CNIL Privacy Research Day | June 4, 2024

Nudging Users to Change Breached Passwords Using the Protection Motivation Theory

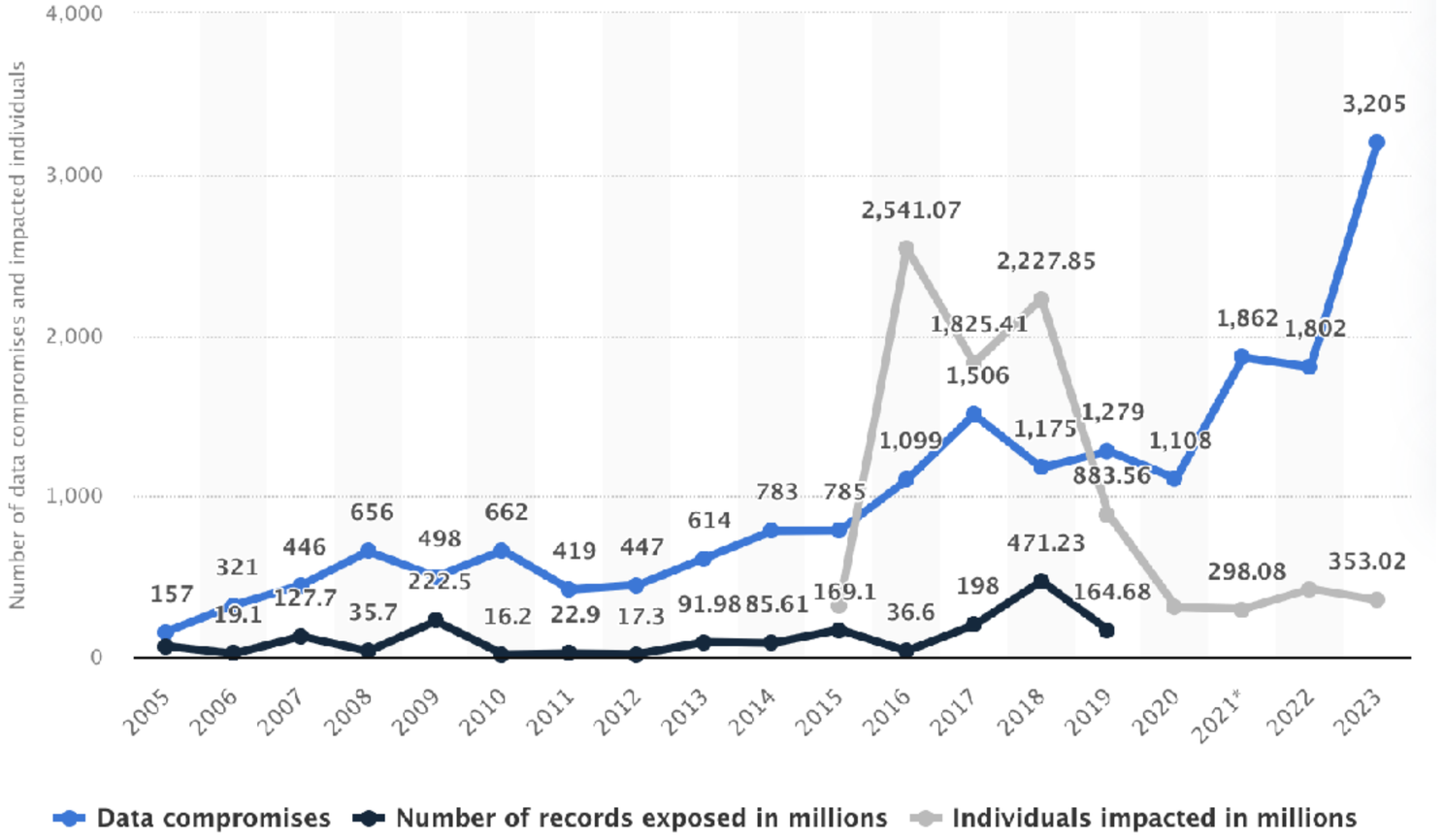
Yixin Zou
Tenure-Track Faculty, MPI-SP

MAX PLANCK INSTITUTE
FOR SECURITY AND PRIVACY

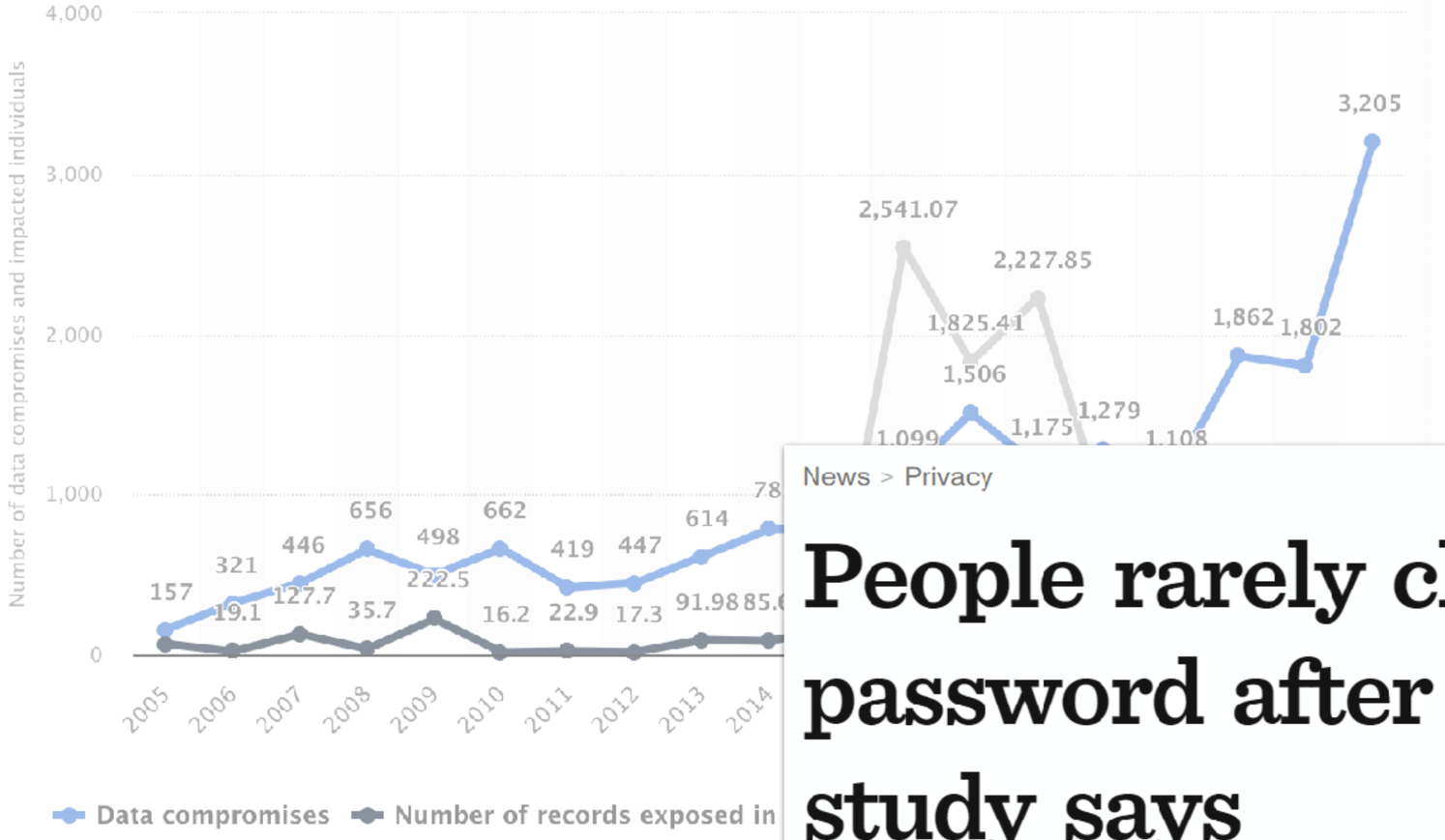
Human-Centered Privacy and Security

Human-Centered Privacy and Security

 data breaches



data source: Identity Theft Resource Center; image source: Statista



News > Privacy

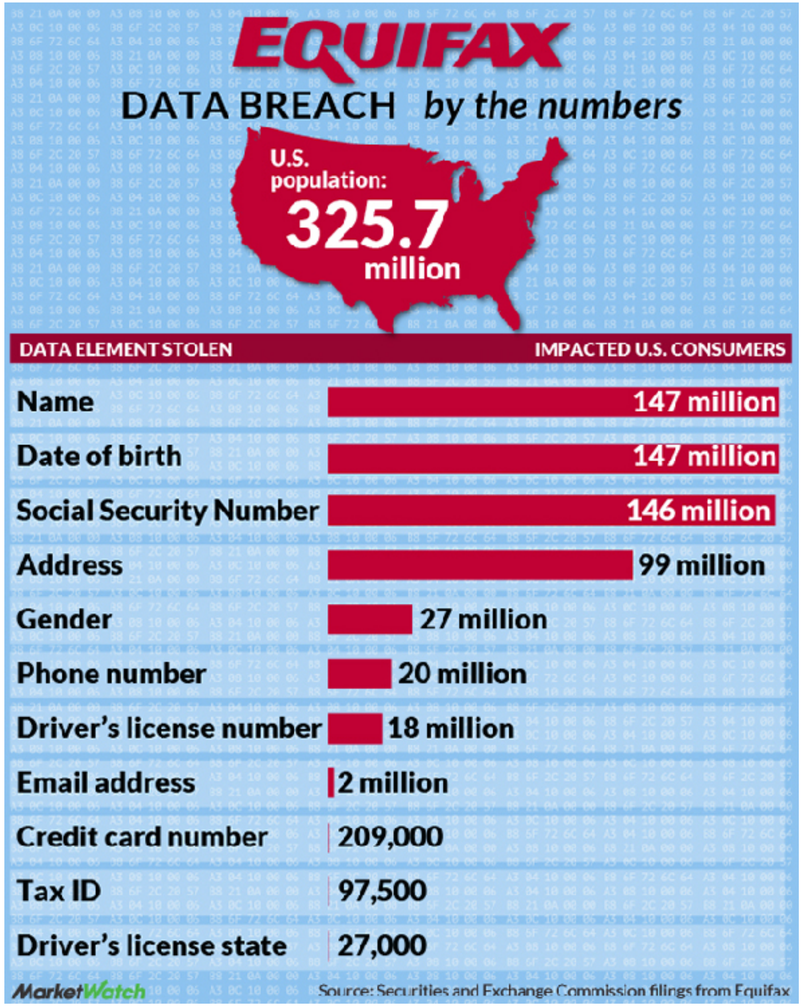
People rarely change their password after a data breach, study says

