Designing Password-Reuse Notifications

“What was that site doing with my Facebook password?”
use unique passwords

You'll need a password

Make your password unique.

Password

Next
“use a password manager!”
people reuse passwords

R0cky!14

R0cky!17

R0cky!17

R0cky!17

R0cky!17

123456

R0cky!17

ROckyStar

R0cky!17

R0cky!17

R0cky!16
Memory-Hard Hash Function

<table>
<thead>
<tr>
<th>Email</th>
<th>Argon2i Hash of Password</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:jim@mail.com">jim@mail.com</a></td>
<td>$argon2i$v=19$m=4096,...</td>
</tr>
</tbody>
</table>

Rate-Limiting Guessing

Password Strength Meter

Username

Password
acmccs18

Show Password & Detailed Feedback

Your password could be better.
- Consider inserting digits into the middle, not just at the end
- Make your password longer than 8 characters
- Consider using 1 or more symbols

A better choice: \a#D18cmccs

How to make strong passwords
AcmeCo

Email

...  
jim@mail.com  
...  

Linkedin

Email

jane@aol.com  
jessey@gmx.net  
jenny@gmail.com  
jim@mail.com  
john@hotmail.com  
...
<table>
<thead>
<tr>
<th>Email</th>
<th>SHA-1 Hash of Password</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:jane@aol.com">jane@aol.com</a></td>
<td>7c4a8d09ca3762af61e595209</td>
</tr>
<tr>
<td><a href="mailto:jessey@gmx.net">jessey@gmx.net</a></td>
<td>5baa61e4c9b93f3f0682250b6</td>
</tr>
<tr>
<td><a href="mailto:jenny@gmail.com">jenny@gmail.com</a></td>
<td>7c222fb2927d828af22f59213</td>
</tr>
<tr>
<td><a href="mailto:jim@mail.com">jim@mail.com</a></td>
<td>ba93664a90285b9ff18a7a081</td>
</tr>
<tr>
<td><a href="mailto:john@hotmail.com">john@hotmail.com</a></td>
<td>b1b3773a05c0ed0176787a4f1</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
crack all the things!

```bash
$> hashcat -m 100 -a0 $TARGET $DICT

123456
Password
R0cky!17
Football!17
CanadaRocks!
```

<table>
<thead>
<tr>
<th>Email</th>
<th>Cracked SHA-1 Hashes</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:jane@aol.com">jane@aol.com</a></td>
<td>123456</td>
</tr>
<tr>
<td><a href="mailto:jessey@gmx.net">jessey@gmx.net</a></td>
<td>5baa61e4c9b93f3f0682250b6</td>
</tr>
<tr>
<td><a href="mailto:jenny@gmail.com">jenny@gmail.com</a></td>
<td>Canada4ever</td>
</tr>
<tr>
<td><a href="mailto:jim@mail.com">jim@mail.com</a></td>
<td>R0cky!17</td>
</tr>
<tr>
<td><a href="mailto:john@hotmail.com">john@hotmail.com</a></td>
<td>HikingGuy89</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
dead on arrival

<table>
<thead>
<tr>
<th>Email</th>
<th>Argon2i Hash of Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td><a href="mailto:jim@mail.com">jim@mail.com</a></td>
<td>$argon2i$v=19$m=4096,...</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
dead on arrival

<table>
<thead>
<tr>
<th>Email</th>
<th>Argon2i Hash of Password</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:jim@mail.com">jim@mail.com</a></td>
<td>$argon2i$v=19$m=4096,...</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Email</th>
<th>Cracked SHA-1 Hashes</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:jane@aol.com">jane@aol.com</a></td>
<td>123456</td>
</tr>
<tr>
<td><a href="mailto:jessey@gmx.net">jessey@gmx.net</a></td>
<td>5baa61e4c9b93f3f0682250b6</td>
</tr>
<tr>
<td><a href="mailto:jenny@gmail.com">jenny@gmail.com</a></td>
<td>Canada4ever</td>
</tr>
<tr>
<td><a href="mailto:jim@mail.com">jim@mail.com</a></td>
<td>R0cky!17</td>
</tr>
<tr>
<td><a href="mailto:john@hotmail.com">john@hotmail.com</a></td>
<td>HikingGuy89</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
dead on arrival

1 guess is enough!
";--have I been pwned?

Check if you have an account that has been compromised in a data breach

314 pwned websites
5,555,329,164 pwned accounts
80,540 pastes
87,820,647 paste accounts

Facebook sadness: 30 million had personal data stolen in recent breach

Hackers were able to access name, birthdate and other data in nearly half of the 30 million accounts that were affected
black market monitoring
black market monitoring

SECURITY

Facebook buys black market passwords to keep your account safe

The company's security chief says account safety is about more than just building secure software.

BY KATIE COLLINS | NOVEMBER 9, 2016 12:56 PM PST
what's the state-of-the-art?
Keep your account secure

Based on our automated security check, your Facebook password matches one that was stolen from another site. We aren't aware of any suspicious activity on your account, but please change your password now to help keep it secure.
24 notifications

6 representative notifications
methodology
STUDY 1

previously sent password-reuse notifications

STUDY 2

individual components of password-reuse notifications
Imagine you have an important account with AcmeCo...
AcmeCo notifications

Keep Your Account Secure

Your security on AcmeCo is a top priority for us. Based on our automated checks, we've discovered that the password you use for AcmeCo is the same as one that was stolen from another site. We haven't detected any suspicious activity on your account, but we recommend you change your password.

