http://shucs.org

Beliefs about Cybersecurity Rules and Passwords

Comparing Two Survey Samples of Cybersecurity Professionals and General Users and Future Data collection Experiments

Ross Koppel
PhD, FACMI
Department of Sociology
Univ. of Pennsylvania
rkoppel@sas.upenn.edu

David Harmon
Undergraduate
Department of Computer Science
Dartmouth College
David.B.Harmon.17@dartmouth.edu

Sean Smith
PhD
Department of Computer Science
Dartmouth College
sws@cs.dartmouth.edu

Jim Blythe
PhD
Information Sciences Institute
University of Southern California
blythe@isi.edu

Vijay Kothari
PhD Student
Department of Computer Science
Dartmouth College
vijayk@cs.dartmouth.edu

WHAT WE DID

We conducted a survey to examine the differential perceptions of cybersecurity professionals (n=15) and of general users (n=13) about access rules and passwords.

Often access rules make little sense to users and create barriers to performing one's work and even to achieving the mission of the organization.

Who Sets Policy? (Experts often less clear than most users)

Most general users assumed cybersecurity policy is set by executive management or regulators (69%), and about a quarter (23%) thought it was set by local leaders. Only 15% said they didn't know. In contrast—and very surprising given their jobs—60% of the cybersecurity professionals said *they didn't know* who set the rules.

Different Beliefs about Users' Involvement in Setting Policy: Almost half, 46%, of the general users said or strongly suspected that input from users was used in setting cybersecurity rules. In contrast, again, only 20% of the cybersecurity professionals said users' input was used in setting these policies.

Cybersecurity Rules Often Frustrate Cybersecurity Pros & Regular Users

72% of general users and 67% of pros frustrated by security rules… but seldom furious

Pros wrote: "Sometimes the authentication is done with my real name; sometimes it's done with an arbitrary username I selected and sometimes it is done with [Enterprise name] ID. I often forget which is which."

•"Recalling multiple passwords each with different complexity rules."

•"Waiting so long when turning on/off the computer as it decrypts/encrypts information."

***General users'* comments were remarkably similar in tone and levels of frustration.**

•"Passwords regularly forgotten (because they have to be changed). Delay in work (because password has changed). Confusion about usernames and passwords (multiple accounts and/or passwords) Confusion about internal and external accounts (for example Microsoft business and private accounts)."

•"Frustration. Not able to do their job. Give up or don't care anymore."

When is Circumvention Justified?

"When do you think most personnel would find circumvention of the access rules is justified? (Check as many as applies.)"	General Users	Security Pros
Critical task, e.g., saving a life, keeping the grid up	83%	79%
When the rules are so foolish that nothing else makes sense	42%	57%
Access associated with role(s) make no sense, e.g., members of the same team can' t see all of the information because only some have official access	17%	36%
When allocation of access is foolish, e.g., people hired before November have access but others with similar functions and responsibilities don' t	28%	9%
When everyone else is circumventing a specific rule	58%	43%
When people were officially taught to use a workaround	58%	71%

Answers are often similar—revealing the widespread awareness of circumvention and the rationales for it. Pros were more accepting of circumvention when there's a need for team-wide access and when users are taught the circumvention as part of their training.

Pros & general users differ markedly on how "sensible" are security rules

When asked about management's security rules,
Pros were far more likely than general users to see the value of:
•Logon rules (87% of pros see them as sensible vs. 46% of general users)
•Password complexity (40% v. 23%)
•The logic of management granting access (31% v. 8%)

Cybersecurity Rules Seen as Unreasonable?

For General Users	Very Likely	Likely	Unlikely	Don't know
Access policies generally reasonable	0%	50%	33%	16%
Assume policy makers not fully aware of workflow needs for all tasks	8	85	8	0
Perceived lack of concern by those in charge of computer security	0	58	42	0
CYBER PROS SAY: Regular users Perceive Cyber Rules as a reflection of incompetence of those who are in charge of security	0%	43%	7%	0%
CYBER PROS SAY Many users' see them as arrogant; users think those in charge of security feel: "I know what is best for you – don't question my authority.."	0	36	64	0

General Users: Half said security rules are generally reasonable, although a third were less convinced. The next question is far more worrisome: **93% thought policy makers don't understand users workflows**

Cyber Pros: 2/5ths of pros said users see them as "incompetent," and half see them as "arrogant."