Just one-third of users took action following breach announcements, according to new research from Carnegie Mellon University.

Reasons behind inaction

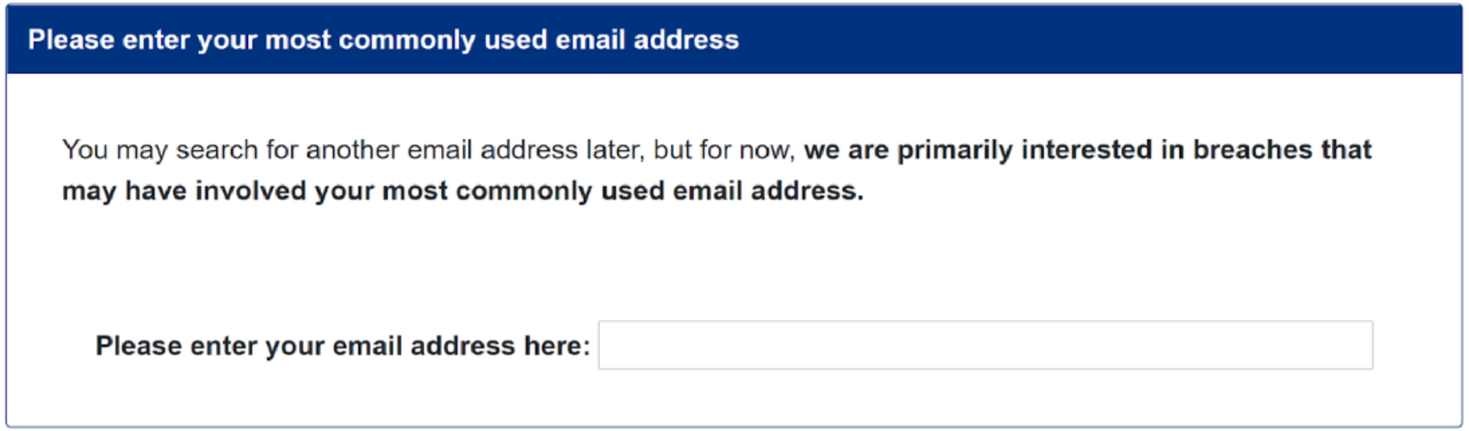
Semi-structured interviews (n=24)

- Optimism bias
- Reactive attitude toward risks
- Misconceptions about protective measures
- Financial costs



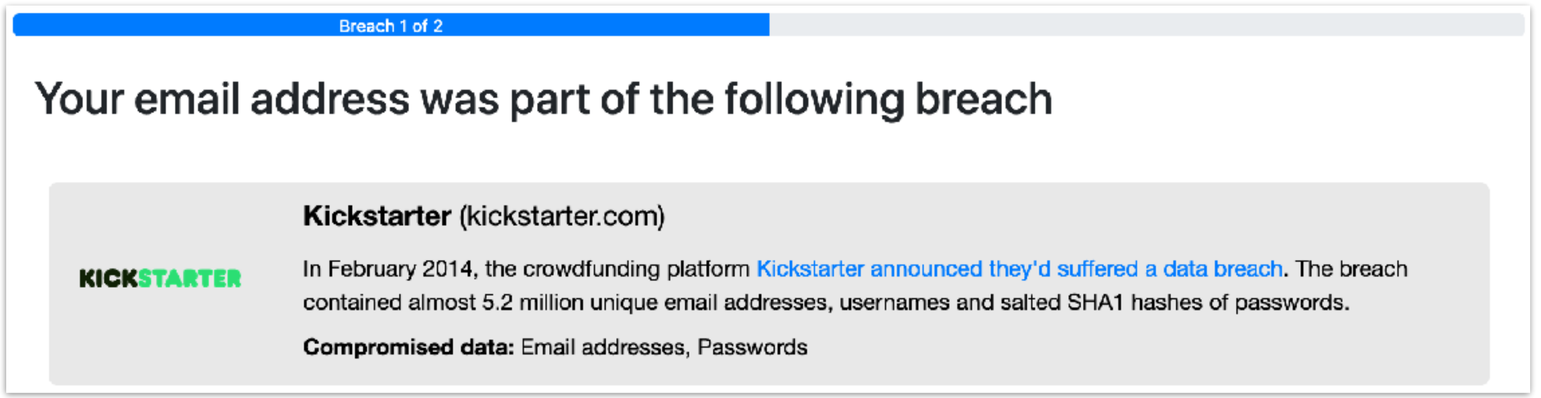
"I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions After the Equifax Data Breach
Yixin Zou, Abraham H. Mhaidli, Austin McCall, Florian Schaub
SOUPS: Symposium on Usable Privacy and Security. 2018. *Distinguished Paper Award* 🏆