Change Password
questions asked

1. notification understanding
2. feelings
3. actions
4. perceptions
5. demographics
survey setup

180 respondents

• Amazon MTurk
• 15 mins
• Compensated $2.50

6 conditions

LinkedIn
Netflix
Instagram
Facebook
Google
Notifications were concerning and a priority for 83% of participants, indicating very high or high priority for notifications.
Why did you receive this notification?

60% hacked account

21% data breach
Don’t mention password reuse

0 - 4% respondents listed password reuse as a cause

Allude to password reuse

48 - 56% respondents
Keep Your Account Secure

Your security on Instagram is a top priority for us. Based on our automated checks, we've discovered that the password you use for Instagram is the same as one that was stolen from another site. We haven't detected any suspicious activity on your account, but we recommend you change your password.

Change Password
Keep Your Account Secure

Your security on Instagram is a top priority for us. Based on our automated checks, we've discovered that the password you use for Instagram is the same as one that was stolen from another site. We haven't detected any suspicious activity on your account, but we recommend you change your password.

Change Password
“The chances of someone guessing that I use the same password are still incredibly low.” (R171)
Current password-reuse notifications

✅ elicit concern

❌ explain the situation
five notification goals

- timely
- sufficient background
- secure actions
- legitimate
- trust
our model notification

Please create a new password

Dear Jo,

During routine checks, we learned of a potential security incident in which your AcmeCo account login and password may have been compromised. This incident was likely a data breach of a service unrelated to AcmeCo, but because many people reuse similar passwords on multiple sites, your AcmeCo login information may have been affected. While we have not detected any suspicious activity on your AcmeCo account, you must create a new password as a precaution.

Please go to the AcmeCo website or mobile app and we will guide you through creating a new password.

To further improve your online security, we recommend:
• Enabling AcmeCo’s Two-Factor Authentication,
• Changing all similar passwords on other accounts,
• Using a password manager.

If you would like to learn more, please visit https://acmeco.com/security. If you have any questions or need any further assistance, please visit the Help Center at https://acmeco.com/help.

Thanks,
The AcmeCo Team
survey setup

588 respondents

• Amazon MTurk
• 15 mins
• Compensated $2.50

15 conditions

- DELIVERY MEDIUM
- INCIDENT DESCRIPTION
- ACCOUNT ACTIVITY
- PASSWORD CHANGE
- EXTRA SUGGESTIONS
- OTHER ACCOUNTS
What would you do about your AcmeCo password?

- Keep it the same: 6%
- Change it: 90%
- Don’t know: 3%
What would your new password be?

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completely new</td>
<td>2%</td>
</tr>
<tr>
<td>PW manager/browser</td>
<td>11%</td>
</tr>
<tr>
<td>Reused password</td>
<td>13%</td>
</tr>
<tr>
<td>Modified password</td>
<td>68%</td>
</tr>
<tr>
<td>Other</td>
<td>6%</td>
</tr>
</tbody>
</table>
“I know my password is already strong and unlikely to be hacked.”

(R338)
“The hack wasn’t specific to this company so it doesn’t worry me.” (R69)
“Until I see evidence of hacking, I prefer to keep my own sanity.” (R300)
After seeing a password-reuse notification, users

- would change passwords
- ... but ineffectively
- have incomplete threat models
conclusion

1. formative, systematic studies of password-reuse notifications
conclusion

1. formative, systematic study of password-reuse notifications

2. developed best practices
best practices

- send via email + more immediate channel
- name password reuse as root cause
- force password reset
- encourage 2FA and password managers
- suggest unique passwords for other accounts
Please create a new password

Dear Jo,
During routine checks, we learned of a potential security incident in which your AcmeCo account login and password may have been compromised. This incident was likely a data breach of a service unrelated to AcmeCo, but because many people reuse similar passwords on multiple sites, your AcmeCo login information may have been affected. While we have not detected any suspicious activity on your AcmeCo account, you must create a new password as a precaution.

Please go to the AcmeCo website or mobile app and we will guide you through creating a new password.

To further improve your online security, we recommend:
- Enabling AcmeCo’s Two-Factor Authentication.
- Changing all similar passwords on other accounts.
- Using a password manager.

If you would like to learn more, please visit https://acmeco.com/security. If you have any questions or need any further assistance, please visit the Help Center at https://acmeco.com/help.

Thanks,
The AcmeCo Team
conclusion

1. formative, systematic study of password-reuse notifications
2. developed best practices
3. future work should study novel notifications
macOS Mojave, Safari 12
conclusion

1. formative, systematic study of password-reuse notifications

2. developed best practices

3. future work should study novel notifications AND find ecosystem-level solutions
Designing Password-Reuse Notifications

Maximilian Golla, Miranda Wei, Juliette Hainline, Lydia Filipe, Markus Dürmuth, Elissa Redmiles, Blase Ur