Passwords are not always stronger on the other side of the fence

Ijlal Loutfi
University of Oslo
ijlall@ifi.uio.no

Audun Jøsang
University of Oslo
josang@ifi.uio.no

***Abstract*—The username-password pair is still a prevalent form of online authentication. However, attacks that are leveraging weak password habits are on the rise. The main response of the security community on the ground is to invest more in educating users. Such an approach leads to believe that the long held assumption stating that an ignorant user is the cause of an inadequate password behavior, still has many opponents. Although different research studies have presented other more likely reasons, practices are still perpetuating the same solution mindset of increasing end users' education. The behavior of users has not improved dramatically over the last decade despite all these efforts. Therefore, this research work explores the hypothesis that knowledge of good password habits is a necessary but not by itself a satisfactory requirement for a safe password behavior. This will be achieved by studying the password habits of the same people advocating for more end user education. To investigate this hypothesis, we conducted a survey targeting an audience of IT professionals with good knowledge about security. The survey results show that cognitive knowledge of password security does not always materialize into practical and secure password practices. The anticipated results would be that confronting IT professionals with their own password practices which fail to adhere to what they preach to end users, will motivate them to let go of their long held assumptions that more education is the solution. This will further support the points made by other studies explaining the rationale behind the inadequate password habits of end users.**

I. INTRODUCTION

Despite recent advances in user authentication methods, the most common mechanism used on the Internet today is still the username and password pair. As a result, users are maintaining a large number of credentials for the many online services they use [7]. This is problematic because password based user authentication brings serious usability challenges.

USEC '15, 8 February 2015, San Diego, CA, USA

http://dx.doi.org/10.14722/usec.2015.23005

The inherent problem with data security is human fallibility. Even with the most advanced security systems in place, if there is a human component to that system, there will be vulnerabilities [9], [13]. Enforced policies are not stopping users from adopting inadequate password habits such as weak passwords, reused passwords and ignoring certificate warnings, just to cite a few. Indeed, security reports over the past decade show that attackers have been leveraging weak passwords in order to gain unauthorized access.

Hence, given the importance of password habits, a number of studies have been conducted by IT professionals with the aim of finding satisfactory solutions. As anticipated, the surveys converge in their results, demonstrating alarming percentages of weak passwords and inadequate password practices [5]. The main response by the security community to these threats against the human link has been users' education. Users are given instructions, advice and mandates as to how to protect themselves and their machines [8]. In this spirit, many IT professionals invest heavily in this regard. From companies including modules while onboarding their new employees, to large online companies posting sophisticated tips to its customers, to researchers investing in designing education modules that ought to be included in schools, the examples are numerous. This behavior presupposes that the idea attributing inadequate password habits to an ignorant and lazy end user, is still being held by IT professionals.

However, more recent research studies have been giving strong evidence for other more likely causes that explain the inadequate password habits of end users. For instance, solid arguments and studies indicate that the security advice received by users does not justify the cost they have to trade for it, making their decision to ignore it a rational one [7]. However, the reality on the ground indicates that IT professionals are still advocating for and implementing more education for end users. This leads to believe that while designing solutions, IT professionals fall back on the traditional explanation of inadequate password habits, which has long been attributed to the ignorance of end users. Several arguments can explain why IT professionals still hold on to their old assumptions despite strong recent evidence for their irrelevance: lack of awareness about such studies, a disagreement with their arguments, or a failure to internalize the implications of their findings while designing solutions. Independently of the reasons, the numbers indicate that password habits have not improved significantly since a decade [1], [16], while more educational efforts have

been deployed. This has to change. In this study, we want to explore the hypothesis that knowledge of good password habits is a necessary but not by itself a satisfactory requirement for a safe password behavior. This will be achieved by studying the password habits of the same people who implement such solutions. It is anticipated that confronting IT professionals with their own password practices which fail to adhere to what they preach to end users through several educational channels, will motivate them let go of their long held assumptions that more education is the solution. This will help further support the points made by other studies explaining the rationale behind the inadequate password habits of end users.