Study breach reactions at scale



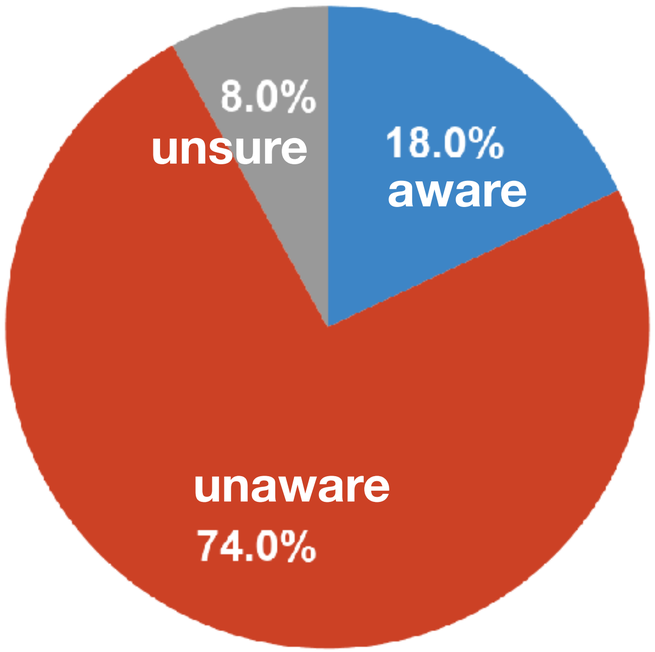
Online survey (n=413)

Real-world breaches affecting participants themselves

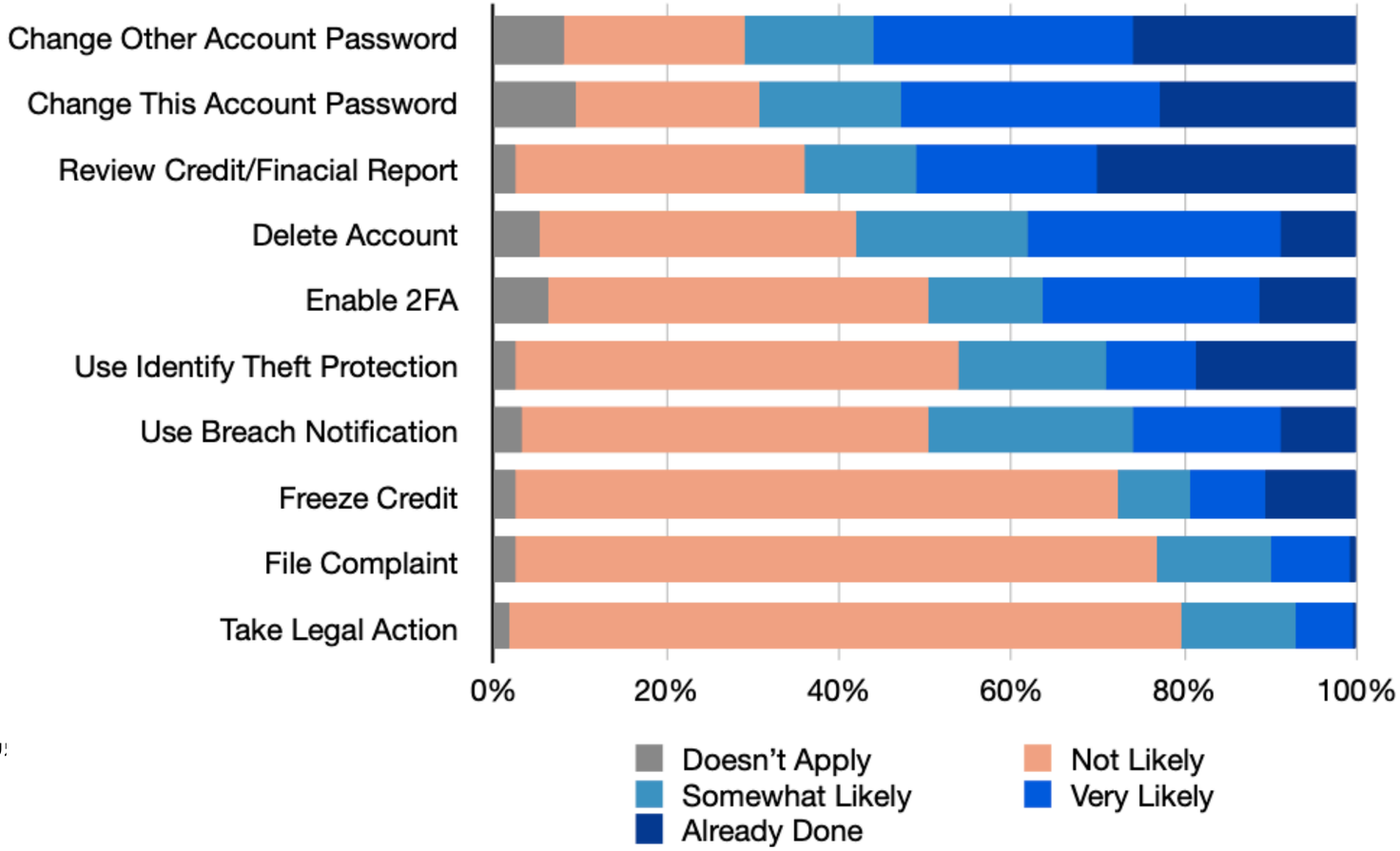


"Now I'm a bit angry:" Individuals' Awareness, Perception, and Responses to Data Breaches
Peter Mayer*, Yixin Zou*, Florian Schaub, Adam J. Aviv (*equal contributions)
USENIX Security Symposium. 2020.

Low awareness, limited action



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



"Now I'm a bit angry:" Individuals' Awareness, Perception, and Responses to Data Breaches
Peter Mayer*, Yixin Zou*, Florian Schaub, Adam J. Aviv (*equal contributions)
USENIX Security Symposium. 2020.

Let's look at breach notifications

Dear <<First Name>> <<Last Name>>,

This letter is to provide you with information about a data security incident that may have affected your payment card information. The privacy and security of your personal information is extremely important to us as we very much appreciate your business and your confidence in us. We are sending this letter to notify you of the incident, to provide you with information about the nature of the incident, and the steps you can now take to protect your personal information.

What Happened. On October 15, 2021, <<Entity>> Warehouse, LLC ("<<Entity>> Warehouse") we became aware of a potential data security incident. We immediately began an internal investigation and engaged an independent computer forensics firm to determine whether any personal information was affected in the incident. The investigation has been extensive, requiring the analysis of a substantial amount of digital evidence. On November 6, 2021, the investigation determined that payment card information was obtained without authorization on October 1, 2021. On November 29, 2021, the investigation determined that your payment card information may have been affected during the incident.