Conclusions

Understanding the perceived reasonableness of cybersecurity policies offers opportunities for improvement, even if one finds users to be naive or misinformed. Only by understanding users' perceptions can we hope to better inform them and to respond to their needs.

While both general users and cybersecurity professionals expressed dissatisfaction with access rules and passwords, their perceptions manifest many misunderstandings; and thus approaches to improving security. A well-informed cybersecurity professional who understands the perceptions of general users will be in a better position to address users' concerns, to establish user trust, and to educate the user by dispelling user misperceptions and legitimizing existing (or new and better) security measures.

Limitations: This was only a pilot study. Sample sizes were very small; generalizing the results to larger populations is unwise. We are, however, expanding the research to larger samples and differing populations.

WHAT COMES NEXT

Background: We have been collecting, and will continue to collect, data and insights regarding password use and misuse via surveys, observations, DASH models, Mechanical Turk experiments, interviews with cybersecurity practitioners, work with Chief Security Officers, formal modeling, working with other groups and scientists to incorporate their data, and collections of passwords from published and unpublished lists and from colleagues.

Next Steps: Collect *data from* ***real world password scenarios & under realistic and differing constraints, parameters, and security needs***

Systematically collect actual password reconfigurations when passwords are altered or added because of required alterations to password rules, e.g., demanding special characters, additional letters or numbers, greater length, more complexity, etc. Including:
•When usernames must change because of related concerns.
•When users' passwords are compromised.
•When users are obliged to create new accounts or increase security on existing accounts, e.g., use of two-factor authentication, need to create new account because of mergers, etc.
•When obliged to provide or alter security questions

Experiment: Two data collection methods

1. "Naturally occurring data" from events where users create or alter existing credentials, as outlined above—parts of natural occurrences (and thus "natural experiments") wherein organizations confront their increasing awareness and the reality of cyber threats by imposing new password rules or otherwise instructing their users to change their credentials

2. Data gathered in response to password rule changes that we partially or wholly help formulate, e.g., by cooperating with existing organizations that wish to increase security or change existing systems. That is, we shall co-design our interventions with cooperating cybersecurity leaders in participating organizations to enact changes that allow us to best understand and document password behaviors.

We then could observe what happens when users are instructed to create passwords in response to different password composition policies:

- 25% of users are instructed to create new passwords without guidance,
- 25% are required to create passwords that comply with a stringent password composition policy,
- 25% are required to create passwords that comply with a lax policy, and
- 25% are forced to use two-factor authentication.

Note that in no case would we ever know the usernames associated with any users. Each user will be assigned a random number for our datasets so that we can follow the trajectory of changes but never know the identity of the user.

Additional Experiments & More Findings

- Alternative password strength indicators and feedback mechanisms (e.g. with user-friendly guidance vs. other systems);
- Rules about affiliations between passwords and user names (vis-a-vis repetition of terms) or passwords and name of service or organization (e.g., password cannot incorporate name of URL or organization);
- Passwords that can or cannot include elements of the previous passwords (e.g., Fluffy1, Fluffy2, fLUfY33, FlufffieS, etc); and so on.

OUTCOMES, LESSONS, FINDINGS

1. Provide real life datasets documenting how people understand password rules, how they respond to rules, how they conceptualize security in use; how passwords are changed to reflect new rules

2. Enrich emerging DASH password modeling efforts, Mechanical Turk parameters, & many simulations and models

3. Building theoretic and empirical basis for the science of security.

4. Provide direct practical value for cybersecurity protection.

Visit shucs.org to learn more about the Science of Human Circumvention of Security

This material is based upon work supported by the Maryland Procurement Office under Contract No. H98230-14-C-0141.

SCIENCE OF SECURITY
VIRTUAL ORGANIZATION
Funded by the National Security Agency.

INFORMATIONTRUST
INSTITUTE