An Empirical Study of Password Policy Robustness

Presenter: Mary Ann Hoppa, PhD
Associate Professor, Cybersecurity Graduate Program Coordinator
Co-Authors: Robert C. Hall & Dr. Yen-Hung (Frank) Hu

Department of Computer Science
Norfolk State University, Norfolk, VA USA

mahoppa@nsu.edu

CISSE 2022
14 November 2022

Disclaimers

- **Opinions expressed are those of the presenter.**
- **Any resources referenced in this briefing are for illustrative purposes only, and should not be interpreted as official endorsements by the presenter, NSU or its research partners.**

- **Dr. Mary Ann Hoppa**
  - CS and Cybersecurity faculty at NSU
  - Co-PI, various DoD & commercially-funded grants
  - Cybersecurity Graduate Program Coordinator
  - 40 years IT R&D experience
  - Research interests:
    - Cybersecurity
    - Cyberpsychology
    - Big Data + ML + AI
    - Quantum Computing
    - ICS/SCADA
    - Serious Games
    - Information Visualization
    - Knowledge Management

https://www.linkedin.com/in/mary-ann-hoppa-phd/

NORFOLK STATE UNIVERSITY

We see the future in you.

700 Park Ave, Norfolk, VA 23504
https://www.nsu.edu

Overview

- **Introduction**
- **Background**
- **Motivation / Research Question**
- **Methodology**
- **Findings**
- **Recommendations**
- **Summary & Future Directions**

About the research…

- **What?**
  - **Cybersecurity Masters Degree (MS.CYB) Capstone Project**
- **Where?**
  - **NSU – online degree program & research experience**
- **Why?**
  - **How big is the “say-do” gap in enforcing password “best practices”?**

We've been *told* what makes a "good" password!

National Institute of Standards & Technology, SP 800-63-3

Recommended:

- **8 to 64 characters**
- **Allow all ASCII characters, including spaces**
  - **Supports "passphrase"**
- **Screening against known weak, common passwords**
- **Lockout enforced**

NOT Recommended:

- **Truncation**
- **Complexity**
- **Short expiration cycle**
- **Knowledge-based authentication ("hints")**
- **SMS-based two-factor authentication (2FA)**
  - **instead: one-time rotating password apps**

Trouble by the numbers…

- **Most popular passwords worldwide:**
  - *123456, Password, 12345678, qwerty, 123456789*
  - *abc123, Password, 123456, Iloveyou, 111111, Qwerty, Admin,Welcome*
- **Over half of all users:**
  - *Include birthdate or name (own/spouse/pet/child) in password*
  - *Share passwords with colleagues/family*
  - *Reuse a favorite password across accounts*
  - *Rely on "sticky notes" for password management*
  - *Forget/reset a password at least once every 3 months*

80% of all breaches involve weak or compromised credentials!

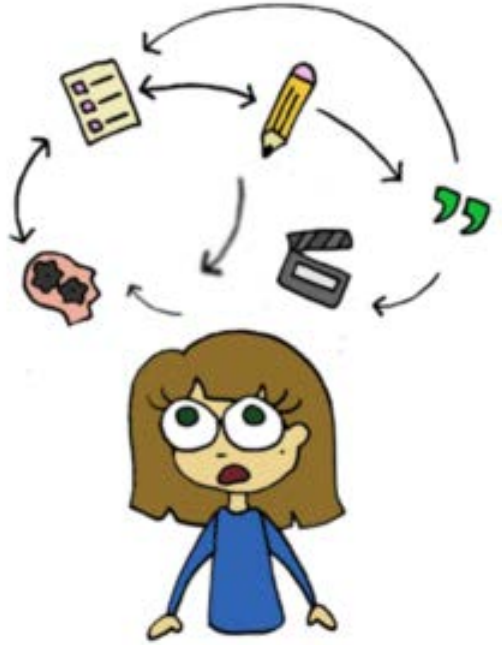
https://www.comparitech.com/blog/information-security/password-statistics/#Password_statistics_and_trends (Jan 2022)

Motivation

- **Despite abundance password policy guidance, users continue to exhibit poor password "hygiene."**
- **There is a lack of current research on password policies of websites that feature account creation.**
- *To what extent do websites that invite visitors to create accounts on them require users to follow authoritative password "best practices?"*

Methodology

1. **Sample population selection**
2. **Volunteer recruitment**
3. **Script and video creation**
4. **Data collection and validation**
5. **Calculations and inferences**



GOAL: During new user account creation, see how rigorously various websites enforce NIST password guidance.

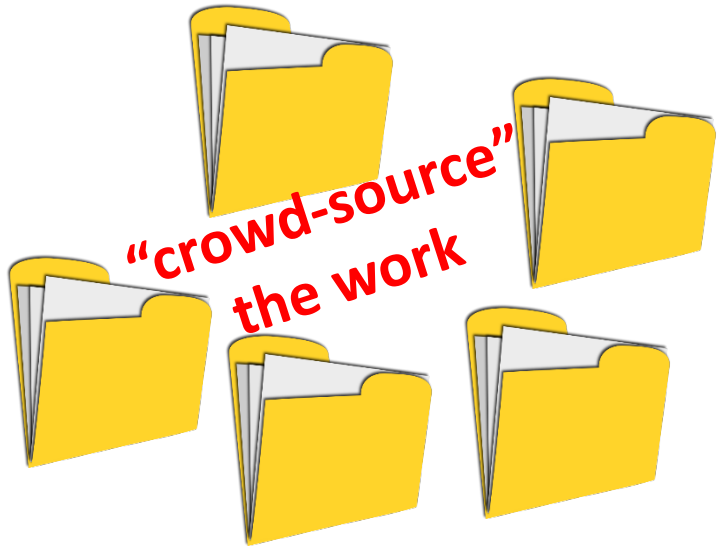
1. Select sample population

- **Verizon Database Incident Report (DBIR) annually rank-orders 21 industries per reported cybersecurity incidents**
- **Picked top 9 (most breaches):** ***Accommodation, Education, Finance, Healthcare, Information, Manufacturing, Professional, Public, Retail***
- **Identified keywords to google relevant websites for the experiment (108 total)**