To answer this question, we conducted our study with an audience that is exactly what the solution of "more education" strives for: IT Professionals. Hence, the metaphor of "the other side of the fence" in the title referring to the community of security and IT professionals who are assumed to be knowledgeable about good password practices and the risks associated with failure to comply with them. This stands in opposition to normal users who are assumed to be relatively ignorant about good password practices. Further, we want to investigate what would explain any highlighted differences in the password behavior of our audience. For this purpose, we also chose to remove a bias that, as per our literature review, is always embedded into the studies: the sensitivity level of different online services is regarded as a universally fixed value for all users. However, this study considers the sensitivity level of a service to be subjective. Indeed, it is a measure that should be evaluated from each user's perspective and usage profile for that specific service. For this reason, we included in our survey, questions that capture the user's perception about the sensitivity level of each service, as well as how that correlates or not with their behavior.

II. RELATED WORK

A. Attacks

Users are typically seen as the weak link in any security chain. In the case of individually targeted attacks, it is usually easier to get sensitive information and passwords by social engineering than by direct assault or brute-force attacks against the system. The best way to get software onto any machine is to get the user to install it and human error is behind many of the most serious exploits [2], [7]. Further, over the past decade, many companies have reported breaches to their user accounts that were caused by brute force attacks against passwords. The latter exploit the weaknesses of the passwords chosen by human users. Early in 2013, the annual Data Breach Investigations Report published by Verizon, stated that approximately 90% of successful breaches in 2012 analyzed by Verizon started with a weak or default password, or a stolen and reused credential [12], [18]. The examples of successful attacks that have compromised the users' credentials are numerous:

- As per the analysis provided by Acunetix for the over 10,000 Hotmail passwords that were leaked online, 42% of them only contain lowercase alpha characters (a-z) and the majority of passwords were between 6-9 characters long [18].
- Usernames, e-mail addresses, password hashes, and password hints for adobe were leaked online. Inspired by this leak, a list of "the worst passwords of 2013" was published which shows passwords like "password1", "letmein", and "123456" are more common than one would think [4], [18].

Attacks against weak passwords are so flourishing that some emerging businesses were built upon this trend: "pznedlist" is a company specializing in monitoring the market of leaked credentials and reporting back to its subscribers when a positive hit is found on one of their accounts [16].

B. Surveys

In order to capture the behavior of online password usage directly from end users, a number of research groups relied on surveys as a means to collect feedback: during 2013, a survey was conducted in Norway by Norstat on behalf of EVRY. The sample size was 1012 respondents from Norway [5]. The findings of the survey were publically shared in order to raise awareness about the current passwords behavior, as well as evangelize for better password habits. In 2012, the organization SCID conducted a consumer survey of password habits among consumers in the USA [5]. Further, SafeNet which conducted a global survey study on passwords, announced an equally alarming password behavior in all the surveyed geographical areas [15].

C. The Assumed Solution is Education

The above mentioned surveys and their analysis have reached many similar conclusions: users are not practicing secure password techniques. After presenting their data, most studies suggest that more education is the solution [2]. As many notable institutions are putting forward the idea that investing in increasing educational efforts about security would eventually resolve the bad password behavior, other researchers are now taking this as a mantra and designing their research with an end goal to prepare education modules.

This research work acknowledges that Cormac Herley has presented a compelling case of why more education is not the answer. One possible plausible explanation given by the latter is the high competition for users' attention. Our work aims to further support this point within the IT professionals' community. This would be achieved by confronting them directly with their own password practices which fail to adhere to what they preach to end users through several educational channels, while they don't lack themselves such knowledge. Such a tactic would be anticipated to push them to make more conscious efforts in exploring different venues and implementing more efficient solutions, other than "more education" [9]. Indeed, research results should not stay confined within the borders of their papers. We should find efficient tactics to reach out not only to end users, but also to IT professional working in the ground: they are indeed in important link in the chain.

