

Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them

Peter Mayer*, Yixin Zou*, Florian Schaub, and Adam J. Aviv



A **data breach** leaks private, sensitive, or confidential personal information to unauthorized third-parties.

Identity thieves raked in billions with your data, even as breaches fell in 2020

On Data Privacy Day, here's long after your data is stolen

INDIGNITY: REDEFINING THE HARM CAUSED BY DATA BREACHES

*George Ashenmacher**

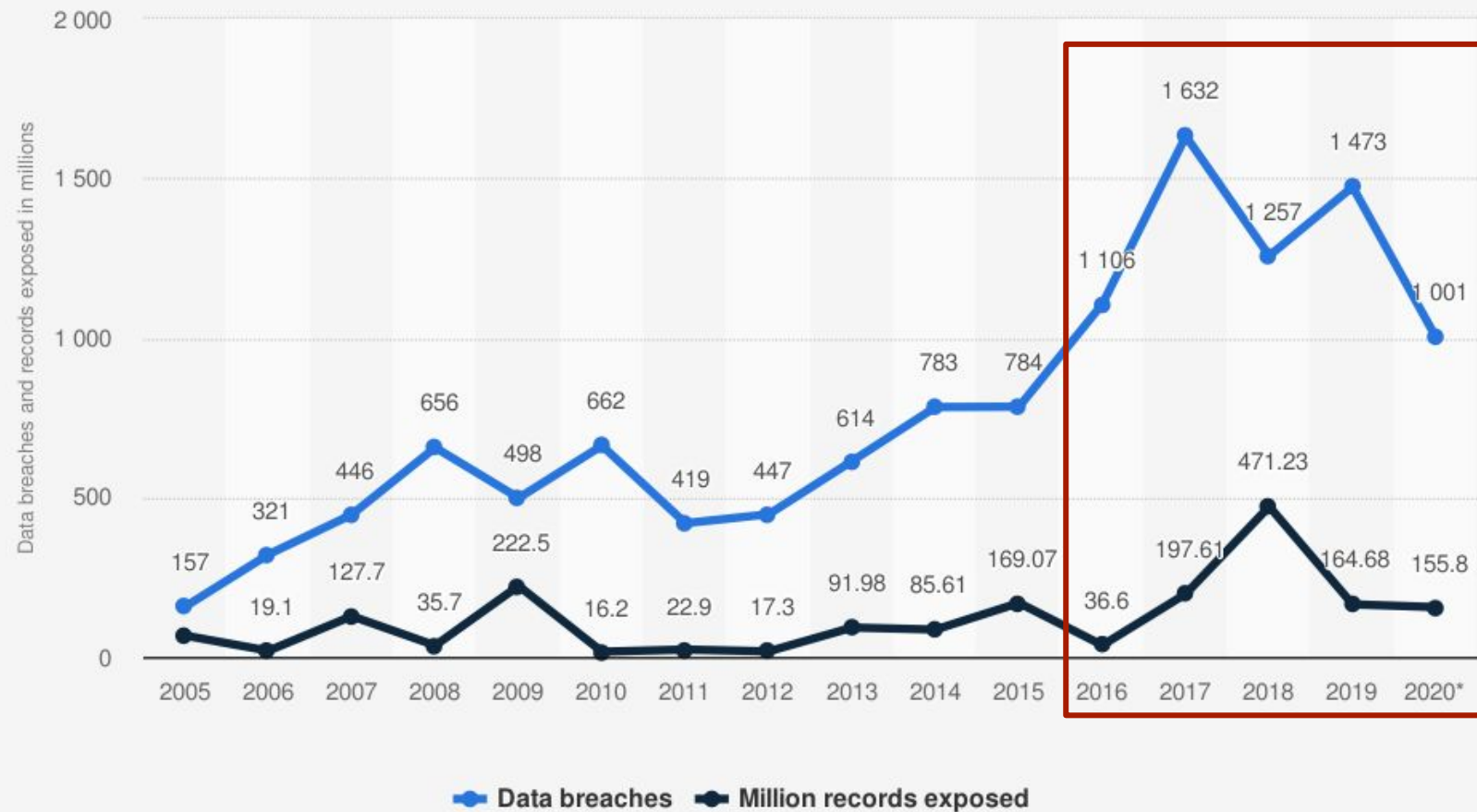
What we have been examining is one facet of man's struggle for a human dimension in a highly structured society, for dignity notwithstanding dependence.