What Information Was Involved. The incident may have involved payment card information, including your name, address, payment card number <<Last 4 Digits>> , expiration date, and payment card security code.

image source: Maryland Attorney General

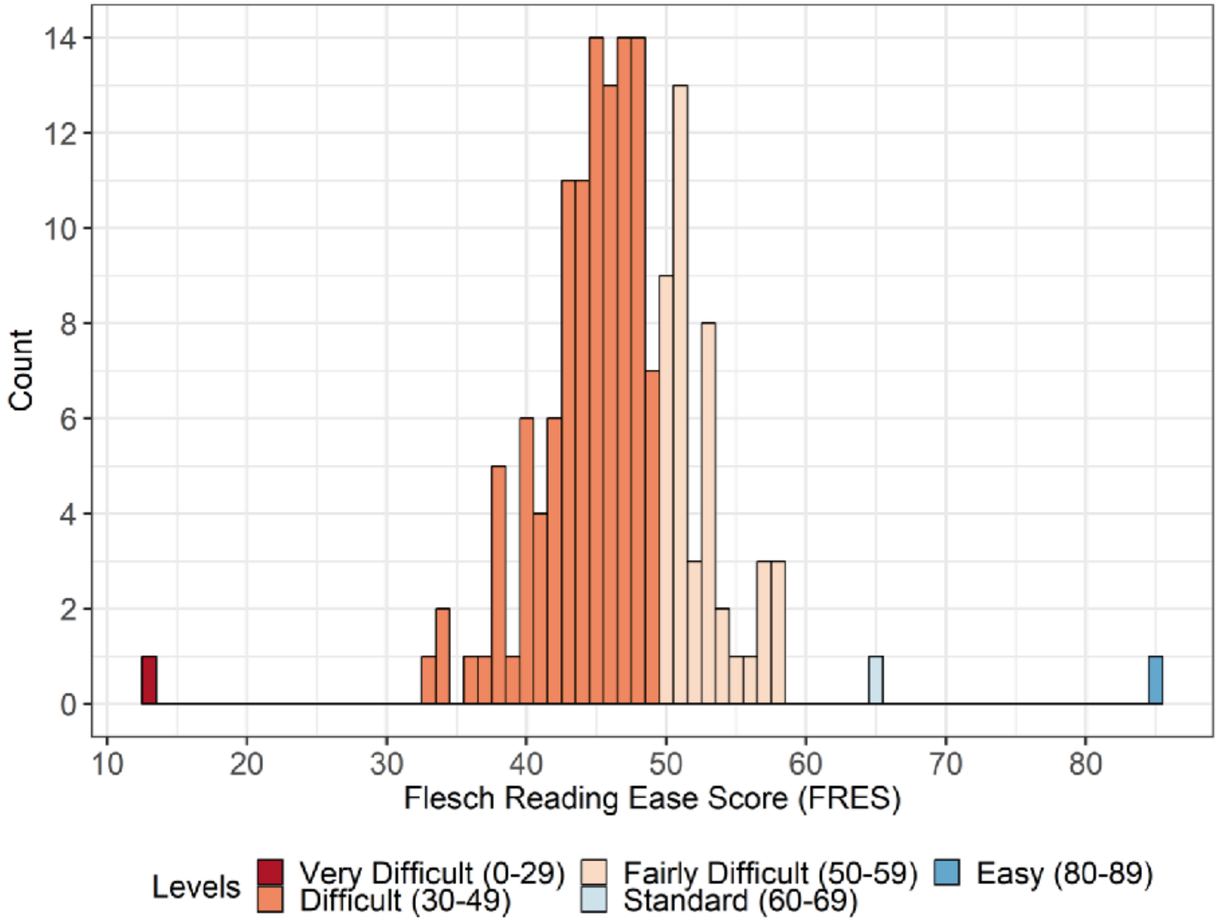
Issues with breach notifications

Content analysis (n=161)

Poor readability

Using hedging terms

Suggesting many
actions with no priority



You 'Might' Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications
Yixin Zou, Shawn Danino, Kaiwen Sun, Florian Schaub
CHI: ACM Conference on Human Factors in Computing Systems. 2019.

Issues with breach notifications

Content analysis (n=161)

Poor readability

Using hedging terms

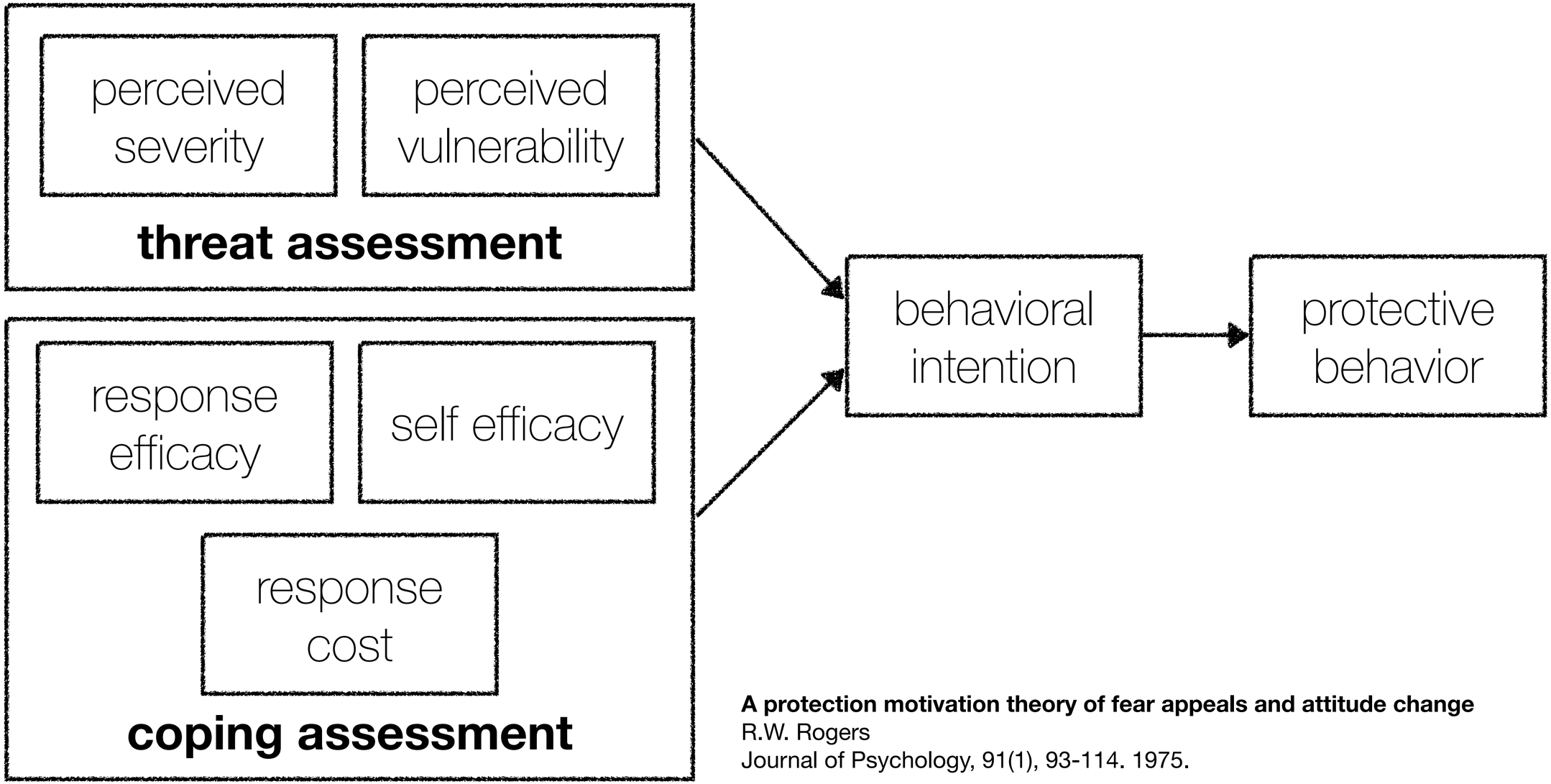
Suggesting many
actions with no priority