III. MOTIVATING QUESTIONS

In this paper, we argue that we should challenge the assumption stating that investing in more education for the end users is the solution for their inadequate password behavior. Such an approach presupposing that the lack of end users' knowledge about safe password practices is the reason cause driving their inadequate password behavior. Given the still unsatisfactory status of online password usage despite the education efforts deployed, our hypothesis hence, is that educating users is a necessary yet not a by itself a satisfactory reason to practicing safe online password behavior.

Specifically, this study investigates this hypothesis through a survey whose respondents were chosen to be the same people who design these educational solutions: IT security professionals. (Please refer to the survey methodology section for more details).

The services we enquired the respondents about were: Facebook, Gmail, LinkedIn, Twitter, Work/studies email, bank account, online gaming accounts and online storage services

Furthermore, unlike the rest of the studies we have surveyed, this research accounts for the bias in identifying the sensitivity of any one service. Indeed, we let the respondents report their own perception the sensitivity level of each service. All possible associations/correlations between the reported sensitivity level, the reported password behavior and the profile of the users are then investigated.

For the sake of clarity, the below concepts are defined as follows, and should be understood and interpreted as such:

- Reported sensitivity level: the level of sensitivity a user judges a service to be to them.
- Reported password behavior: this is a measure induced from the individual answers the users provide about specific aspects of the password they use for each service (e.g.: length, character mix...etc.)
- Perceived password behavior: the judgment the users hold about how healthy their password behavior is.

Lastly, an emerging alternative to the passwords based web authentication is federated login. However, this mechanism raises serious privacy issues. One other goal of the study is to measure to which extent is this a concern for a person who is well informed about the issue [11].

Based on the above, the analysis of the results, coupled with other relevant studies, should enable us to get more insights into the following high level questions:

- To which extent does cognitive knowledge about passwords behavior materialize into practical behavior?
- To which extent can we claim that education is a necessary yet not a satisfactory requirement for a safe online password behavior
- Are we making the right investment to resolve the password behavior challenge by increasing education channels about it?
- Is there a disparity between the perceived strength of passwords IT professionals use, and the strength we induce from their self-reported behavior?
- Does cognitive knowledge about how sensitive a service correlate with how well the password habits related to that account are?
- Is more granular advice about passwords' behavior the answer?
- Are people who perceive themselves as concerned with their online privacy, less willing to use federated login?
- What would trigger a user to become more aware about their password behavior?

IV. SURVEY METHODOLOGY

D. Audience and Methods

Because this survey is aimed at a specific focus group, we did not open it for the large public. The target audience of the survey is IT professionals who are working in different industries.

We used a web based version of the survey that we have designed with a premium account of Surveymonkey. The URL of the web-based survey was distributed via email.

We solicited the response of 112 people. A number of participants did not complete the survey or answered questions inconsistently. Their responses were removed from the data set, leaving 66 valid responses.

Further, it was our intention not to disclose to the audience that we are targeting IT professionals for this study. This would help minimize any kind of bias the respondent might develop while answering the survey questions.

The participants came from our mailing list of industry partners, as well graduate level students and above at the informatics department at the University of Oslo, Norway. Amongst the latter, we included a list of graduate level students who were taking an advanced security class during the semester the survey was conducted.

Thus, this work assumes that the audience sample chosen has sufficient knowledge about good password practice. However, the study did not employ any further mechanisms to account for any possible dishonesty from the respondents.

E. Design

The independent variables of the study are gender, age, ethnic background, country of residence, marital status, occupation, education level, number of online accounts of the user and IT Skills. The independent variables that aim at capturing features of the psychology of the user are: view of the world, introversion vs extroversion.

Our dependent variables can be classified in 3 categories:

- Parameters capturing perception: confidence in the strength of the used passwords, perceived sensitivity of an online service, and the reported concern about privacy.
- Parameters capturing the reported behavior: storage behavior of the password for each service, length, characters mix, memorability, reuse, usage of social login features, and usage of password managers.
    - For each one of the above mentioned parameters capturing the reported behavior, the survey results include results about the following online services: Facebook, Gmail, LinkedIn, Twitter, Work/studies email, bank account, online gaming accounts and online storage services
- Looking into the future: expressed willingness to improve password habits.