Science has vastly complicated this elemental contest.¹

Image sources:

CNET (left),
heionline (right)

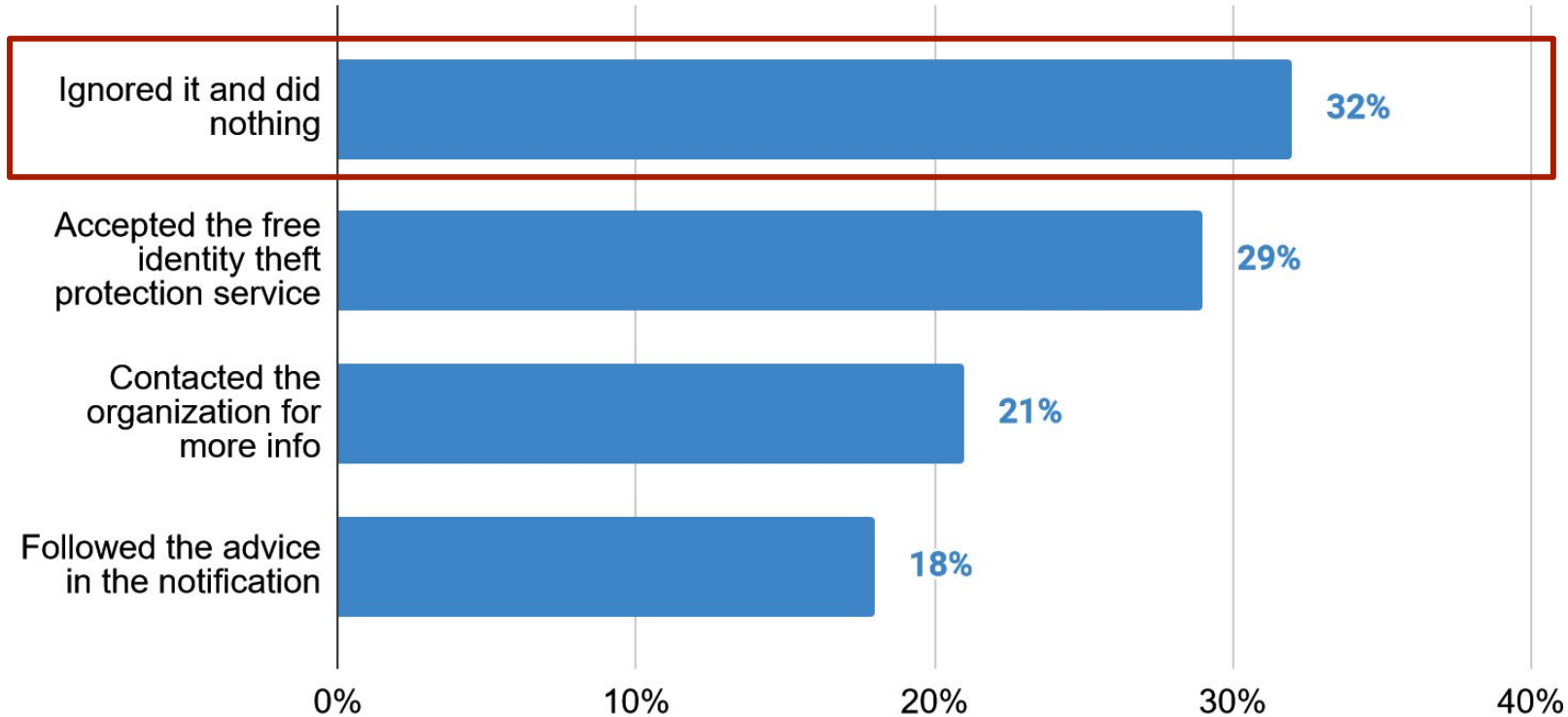
Annual number of data breaches and exposed records in the United States from 2005 to 2020 (in millions)



Data source:
Identity Theft
Resource Center

Image source:
Statista

How did you respond to the notification you received? (Ponemon Institute, 2014)



Prior work asked about **breaches in general** or intended reactions in **hypothetical scenarios**.

