards of the state, prisoners/detainees, adults not competent to consent, employees or students of the University of Chicago, and non-English speakers are not eligible to participate in this survey. Participation should take about 10-15 minutes.

The risks to your participation in this online study are those associated with basic computer tasks, including boredom, fatigue, and mild stress. The benefit to society is the contribution to scientific knowledge. We will distribute Amazon gift cards for $5 to participants that successfully complete the interview.

If you would like to participate, please respond to this email with a list of your current email addresses and your availability over the next couple of days. Thank you for your time and consideration.

Sincerely,
UChicago Breach Notifications

Figure 3: The consent form to participate to the study. We individually reached out to friends of friends and sent them this form.



THE UNIVERSITY OF CHICAGO

Hello,

We are a privacy and security research group at the University of Chicago. We are writing to notify you that the following accounts associated with your email have been part of the following data breaches:

HauteLook – Dates of birth, Email addresses, Genders, Geographic locations, Names, Passwords
LinkedIn – Email addresses, Passwords
Ticketfly – Email addresses, Names, Phone numbers, Physical addresses
Comcast - Email addresses, Passwords, Physical addresses

These accounts could be accessed by a stranger who acquires the leaked usernames and passwords. We recommend that you take action to secure your accounts.

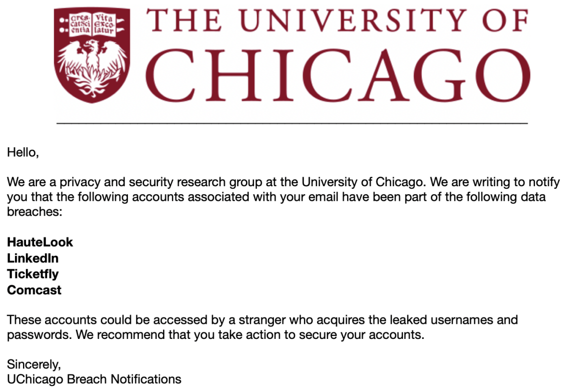
Sincerely,
UChicago Breach Notifications

Figure 4: A specific notification with account websites and details about types of information revealed in the breach

Interview Script

1. Did you know that these accounts had been breached prior to our notification?

2. What parts of our notification did you trust?


THE UNIVERSITY OF CHICAGO

Hello,

We are a privacy and security research group at the University of Chicago. We are writing to notify you that the following accounts associated with your email have been part of the following data breaches:

HauteLook
LinkedIn
Ticketfly
Comcast

These accounts could be accessed by a stranger who acquires the leaked usernames and passwords. We recommend that you take action to secure your accounts.

Sincerely,
UChicago Breach Notifications

Figure 5: A less specific notification with just account websites

3. What information do you remember seeing as a part of the breach notification?

4. What were the most striking features of the breach notification?

5. Did you take any steps after receiving our breach notification?

6. What if any steps do you still plan on taking or have not had a chance to take yet?

7. What do you think you need to do after a data breach?

8. For each account breached:

How do you think perpetrated the data breach?

Do you remember what your password was for this account (you dont need to tell us what it is)?

Have you used this password for any other accounts? If so how many?

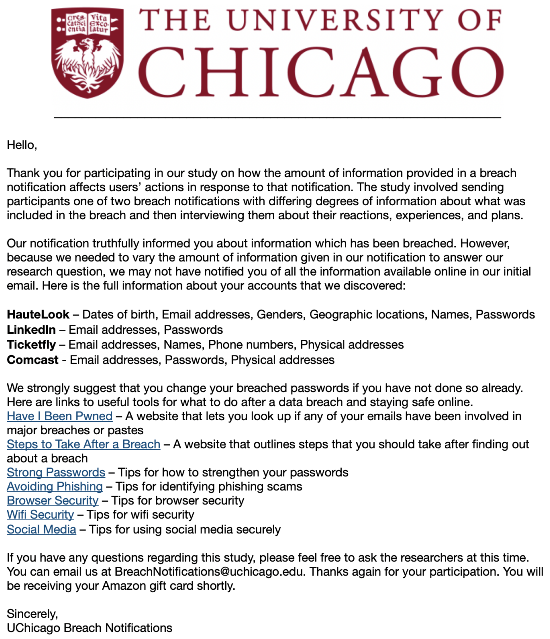
9. Have you received breach notifications before? If so, how did you receive them and were they from the company that had been breached or another source?

10. What worries you most about a data breach?

11. What types of information do you think could be at risk from this breach?

12. How valuable do you consider the account which was breached?

13. Is there anything else you would like to tell us about?


THE UNIVERSITY OF CHICAGO

Hello,

Thank you for participating in our study on how the amount of information provided in a breach notification affects users' actions in response to that notification. The study involved sending participants one of two breach notifications with differing degrees of information about what was included in the breach and then interviewing them about their reactions, experiences, and plans.

Our notification truthfully informed you about information which has been breached. However, because we needed to vary the amount of information given in our notification to answer our research question, we may not have notified you of all the information available online in our initial email. Here is the full information about your accounts that we discovered:

HauteLook – Dates of birth, Email addresses, Genders, Geographic locations, Names, Passwords
LinkedIn – Email addresses, Passwords
Ticketfly – Email addresses, Names, Phone numbers, Physical addresses
Comcast - Email addresses, Passwords, Physical addresses

We strongly suggest that you change your breached passwords if you have not done so already. Here are links to useful tools for what to do after a data breach and staying safe online.
Have I Been Pwned – A website that lets you look up if any of your emails have been involved in major breaches or pastes
Steps to Take After a Breach – A website that outlines steps that you should take after finding out about a breach
Strong Passwords – Tips for how to strengthen your passwords
Avoiding Phishing – Tips for identifying phishing scams
Browser Security – Tips for browser security
Wifi Security – Tips for wifi security
Social Media – Tips for using social media securely

If you have any questions regarding this study, please feel free to ask the researchers at this time. You can email us at BreachNotifications@uchicago.edu. Thanks again for your participation. You will be receiving your Amazon gift card shortly.

Sincerely,
UChicago Breach Notifications

Figure 6: A debrief email sent to participants after completion of the interview