2. Recruit volunteers
3. Create test script and training video*
4. Collect & validate data

1	Navigate to _____ Website	
2	Search for method to sign in/create account	
3	Fill out all required information, except for the password. Continue to the password data collection portion	
	Password Data Collection	
4	Are you given guidance on the requirements for a password before entering one?	
5	Enter "1 " as a password (no quotations, with a sp… after). Are you now given the requirem… password?	
6	Is there a minimum c…	…er length*
7	Does the password … characters?	
8	Does the password re…	
9	Are the special charac…	Yes / No
10	If so, what special characters …	*Insert special characters*
11	Try to use a space as the passw… …owed?	Yes / No
12	Enter in the password "um1234 …ocation marks). Does it let you continue?	Yes / No
13	Enter in the password "P@ssw0rd" (no quotation marks). Are you allowed to continue?	Yes / No
14	If you are not allowed to continue, enter in any robust password that meets the criteria required.	
15	Are you required to prove you are human? (Captcha?)	Yes / No

25-step script excerpt



* *Ensure consistent, repeatable data collection*

5. Perform calculations and derive inferences

Variable	Policy Category*	Scoring
Char Min	Minimum length enforced	0 – < 8 characters allowed 1 – otherwise
Char Type	All ASCII characters plus space allowed	0.5 – Spaces allowed 0.5 – Allowed special characters not listed
Passcheck	Easy-to-guess passwords excluded	0 – "um1234" or "P@ssw0rd" allowed 1 – otherwise
Complexity	Complexity ignored	0.5 – Upper/lower case mix required 0.5 – Special characters not required
Acct Lockout	Lockout enforced	0 – No lockout 0.5 – < 10 attempts before lockout 1 – 10 attempts before lockout
Pass Hint	Password hints excluded	0 – Yes 1 – No
Sec Quest	Knowledge-based authentication excluded	0 – Yes 1 – No
2FA	SMS-based 2FA excluded	0 – No 1 – Yes

NIST COMPLIANCE SCORECARD

0 = non-compliance

0.5 = partial compliance

1 = perfect compliance

applied to each website's test results

RANGE: 0 to 8 points

**** Expiration policy compliance was not explored***

Aggregated score data

Count	Industry	Total Score	Char Min	Complexity	Char Type	Passcheck	Sec Quest	Pass Hint	2FA	Acct Lockout
19	Accommodation	75%	79%	63%	67%	47%	95%	100%	100%	45%
19	Education	74%	42%	97%	97%	29%	100%	100%	100%	24%
10	Finance	75%	70%	70%	88%	55%	100%	100%	70%	50%
5	Healthcare	71%	100%	30%	60%	50%	80%	100%	100%	50%
10	Information	77%	60%	85%	93%	40%	100%	100%	100%	35%
10	Manufacturing	73%	90%	40%	53%	60%	80%	100%	100%	65%
14	Professional	75%	43%	89%	95%	32%	100%	100%	100%	39%
4	Public	77%	75%	75%	81%	50%	100%	100%	75%	63%
17	Retail	74%	41%	88%	79%	35%	94%	100%	100%	50%
108	**Total**	**74%**	**61%**	**76%**	**81%**	**42%**	**95%**	**100%**	**96%**	**44%**

EXAMPLE INTERPRETATIONS:

Only 29% of Education websites forbid easy-to-guess passwords

Across all 9 industries, 61% enforce a minimum password length of 8 characters

Findings – ‘typical’ websites “internet wide”

- 95% have no security questions or SMS-based 2FA
- 76% comply with character types, avoid complexity rules
- 61% require 8+ characters
- 59% have lockout

- One-third DO NOT follow character types, still impose complexity rules
- Nearly half DO NOT enforce minimum length & DO NOT have account lockout policy
- 80% DO NOT forbid easy-to-guess passwords

Sample size sufficient for 95% confidence with 10% error
Should deviate no more than +/- 0.1 from population (all websites on the internet)
LIMITATION: Selection methodology is “pseudo-random” at best

Findings – ‘typical’ websites per industry

- **Healthcare** websites still enforce “complex” passwords
  - leads to risky habits like password reuse and sharing
- **Retail, Educational, Professional** websites allow short, easy passwords and don’t enforce lockout
  - reduces “friction” between visitors and their purchasing activities
- **Kenexa’s Brassring Human Resources (HR) portal** has very lax policies
  - **MANY industries** use it, putting employee and applicant personal data at risk
- Though not favored by NIST, **2FA is a global trend in Financial** technology

<u>LIMITATION</u>: sample sizes are TOO SMALL to have high confidence in these observations

MORE per-industry DATA COLLECTION NEEDED!

Recommendations

- **Use experimental scorecard to personally rate sites before creating accounts on them.**

- **Develop NIST-compliant user registration and profile manager plugin.**
- **Increase user-friendliness of password manager tools.**
- **Enforce tougher consequences for owners of breached sites.**
  - **Level up legal consequences nationwide and enact federal legislation including stiff fines**
- **Expand upon this experiment:**
  - **More industries (e.g., low reporters); more samples per industry**
  - **Explore additional variables: Expire, Allow Paste**

mahoppa@nsu.edu