We examined individuals' reactions to **real-world breaches** that have **exposed their personal data**.

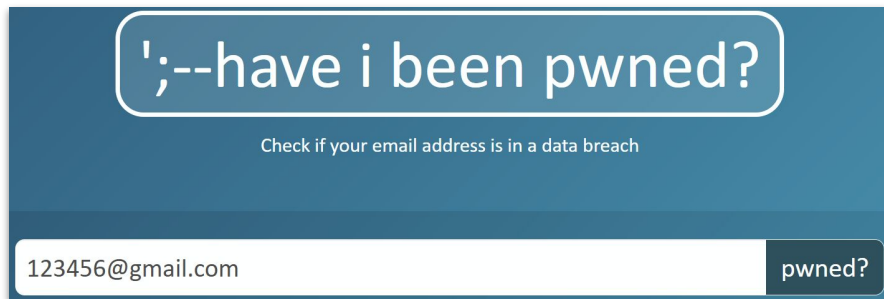


Ecologically
valid responses



Mitigate potential
recall bias

We built our own survey platform that could query the API of **Have I Been Pwned**.



';--have i been pwned?

Check if your email address is in a data breach


123456@gmail.com

pwned?



Breach 1 of 2

Your email address was part of the following breach



Kickstarter (kickstarter.com)

In February 2014, the crowdfunding platform [Kickstarter announced they'd suffered a data breach](#). The breach contained almost 5.2 million unique email addresses, usernames and salted SHA1 hashes of passwords.

Compromised data: Email addresses, Passwords

Research Questions

RQ 1 **Factors** influencing the **likelihood of exposure** to data breaches?

RQ 2 Perceptions of **causes** and **impacts** when affected by data breaches?

RQ 3 Participants' **awareness** of data breaches?

RQ 4 Participants' **emotional reactions** to data breaches?

RQ 5 Participants' **behavioral responses** to data breaches?

1

**Email-related
questions**

2

**Breach-related
questions**

3

**Demographics
and debrief**

We asked
participants to
provide their **most
commonly used
email address** for
querying HIBP.

1

Email-related
questions

2

Breach-related
questions

3

Demographics
and debrief

We asked participants to provide their **most commonly used email address** for querying HIBP.

For up to 3 breaches:

- Awareness
- Perception
- Emotional reaction
- Behavioral reaction

1

Email-related questions

We asked participants to provide their **most commonly used email address** for querying HIBP.

2

Breach-related questions

For up to 3 breaches:

- **Awareness**
- **Perception**
- **Emotional reaction**
- **Behavioral reaction**

3

Demographics and debrief

We showed a **complete list** of breaches and provided **resources** to help participants with the coping process.

What did we find?

RQ 1

Factors influencing the **likelihood of exposure** to data breaches?

RQ 1

Factors influencing the likelihood of exposure to data breaches

73%

participants had one or more data breaches.

