Effect of Breach Notifications on Victims of Previous Security Breaches

Final Report:
Ni'Gere Epps, Masha Boyarinova, Santiago Giron, Alexandra Nisenoff, Adam Rivkin

Research Question & Hypothesis

How does the design of a breach notification affect what users think they should do after a data breach?

More specifically, how does the display of compromised information in a data breach affect how users believe they should act?

We hypothesize that more detailed information on what was breached will give users a more concrete idea of what steps they need to take.

Process & Iterations

- Our study went through many iterations:
  - **Initial:** Have people think aloud as they are presented with a mock breach notification and then interview them
  - **Second:** Have people sign up for study and then send email from separate source about breached accounts (deception)
  - **Third:** Email people from collected pastes
  - **Final:** People sign up for study on security and we email them about their breached emails
- We ended up conducting 8 interviews with the final design
- All interview data was qualitatively coded

Breach Collection

We found participants by sending a consent form to participate to friends of friends in an older generation.

Once we received consent from participants and a list of all their current emails, we sent a breach notification with information about their personal breaches from the website “Have I Been Pwned”

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.

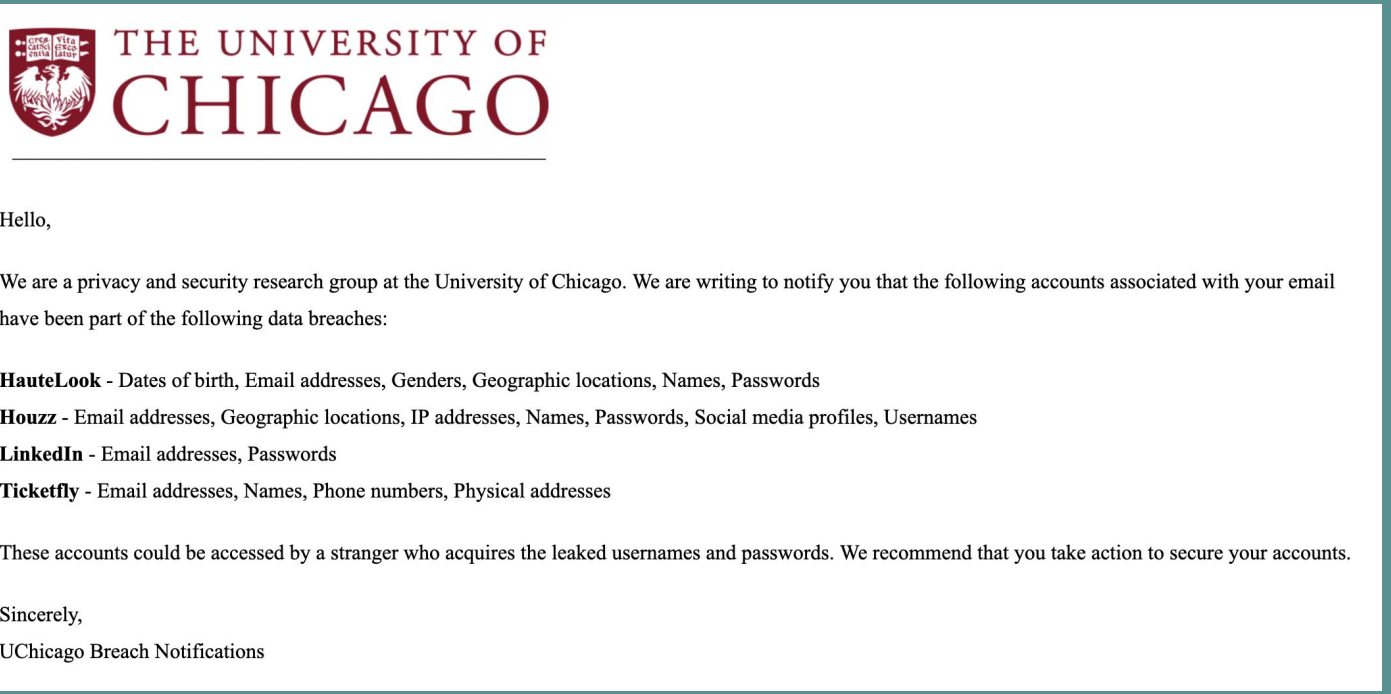
If you would like to participate, please respond to this email with a list of your current email addresses and your availability over the next couple of days. Thank you for your time and consideration.

Consent Form

Notification Design

We used A/B testing for our breach notifications. Participants were randomly sorted into either a “specific” or “less specific” notification.

- Specific: account websites and details about types of information revealed in the breach
- Less specific: account websites



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
Houzz - Email addresses, Geographic locations, IP addresses, Names, Passwords, Social media profiles, Usernames
LinkedIn - Email addresses, Passwords
Ticketfly - Email addresses, Names, Phone numbers, 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

Example of an Specific Notification

Interview Design

We performed online semi-structured interviews to ask the respondents 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

Debriefing

After completing the interview notification, we sent them a follow-up debrief that informed them as to all the information that was known to be breached and what steps they can take to further secure their information, so that they could take additional actions. We also emailed them a $5 Amazon gift card as compensation.

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:

- Houzz – Email addresses, geographic locations, IP addresses, names, passwords, social media profiles, usernames
- LinkedIn – Email addresses, password

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

Example Debrief

Ethics

- Got consent from the participants before we sent them a breach notification
- Filtered out vulnerable populations
- Only used the emails they voluntarily shared with us
- Answered questions after interviews
- Sent them a debrief with all the information that we found on Have I Been Pwned, links to useful tools for what to do after a data breach, and links to resources about staying safe online

Results

- Most participants did not know these accounts were breached
- Most participants trusted the email because it came from University / they knew they were part of a study
- Most participants remembered seeing the accounts that were breached over any other information in the email
- Most participants did nothing to protect their accounts aside from trying to log in to them again. Many waited for us to tell them what to do.

Results Cont.

- Many considered changing passwords for the accounts that were breached
- Most participants were worried about financial and identity information being stolen from data breaches
- When asked about what type of data they thought was at risk people who received informative notifications were more likely to mention the items that were listed in the notification where as people who received less informative notifications were more likely to mention general types of data

Discussion

- In designing the notification, it is important that the users receive it from a credible source
- Listing what was breached and the vulnerable information increased worry and call to action
- It is important to include what steps to take next because many of the participants didn't know what to do or waited for us to give directions
- It is especially crucial for companies that deal with financial information to send informative breach notifications with the next steps to take because these companies caused the most worry / risk for participants

Limitations

- Small sample size
- Participants were friends of friends of college students
- Notification about many accounts while usually single account in real life
- Notification comes from university rather than organization that was breached
- Participants knew they were a part of a study on data breaches and would be talking to us
- Inconsistent timing
- Inconsistent interviewer
- Variance in breached accounts
- Linked accounts

Future Research

- Repeat study with a larger number of participants and more consistent timing between notification and interview
- Have notification come from a primary source
- Focus on one data breach
- Try varying the instructions given to people
- Attempt the deception study

Interesting Mental Models and Interview Responses

- Companies selling data and advertising agencies buying the data (how the breach occurred)
- Cycling passwords
- Sharing account (thought that counted as a breach)
- Someone else signed a participant up for an account
- Worried it might happen to more important people