Beliefs about Cybersecurity Rules and Passwords

A Comparison of Two Survey Samples of Cybersecurity Professionals Versus Regular Users

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

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

* This poster is an adaptation of an earlier paper: Beliefs about Cybersecurity Rules and Passwords: A Comparison of Two Survey Samples of Cybersecurity Professionals Versus Regular Users. Security Fatigue Workshop, SOUPS 2016

Abstract

We examine the differential perceptions of cybersecurity professionals and of general users about access rules and passwords. We conducted a small pilot study of two parallel survey instruments to elicit the perceptions and beliefs about cybersecurity policies (including who sets policy and if they include general users in that process), rationales, and compliance.

Circumvention of Access Policies is Pandemic

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 less clear than most users)

BIG DIFFERENCES BETWEEN GENERAL USERS AND THE EXPERTS. 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.

Were Users Asked When 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.

Both Cybersecurity Professionals and General Users Were Somewhat Frustrated By Rules

Neither general users nor pros were deeply frustrated by the rules; and most sought to understand the reasons for them. In fact, 23% of general users and 33% of pros were not frustrated at all.

Frustrated by Security policies	1 (Not Frustrated)	2	3	4	5 (Very Frustrated)
General users	23%	39%	15%	23%	0
Cybersecurity professionals	33%	27%	33%	7%	0

***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."

"The requirement to change the password every 70 days."

"Getting logged out because of timing when you're in a rush."

"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. They: *wrote:

"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."

"Work delayed: 2 extra minutes like 10 times a day is true. Hate using the system."

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.

Sensibility of Rules

How Sensible are Several Rules?

	Generally Sensible		Sometimes Sensible		Not Sensible		Don't Know	
	Gen	Pros	Gen	Pros	Gen	Pros	Gen	Pros
Log on rules	46%	87%	46%	0%	8%	13%	0%	0%
Password rules for different passwords for each app	30	7	20	53	50	27	0	13
Password complexity	23	40	38	20	38	40	0	0
Password change frequency	25	13	58	40	17	33	0	13
Management's rules on granting access	8	31	69	23	15	8	8	38
Inactivity timeouts	31	53	54	33	15	13	0	0
Different rules for different systems	17	21	42	43	33	14	8	21
Rules by how/why access is provided	38	53	46	20	15	13	0	13

When asked about management's security rules, the two groups' reactions were often starkly different. 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%)

Why are Cybersecurity Rules Seen as Unreasonable?

Why are the Access Rules (Perceived as) So Foolish?
Light Rows: Asked of only general users (rows 1-3); Dark Rows =only cyber security professionals (row 4)

	Very Likely		Likely		Unlikely		Don't know	
	Gen	Pros	Gen	Pros	Gen	Pros	Gen	Pros
1 Not applicable: Users find access policies generally reasonable (**asked only of gen. users**)	0%	^	50%	^	33%	^	16%	^
2 Users may assume policy makers not fully aware of workflow needs for all tasks (**gen users only**)	8	^	85	^	8	^	0	^
3 Perceived lack of concern by those in charge of computer security (**asked only of gen. users**)	0	^	58	^	42	^	0	^
4 Perceived incompetence of those who are in charge of security (**only asked of pros**)	^	0%	^	43%	^	57%	^	0%
5 Perceived arrogance of those who are in charge of security ("I know what is best for you – don't question my authority…")	8	0	43	36	50	64	0	0
6 Externally-imposed regulations which do not appear to be reasonable, dictating access rules	33	14	17	36	42	36	8	14
7 Using security as an excuse for laziness, e.g., they should fix something but just say it must be as is because of "security"	17	0	25	20	58	53	0	27
^ = question(s) not asked of that group								

Half of general users 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. [Rows 4 & 5]: 2/5ths of pros said users see them as "incompetent," and ½ see them as "arrogant."

Conclusions

Answers to these questions about the reasonableness or foolishness of cybersecurity policies offer 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 were in some ways very different, in ways that suggest misunderstandings and misdirected approaches to improved security. This preliminary study serves as a step toward informing both cybersecurity professionals and general users to ultimately improve user behavior and cybersecurity policy. 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 to larger populations is unwise. We are, however, expanding the research to larger samples and differing populations.

For more information on this and our other project work, visit http://shucs.org.

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