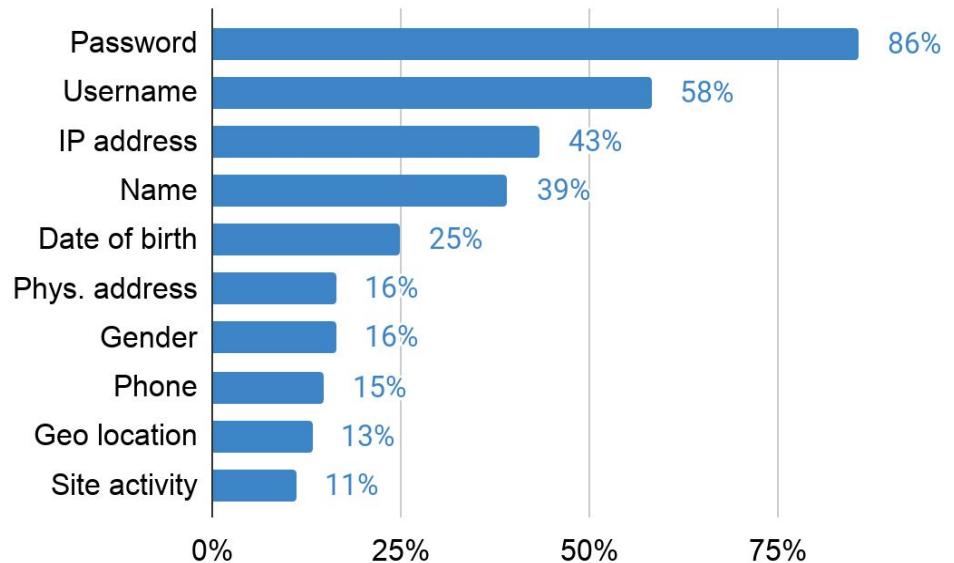
5.4

as the average number of breaches per participant.

189

unique breaches across all provided email addresses.

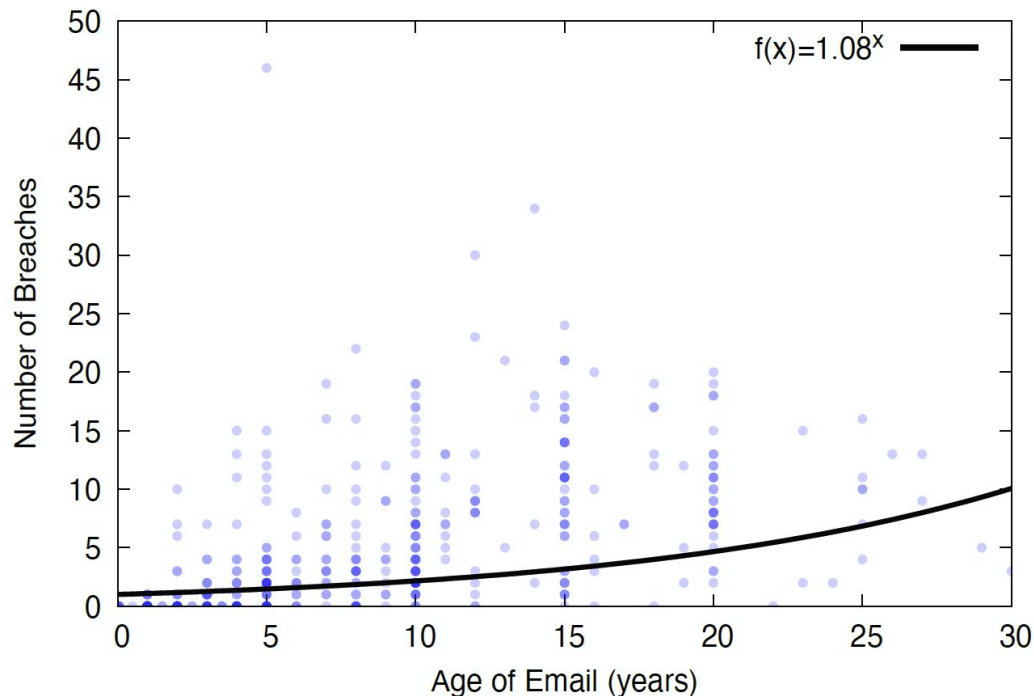
Leaked data types in our sample's breaches (n=189)



RQ 1

Factors influencing the likelihood of exposure to data breaches

The number of breaches associated with an email address **increases 8% per year of use**.



RQ 1

Factors influencing the **likelihood of exposure** to data breaches?

Exposure to breaches was **common**.
The **longer** the email was used, the more likely it was exposed.

RQ 2

Perceptions of **causes** and **impacts** when affected by data breaches?

RQ 2

Perceptions of **causes** and **impacts** when affected by data breaches

Email practices
(159; 53%)

“It’s on the website of every business I have an online relationship with.”

Insecure behaviors
(31; 10%)

“Because I was not careful with what emails I clicked.”

External factors
(42; 14%)

“These companies did not try hard enough to keep my info private.”

Self-Blame

External Blame

RQ 2

Perceptions of **causes** and **impacts** when affected by data breaches

More than half of responses assessed the breach's impact as **none (343; 43%)** or **very little (85; 11%)**.