We need stronger data breach notification laws!

cfpb Consumer Financial Protection Bureau

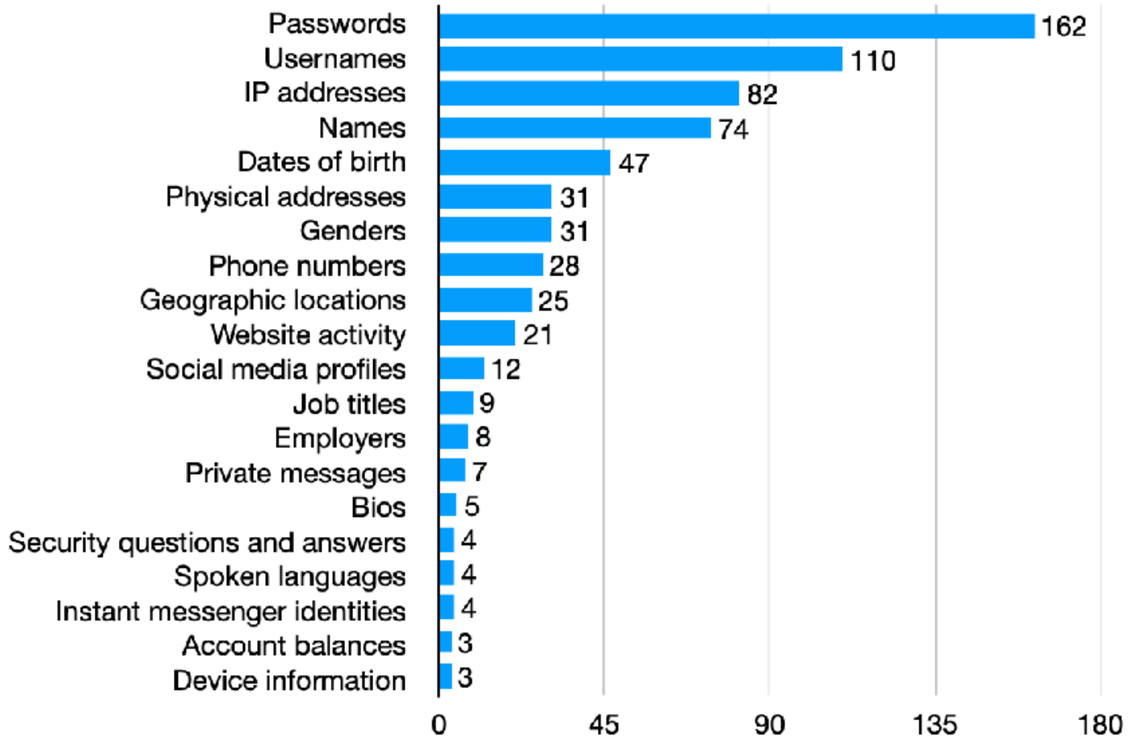
You ‘Might’ Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications
Yixin Zou, Shawn Danino, Kaiwen Sun, Florian Schaub
CHI: ACM Conference on Human Factors in Computing Systems. 2019.

Protection Motivation Theory

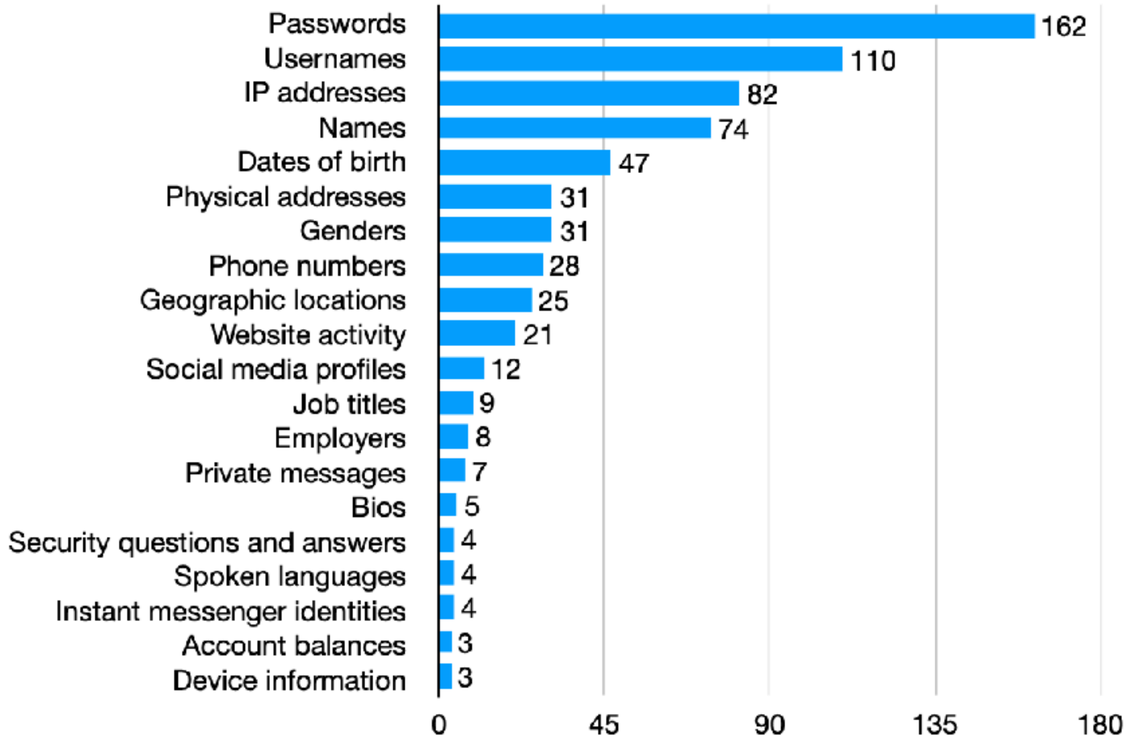


A protection motivation theory of fear appeals and attitude change
R.W. Rogers
Journal of Psychology, 91(1), 93-114. 1975.

Focus on breached passwords



Focus on breached passwords



We recommend that you change the password for your Appen account.

Appen

www.appen.com

Website Breach

Overview

In June 2020, the AI training data company Appen suffered a data breach exposing the details of almost 5.9 million users which were subsequently sold online. Included in the breach were names, email addresses and passwords stored as bcrypt hashes. Some records also contained phone numbers, employers and IP addresses. The data was provided to HIBP by dehashed.com.

What data was compromised

Passwords

Additional Information: Email addresses, Employers, IP addresses, Names, Phone numbers

What to do

Change the password for your Appen account **now**.

Design breach notifications from PMT

What are the risks ▼

- Criminals may access your account to steal your personal information, impersonate you, or make fraudulent purchases in your name.
- If you used the same password elsewhere, criminals may take over your other accounts too.
- Criminals use automated programs to test compromised passwords on hundreds of accounts in just a few seconds. **You're at risk regardless of whether you are a promising target or not.**
- Once your password is out there, criminals may try to take over your account **anytime after a breach, no matter how long ago the breach happened.**

How to change your password ▼

Changing your Appen account password would prevent criminals from using the breached password to access your account. **It only takes a few minutes.** Just follow these easy steps:

1. Go to www.appen.com and log into your account.
Unsure if you have a Appen account or can't log into it? Contact Appen to recover the account or have your account deleted. You can usually find contact information in the privacy policy.

