User Behaviors and Attitudes Under Password Expiration Policies

Hana Habib, Pardis Emami Naeini, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor

Carnegie Mellon University

CyLab Usable Privacy & Security Laboratory
Let’s talk about password expiration policies

Sources: https://www.portalguard.com/blog/2016/05/04/password-expiration-policy-best-practices/
https://www.top-password.com/blog/tag/disable-windows-password-expiration/
https://makeameme.org/meme/finally-learned-to
Do expiration policies help improve security?

- No evidence that expiration protects from modern password guessing attacks
- Attackers can use password history to launch better attacks (Zhang et al. CCS’10)

"Why do we have to change our passwords? It's not like anyone could ever guess it"

Sources: http://www.designerhipster.com/Cartoons/Business
1. What happens when people are FORCED to change their passwords?

Do users make weaker passwords?

Do they have a harder time using their passwords?

Do they have negative sentiments toward their policies?

How important do they view password expiration?
2. How does human behavior impact the effectiveness of password expiration policies?
Conducted 2 Mechanical Turk surveys

- “Workplace passwords survey” and “password perceptions survey”
- Total of 695 participants
- Age 18 or older
- Residents of the United States
- 55% had an expiration policy for their main workplace password
Workplace passwords survey

● Screening
  ○ Ensure at least one workplace password

● Full survey
  ○ 31 multiple choice questions
  ○ 5 open-ended response questions

● Password management experiences
  ○ Creating, updating, and recalling passwords

● Sentiments toward password expiration
How do people CREATE passwords?

- Use a word in English: 41%
- Use a name: 37%
- Add numbers to beginning or end: 59%
- Add symbols to beginning or end: 32%
How do people UPDATE passwords?

- Modified their current password: 67%
- Created a new password: 24%
- Reused a password from another account: 10%
Techniques to update passwords

Capitalizing a character
soups# → soupS# 30%

Incrementing a character
soupsalad#1 → soupsalad#2 17%

Adding a sequence
alphabetsoupa → alphabetsoupabc 15%

Adding a date
noodlesoup → noodlesoup2018 12%

Substituting digits/special characters
Hot!soup1 → hot!soup9 12%
Coping with password expiration policies

- Use the same strategy they used to create their passwords (64%)
  - Password generator (7%)
  - Substituting letters and symbols

- New fast food receipt
  - looking37Pickles1402

- Updated password was believed to be about the same strength as previous (66%)

Source: https://www.thehollywoodgossip.com/2012/08/best-butt-discount-woman-receives-surprising-credit-on-fast-food/
Password perceptions survey

Management behaviors

1. Using a complex password
2. Storing a password safely
3. Avoiding reuse
4. Changing passwords periodically

- Rate importance of management behaviors for account security
- Rank the harm of not following each practice
- Choose which practice contributes most to account security when shown pairs
- Anticipate behaviors in a hypothetical scenario where their workplace:
  - Implemented expiration policy
  - Removed expiration policy
Expiration is important... but not as important as others

- Use a complex password
- Store your password in a safe place
- Create a password you do not already use
- Change your password periodically

% Who Agreed the Practice was Important

Password expiration
“It takes time to hack or steal a password and if it is changed frequently it is less likely that the hacker will have time to obtain the password.”

“There will be less time for a hacker to retrieve your information.”
Downsides of expiration

- Inconvenient
- Insecure
- Unusable
- Ineffective
“I don’t think [periodic password change] is as important as people say...A really strong password doesn’t just automatically become weaker simply because you’ve been using it for a while.”

“I don’t believe it’s necessarily important to change your password, if you have a secure one in the first place”
Expiration frequency had minor impact on usage

- No reported influence on:
  - Update strategies
  - Account lockouts
  - Similarity with other passwords
  - Sentiments about expiration

- Slight influence on:
  - Password memorization

Source: https://www.kaspersky.com/blog/remember-strong-passwords/6386/
People accept the advice they’re told

- About 50% would continue changing their password if their expiration policy was removed

- Reported reasons:
  - Habit
  - Beneficial to security
“It’s the standard we use and it works well.”

“It’s just a natural habit to do now for my own security.”
“I would forget as it is not on my high priority list.”
Expiration does not lead to weaker passwords or extremely negative reactions...

BUT

...people have developed coping mechanisms which may not benefit account security as much as one would like
Main recommendation

- Enable users to create and manage complex passwords
- Sufficiently random
  - Password managers
  - Password generators

Source: https://support.managed.com/kb/a2245/best-practice-strong-password-policy.aspx
User Behaviors and Attitudes Under Password Expiration Policies

Hana Habib, Pardis Emami Naeini, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor

For more on this: cups.cs.cmu.edu/passwords/