Experienced impacts

“*I receive phone calls constantly from scam artists...It has caused me to rarely ever answer my phone.*”

Anticipated impacts

“*Not at all, just scammers occasionally attempt to access some of my older accounts that hold no sensitive information.*”

RQ 2

Perceptions of **causes** and **impacts** when affected by data breaches?

Most participants **blamed themselves** for being affected, and thought the breach **would not impact** them.

RQ 3

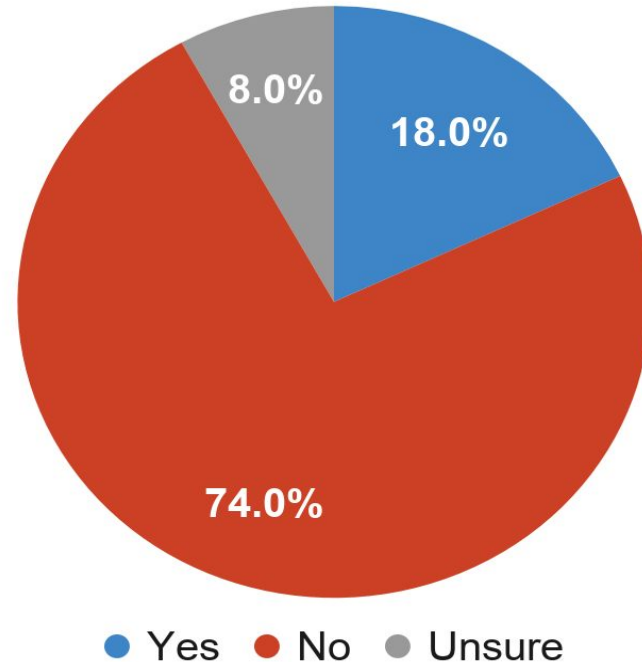
Participants' **awareness** of data breaches?

RQ 3

Participants' **awareness** of data breaches

“Prior to this study, were you aware that you are affected by this breach?”

(n=792)



RQ 3

Participants' **awareness** of data breaches?

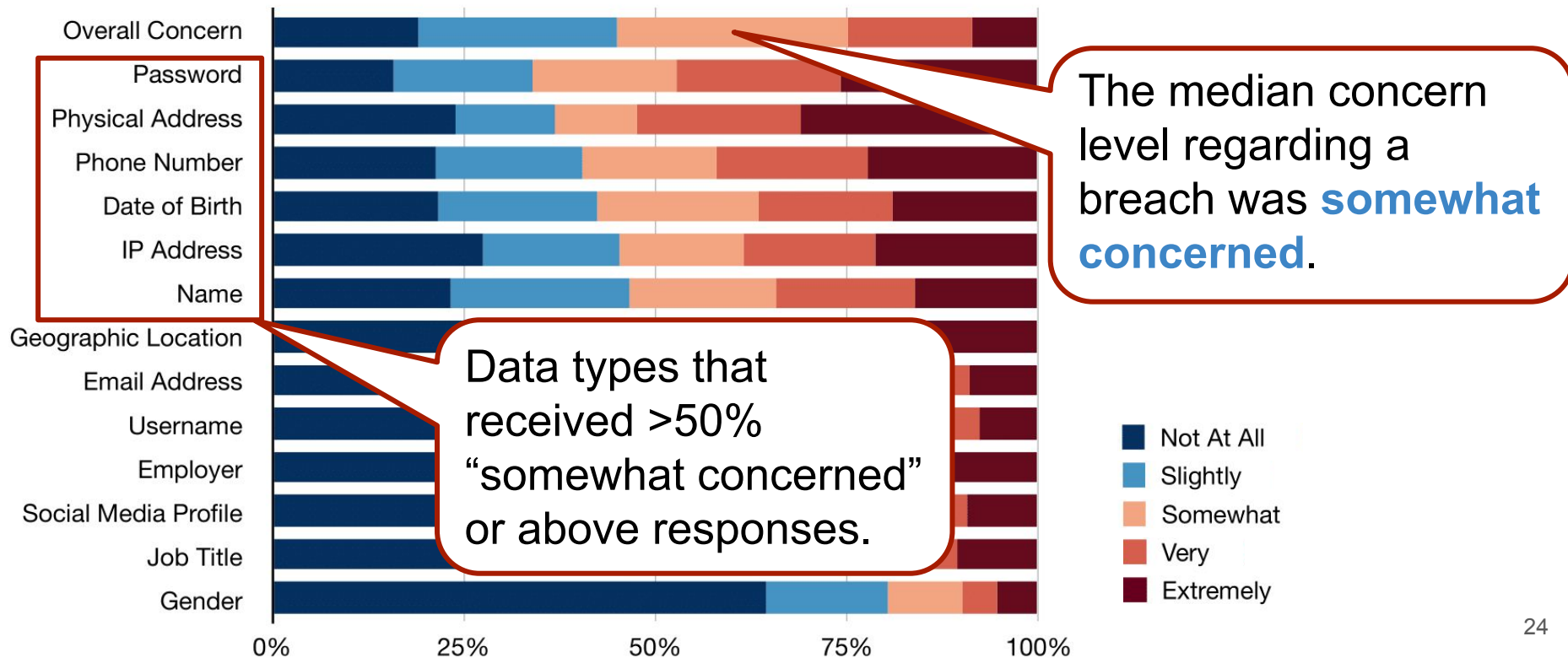
Participants were **unaware** of most breaches displayed to them.