2. Create a unique and strong password in account settings.
Longer passwords are best. Do not reuse the same password for other accounts. Check out **this guideline** for more do's and don'ts about passwords.

3. You're all set!
If you used your old password for other accounts, make sure to change your password for those accounts too.

Design breach notifications from PMT

threat nudge

What are the risks ▼

- Criminals may access your account to steal your personal information, impersonate you, or make fraudulent purchases in your name.
- If you used the same password elsewhere, criminals may take over your other accounts too.
- Criminals use automated programs to test compromised passwords on hundreds of accounts in just a few seconds. **You're at risk regardless of whether you are a promising target or not.**
- Once your password is out there, criminals may try to take over your account **anytime after a breach, no matter how long ago the breach happened.**

How to change your password ▼

Changing your Appen account password would prevent criminals from using the breached password to access your account. **It only takes a few minutes.** Just follow these easy steps:

1. Go to www.appen.com and log into your account.
Unsure if you have a Appen account or can't log into it? Contact Appen to recover the account or have your account deleted. You can usually find contact information in the privacy policy.

2. Create a unique and strong password in account settings.
Longer passwords are best. Do not reuse the same password for other accounts. Check out **this guideline** for more do's and don'ts about passwords.

3. You're all set!
If you used your old password for other accounts, make sure to change your password for those accounts too.

Design breach notifications from PMT

threat nudge

What are the risks ▼

- Criminals may access your account to steal your personal information, impersonate you, or make fraudulent purchases in your name.
- If you used the same password elsewhere, criminals may take over your other accounts too.
- Criminals use automated programs to test compromised passwords on hundreds of accounts in just a few seconds. **You're at risk regardless of whether you are a promising target or not.**
- Once your password is out there, criminals may try to take over your account **anytime after a breach, no matter how long ago the breach happened.**

coping nudge

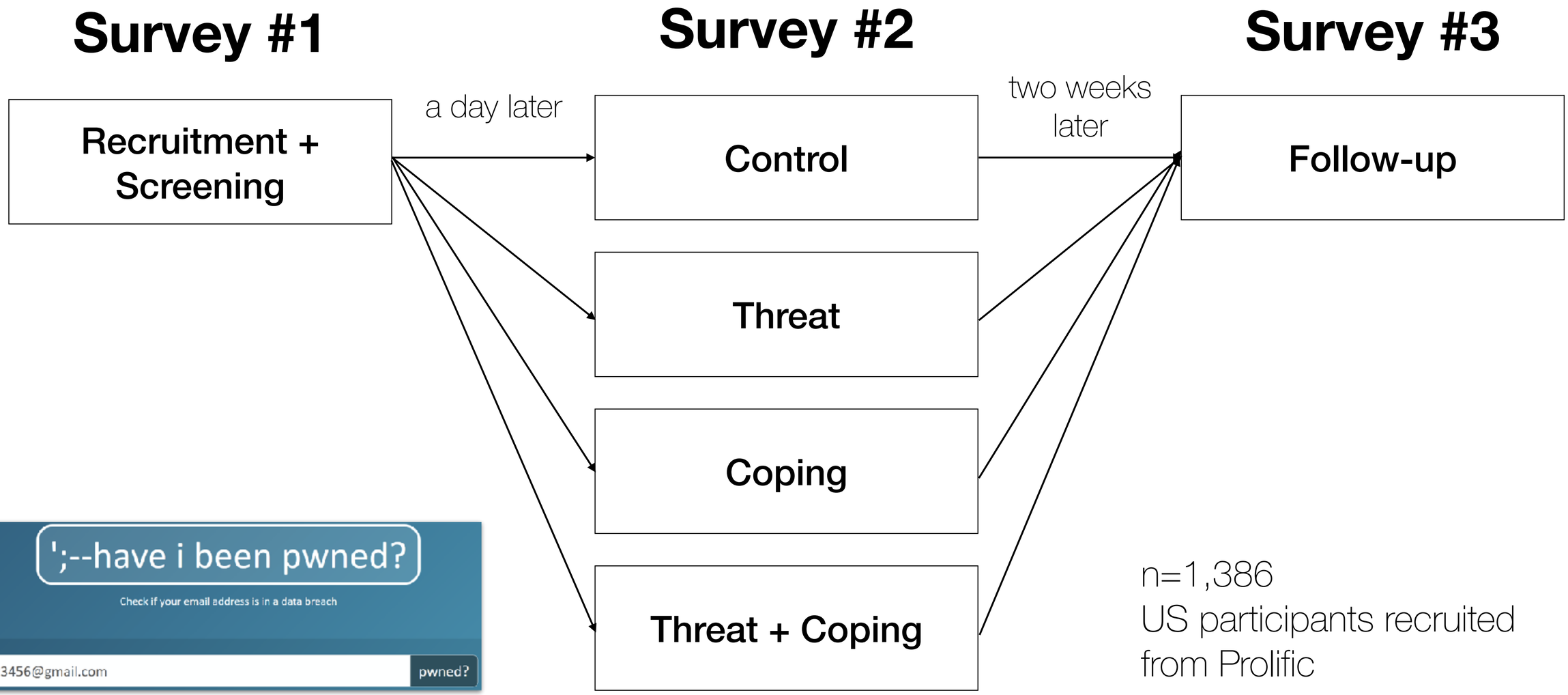
How to change your password ▼

Changing your Appen account password would prevent criminals from using the breached password to access your account. **It only takes a few minutes.** Just follow these easy steps:

1. Go to www.appen.com and log into your account.
Unsure if you have a Appen account or can't log into it? Contact Appen to recover the account or have your account deleted. You can usually find contact information in the privacy policy.

2. Create a unique and strong password in account settings.
Longer passwords are best. Do not reuse the same password for other accounts. Check out **this guideline** for more do's and don'ts about passwords.

3. You're all set!
If you used your old password for other accounts, make sure to change your password for those accounts too.



n=1,386
US participants recruited from Prolific

Comparisons between conditions

Conditions	% w/ intention	OR	p-value
Threat only vs. Control	67.3% vs. 58.2%	1.48	.02
Coping only vs. Control	62.9% vs. 58.2%	1.22	.23
Combined vs. Control	62.3% vs. 58.2%	1.19	.30

Conditions	% w/ action	OR	p-value
Threat only vs. Control	28.0% vs. 22.7%	1.32	.14
Coping only vs. Control	27.0% vs. 22.7%	1.26	.23
Combined vs. Control	31.1% vs. 22.7%	1.54	.02

threat nudge alone can motivate intention

both threat and coping nudges needed for motivating action

An intention-behavior gap

Conditions	% w/ intention	OR	p-value
Threat only vs. Control	67.3% vs. 58.2%	1.48	.02
Coping only vs. Control	62.9% vs. 58.2%	1.22	.23
Combined vs. Control	62.3% vs. 58.2%	1.19	.30

58-67% showed intention

Conditions	% w/ action	OR	p-value
Threat only vs. Control	28.0% vs. 22.7%	1.32	.14
Coping only vs. Control	27.0% vs. 22.7%	1.26	.23
Combined vs. Control	31.1% vs. 22.7%	1.54	.02

22-31% changed the password

The “why” behind the intention-behavior gap

Password Change: Yes	Count
to be safe	319
bad things	284
take other actions	222
triggered by breach	140
inactive use	123

Password Change: No	Count
inactive use	471
no account	321
no sensitive info	166
take other actions	120
unimportant account	109

The “why” behind the intention-behavior gap

Password Change: Yes	Count
to be safe	319
bad things	284
take other actions	222
triggered by breach	140
inactive use	123

Password Change: No	Count
inactive use	471
no account	321
no sensitive info	166
take other actions	120
unimportant account	109

“This account isn’t important, and I’m pretty sure I haven’t logged into it in almost a decade.