RQ 4

Participants' **emotional reactions** to data breaches?

RQ 4

Participants' **emotional reactions** to data breaches



RQ 4

Participants' **emotional reactions** to data breaches?

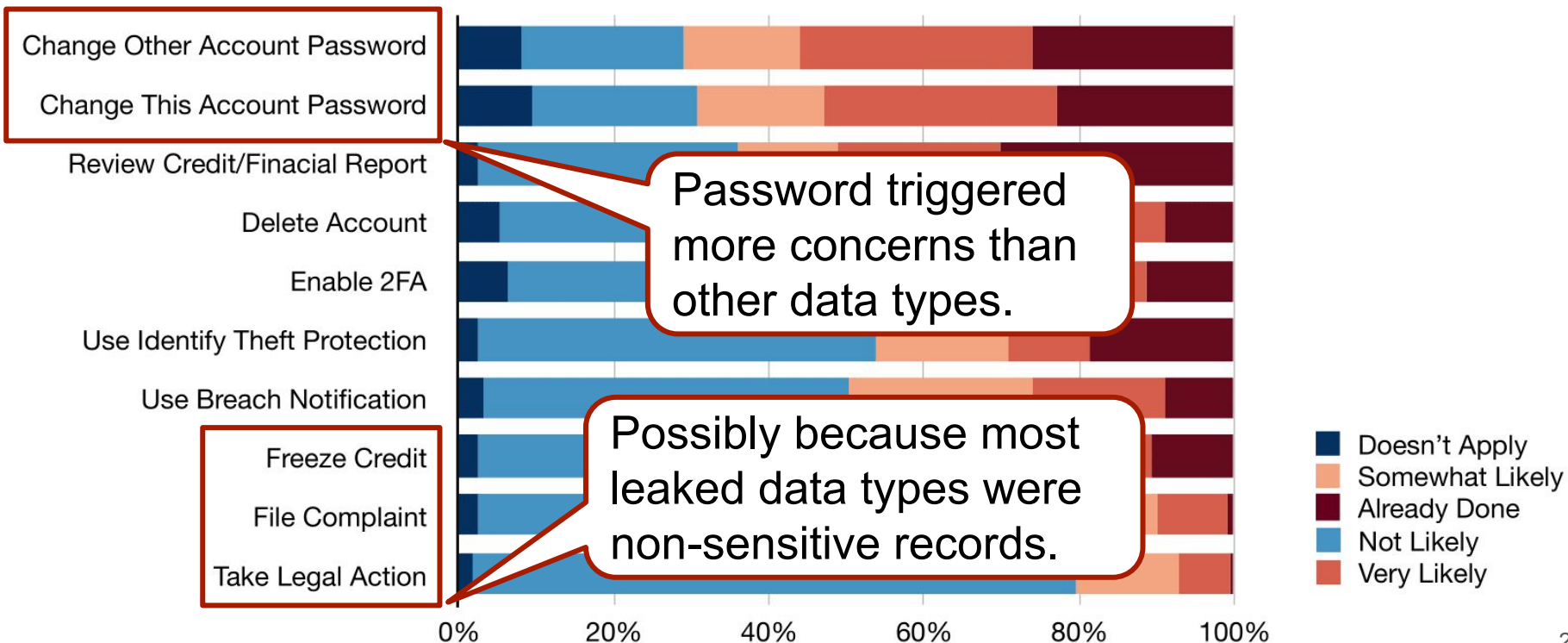
Overall **concern level** remained **low**; more concern about exposed password, physical address, and phone number.

RQ 5

Participants' **behavioral responses** to data breaches?

RQ 5

Participants' **behavioral responses** to data breaches



RQ 5

Participants' **behavioral responses** to data breaches

For a one-unit increase on a 5-point scale, the odds of having taken action increased by 2.2.

	Est.	OR	95% CI	p-value
(Intercept)	-3.27	0.04	[0.002, 0.61]	.02
Awareness yes (vs. no)	5.97	390.48	[45.72, 3334.79]	< 0.001
Breach age years	-0.03	0.97	[0.77, 1.21]	.77
Num. of types numeric	.12	1.13	[0.85, 1.50]	.39
Password yes (vs. no)	-0.18	0.84	[0.18, 3.79]	.82
Physical Addr. yes (vs. no)	-0.26	0.77	[0.16, 3.71]	.75
Phone Num. yes (vs. no)	-0.29	0.75	[0.19, 3.02]	.69
Date of birth yes (vs. no)	-0.24	0.79	[0.17, 3.62]	.76
IP Addr. yes (vs. no)	-0.20	0.82	[0.26, 2.64]	.74
Name yes (vs. no)	-0.19	0.83	[0.21, 3.22]	.79
Concern numeric	0.80	2.22	[1.28, 3.86]	.005

To react to a data breach, one need to be aware of the breach.

Logistic regression on having taken any of the ten provided actions (yes vs. no).

RQ 5

Participants' **behavioral responses** to data breaches?

Changing passwords was more popular than other actions. **Prior awareness** and **higher concern** were **key motivators**.

Summary of Results

We surveyed (n=413) individuals' **awareness**, **perception**, and **responses** to specific breaches that affected them.

- ➡ Exposure to breaches **increases** as an email address gets used **for a longer time**.
- ➡ Participants were **unaware of most breaches** displayed to them.
- ➡ Most participants **blamed themselves** for being affected, and thought the breach **would not impact** them.
- ➡ Participants' overall concern level **remained low**, yet **awareness** and **concern** were key motivators of **taking action**.