The information contained in it would be minimal since I never really shared personal details or provided accurate information to websites for certain questions.”

The “why” behind the intention-behavior gap

Password Change: Yes	Count
to be safe	319
bad things	284
take other actions	222
triggered by breach	140
inactive use	123

Password Change: No	Count
inactive use	471
no account	321
no sensitive info	166
take other actions	120
unimportant account	109

“When I tried to reset my password, the email never came.

Maybe these sites had bought my information somehow from some other place, and therefore were able to obtain a username/email and password from me despite me never opening an account with them directly.”

Other factors also matter

	B (SE)	OR	95% CI	p-value
(Intercept)	−2.88(0.59)	0.06	[0.02, 0.18]	< .001
Condition: coping (vs. control)	0.28(0.24)	1.32	[0.83, 2.11]	.24
Condition: threat (vs. control)	0.61(0.24)	1.84	[1.15, 2.95]	.01
Condition: combined (vs. control)	0.28(0.29)	1.32	[0.82, 2.17]	.25
Account exist: yes (vs. no)	−0.15(0.32)	0.86	[0.45, 1.60]	.63
Account exist: yes (vs. no)	−0.28(0.30)	0.75	[0.42, 1.37]	.35
Aware account: yes (vs. no)	0.50(0.35)	1.64	[0.82, 3.29]	.16
Aware account: unsure (vs. no)	0.15(0.34)	1.17	[0.59, 2.28]	.65
Password reuse: yes (vs. no)	1.10(0.31)	3.01	[1.66, 5.69]	< .001
Password reuse: unsure (vs. no)	0.60(0.19)	1.82	[1.25, 2.67]	.002
Security attitudes (5-point scale)	0.65(0.10)	1.92	[1.58, 2.34]	< .001

whether the breached password was reused elsewhere (for intention)

Other factors also matter

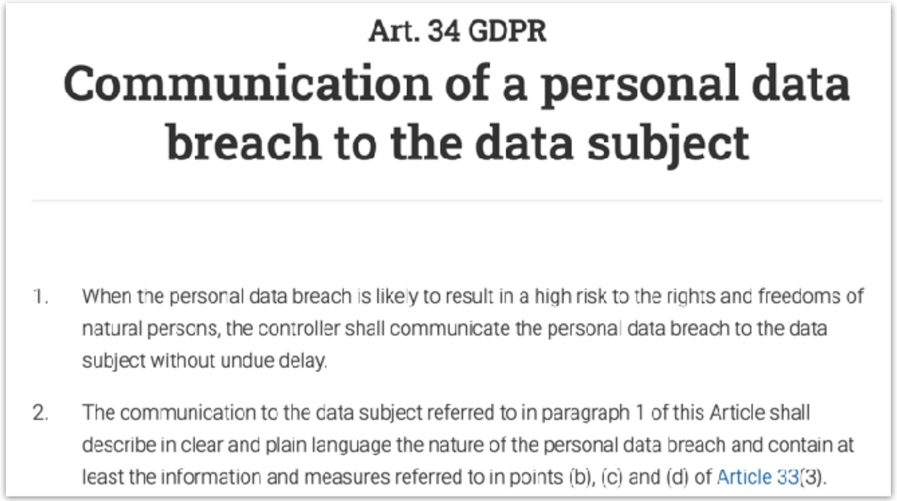
	B (SE)	OR	95% CI	p-value
(Intercept)	−2.88(0.59)	0.06	[0.02, 0.18]	< .001
Condition: coping (vs. control)	0.28(0.24)	1.32	[0.83, 2.11]	.24
Condition: threat (vs. control)	0.61(0.24)	1.84	[1.15, 2.95]	.01
Condition: combined (vs. control)	0.28(0.29)	1.32	[0.82, 2.17]	.25
Account exist: yes (vs. no)	−0.15(0.32)	0.86	[0.45, 1.60]	.63
Account exist: yes (vs. no)	−0.28(0.30)	0.75	[0.42, 1.37]	.35
Aware account: yes (vs. no)	0.50(0.35)	1.64	[0.82, 3.29]	.16
Aware account: unsure (vs. no)	0.15(0.34)	1.17	[0.59, 2.28]	.65
Password reuse: yes (vs. no)	1.10(0.31)	3.01	[1.66, 5.69]	< .001
Password reuse: unsure (vs. no)	0.60(0.19)	1.82	[1.25, 2.67]	.002
Security attitudes (5-point scale)	0.65(0.10)	1.92	[1.58, 2.34]	< .001

whether the breached password was reused elsewhere (for intention)

	B (SE)	OR	95% CI	p-value
(Intercept)	−3.46(0.77)	0.03	[0.01, 0.14]	< .001
Condition: coping (vs. control)	0.42(0.30)	1.52	[0.85, 2.75]	.16
Condition: threat (vs. control)	0.50(0.28)	1.66	[0.96, 2.89]	.07
Condition: combined (vs. control)	0.86(0.31)	2.37	[1.30, 4.36]	.005
Aware site: yes (vs. no)	0.29(0.39)	1.34	[0.63, 2.91]	.46
Aware breach: yes (vs. no)	0.47(0.35)	1.60	[0.79, 3.20]	.19
Account exist: yes (vs. no)	0.16(0.43)	1.17	[0.50, 2.78]	.72
Account exist: unsure (vs. no)	0.03(0.42)	1.03	[0.45, 2.39]	.94
Password reuse: yes (vs. no)	−0.37(0.32)	0.69	[0.37, 1.28]	.24
Password reuse: unsure (vs. no)	−0.22(0.23)	0.81	[0.51, 1.26]	.35
Security attitudes (5-point scale)	0.27(0.12)	1.31	[1.03, 1.67]	.03

a more proactive attitude toward security in general (for action)

Incorporate PMT-based nudges in practice



Art. 34 GDPR

Communication of a personal data breach to the data subject

1. 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.
2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