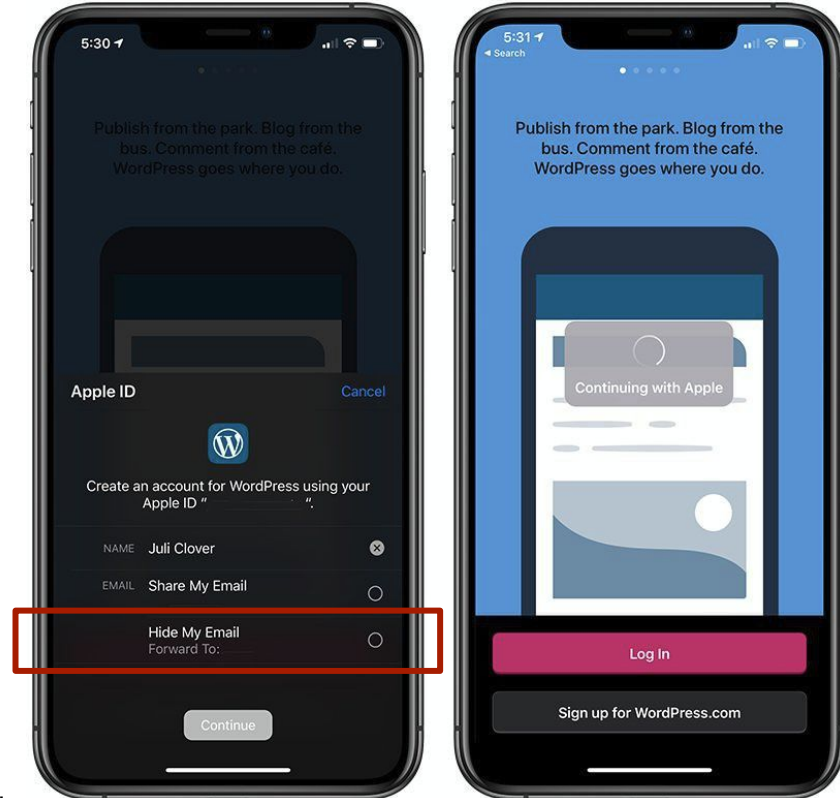
**What are the
implications?**

Tools to help consumers react to breaches

As an email gets used **longer**, the email address becomes **more likely to appear in data breaches**.



Promote tools that automate the creation of **unique email aliases**.

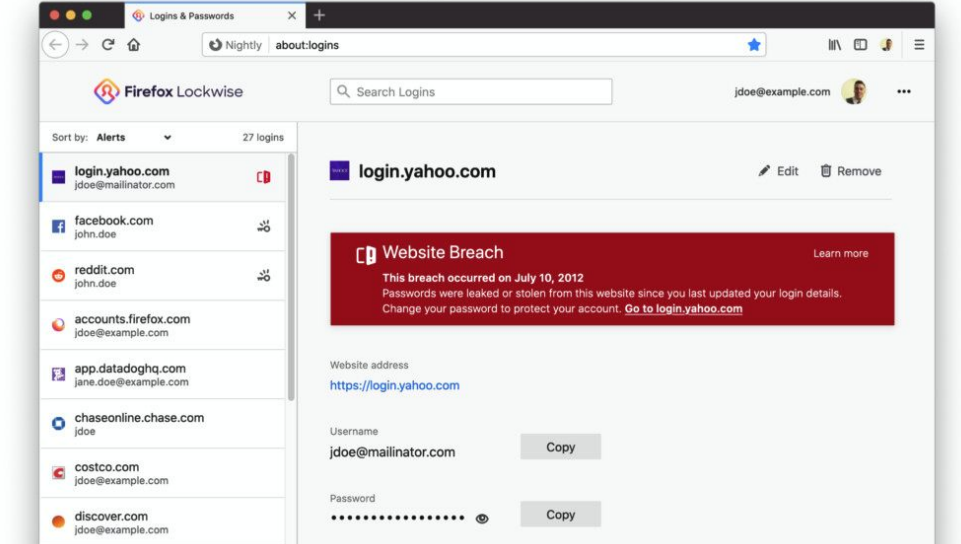


Tools to help consumers react to breaches

74% of shown breaches were new to participants.



Use **in-situ methods** to notify consumers of breaches.



Increase responsibility of breached companies

Set stricter requirements for **notifying affected consumers**.

GDPR Art. 34:

When the personal data breach is likely to **result in a high risk** to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

Mandate notifications **for all breaches** considering harms in legal terms.



Deliver notifications via **multiple channels**.



Make sure notifications are **understandable** and **usable**.

Increase responsibility of breached companies

Require companies to be more involved in helping consumers **recover from breaches**.

WHAT YOU CAN DO

We are offering a complimentary one-year membership of Experian's® IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides identity protection services focused on identification and resolution of identity theft. IdentityWorksSM Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorksSM Credit 3B, including instructions on how to activate the complimentary one-year membership, please see the additional information provided with this letter.



How about providing tools such as email alias generators or password managers?

Peter Mayer
peter.mayer@kit.edu

Yixin Zou
yixinz@umich.edu

Florian Schaub
fschaub@umich.edu

Adam J. Aviv
aaviv@gwu.edu

- ➔ Exposure to breaches **increases** as an email address gets used **for a longer time**.
- ➔ Participants were **unaware of most breaches** displayed to them.
- ➔ Most participants **blamed themselves** for being affected, and thought the breach **would not impact** them.
- ➔ Participants' overall concern level **remained low**, yet **awareness** and **concern** were key motivators of **taking action**.