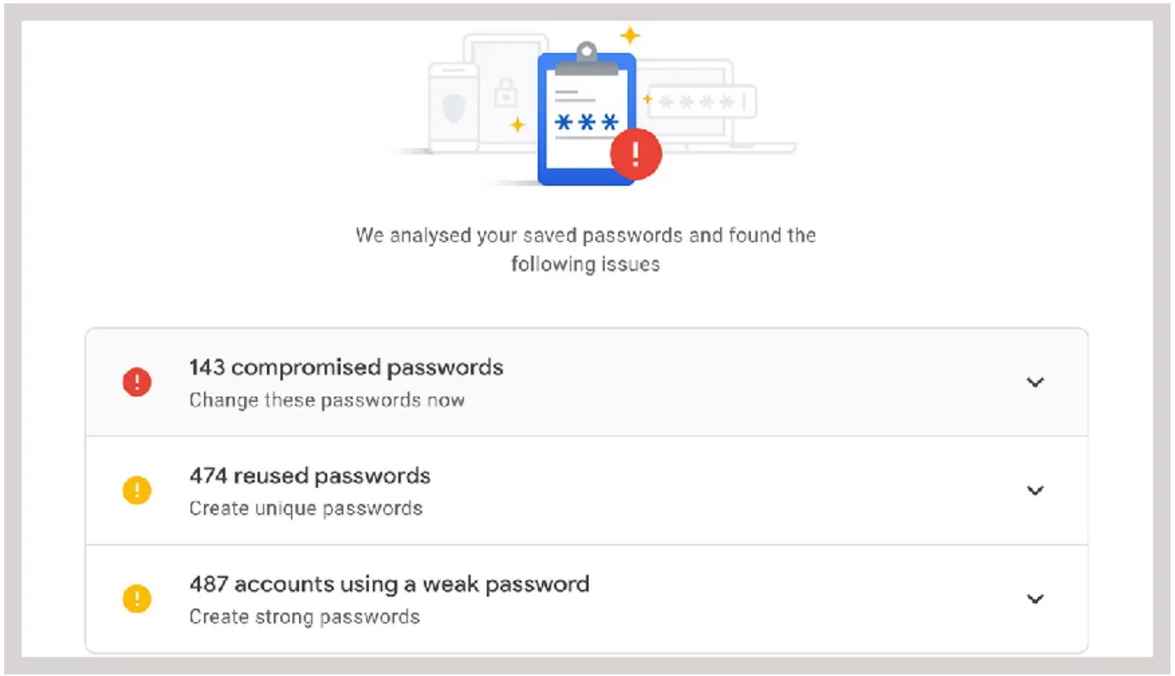
General Data Protection Regulation (GDPR)

Passwords: a new recommendation to control your security

October 14, 2022

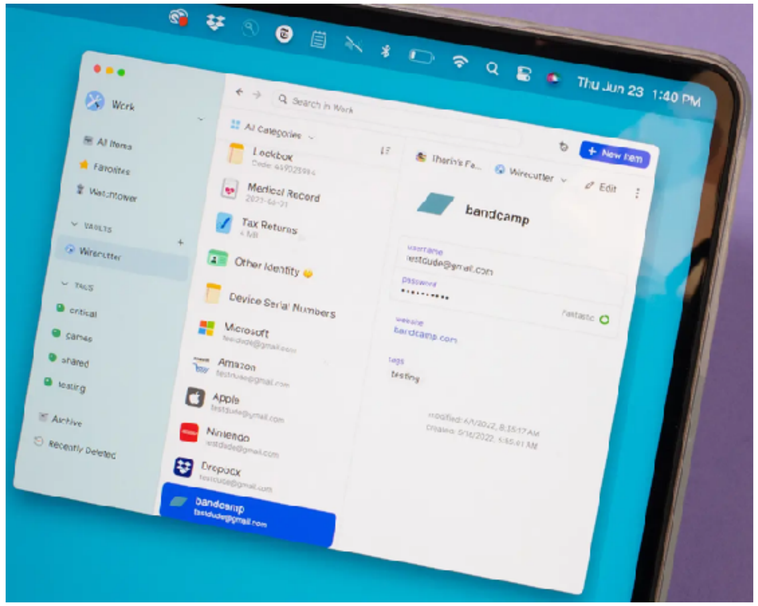
In a context of multiplication of password database compromises, the CNIL is updating its 2017 recommendation to take into account the evolution of knowledge and allow organizations to guarantee a minimum level of security for this authentication method.

guidelines from data protection agencies

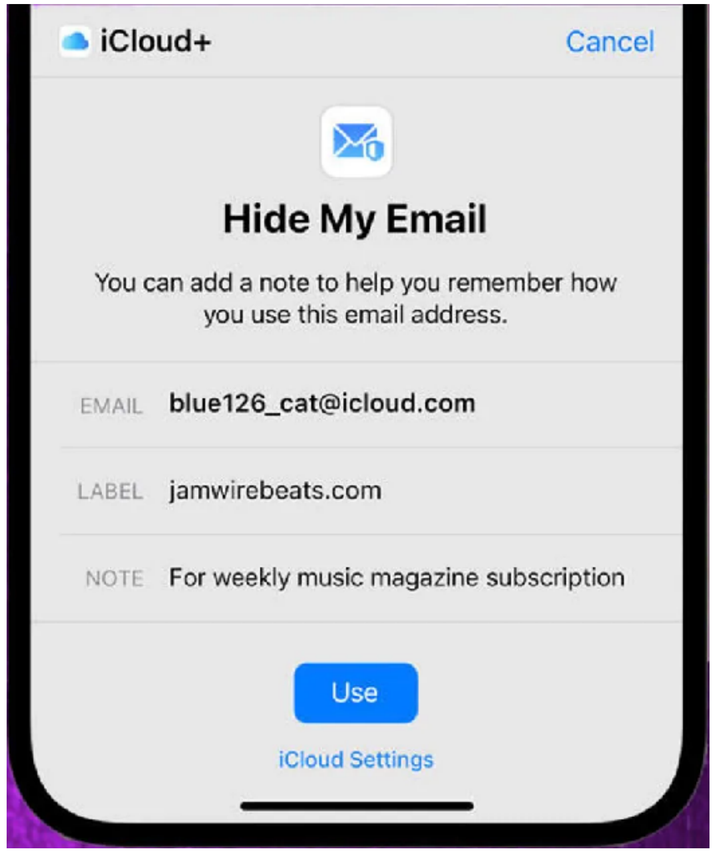


compromised credential notifications

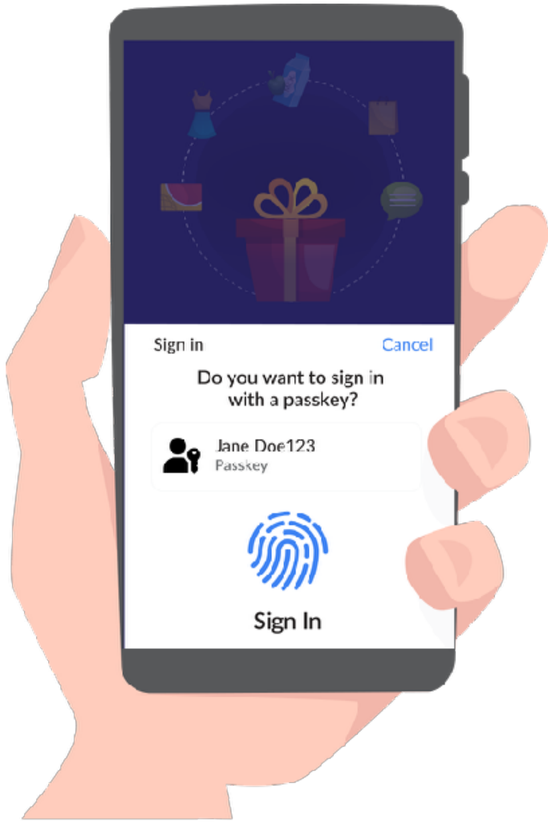
Recommend alternative actions



password managers



email alias generators



passwordless authentication

image source: Wirecutter (left), CNET (center), FIDO alliance (right)

Insights

consumers take limited action after data breaches

breach notifications are fraught with usability issues

threat and coping nudges motivate users to change breached passwords

Opportunities

align notifications and guidelines with consumer behaviors

incorporate PMT-based nudges in practice, while recognizing the limitations

move toward a passwordless future

Nudging Users to Change Breached Passwords Using the Protection Motivation Theory
Yixin Zou, Khue Le, Peter Mayer, Alessandro Acquisti, Adam J. Aviv, Florian Schaub
TOCHI: ACM Transactions on Computer-Human Interaction. Accepted with minor revision.

Yixin Zou
Tenure-Track Faculty, MPI-SP

yixin.zou@mpi-sp.org

yixinzou.github.io