The placement of the questions was designed in a way that would optimize the accuracy of the responses by minimizing embedded biases [3], [19]. Respondents answer questions about their password habits for each online service prior to rating the sensitivity of these services. The goal is to avoid any minimize any intentional bias that would correlate the sensitivity level of a service with its corresponding password behavior when there is none. Further, the respondents rate their confidence level in their passwords' strength prior to determining their intent to improve their password behavior or not. Lastly, the respondents report their federated login usage before rating their privacy concern. This would help avoid exposing the correlation/association the study aims to measure.

V. Results and Analysis

For the purposes of this paper, and in line with the objectives outlined above, we will focus on presenting and analyzing the below data:

- The profile of the respondents:
- Password usage
    - The behavior reported by users for each service.
    - The perception the respondents hold about the strength of their password behavior.
    - Association and correlation analysis between the reported/self-perceived behavior and perceived sensitivity of each service.
- Privacy
    - The reported privacy concern.
    - The reported privacy behavior expressed in the federated login scenario.
    - Association/correlation analysis between the self-reported and self-perceived behavior regarding privacy and federated login.
- Profile of people who express a willingness to reconsider their password behavior. Further, for the purposes of this paper, we did not include the data of Bank account behavior in the analysis. Most respondents referred to using 2 factor authentication for this service, and we will be discussing the impact of 2FA in the context of another research activity.

F. Respondents Profile

TABLE I. Parameters of the respondents profile

Demographic profile	Psychological profile	Digital behavior profile
Gender, Age, Ethnic background, Residence, Country, Civil status, Occupation, Education.	Mood, Worldview, Social login activity.	History with digital hacking, Number of online accounts.

The full distribution of the respondents' profile can be found attached in appendix 2.

G. Personal Usage

For each one of the 8 services studied(Facebook, Gmail, LinkedIn, Twitter, Work/studies email, Bank account, online storage, online video games), the respondents reported on their password behavior by answering questions enquiring for the below information(Questions 19 through 23 in the survey attached in appendix 1):

- Length of the password.
- Characters Mix in a password.
- Frequency of password changes.
- Usage of password recovery.
- Uniqueness of the password.

Further, the respondents reported on their password storage behavior.

From the above, we can note that:

- For each one of the 66 respondents: the study collected 41 individual pieces of information about their password usage.
- For each one of the 8 services: the study collected 494 piece of information about how our respondents interact with their password based authentication.

- Collectively, this makes up a total of 2970 pieces of information about how all of our respondents interact with all the services studied.

The analysis of the data was completed in two iterations. The focus of the first iteration was analyzing the dataset as an aggregated set. This iteration is qualified as initial because aggregated data does not provide insight into how the observed behavior relates to neither the user's profile nor to the sensitivity level of the online services. Further, this first iteration provides little insight into the statistical relevance of the results. Indeed, judgment cannot be made about whether the highlighted correlations have any statistical significance. All these noted shortcomings of the aggregated analysis of. Nonetheless, aggregated data provides a great first stone in getting acquainted with the date set and in spotting patterns. The focus of the second phase is the study of more granular data, to the level of each respondent and each service.

The observations made in the initial iteration of data analysis are highlighted below:

1) Hacking Attacks don't Discriminate: 26 percent of respondents have been victims of hacking in the past. This number, naturally, does not account for people who have been victims to hacking without being aware of it. To put things into context, during 2014, 47 percent of Americans were hacked. This goes into showing that IT professionals are not immune to attacks.

2) *IT Professionals Are Guilty:* 11 percent of the respondents use non safe ways to store their passwords: digitally in the clear or on paper. While this might appear to be a small proportion of the respondents, the result should be read and interpreted in the context that the people surveyed are working in the IT field. These respondents are hence, likely to have responsibilities involving handling whole IT infrastructures and/or end user data. while there are views stating that writing down a password and physically storing in a secure location is a secure behavior, we disagree with this stand. As a matter of fact, a user would store a password physically if they estimate a high likelihood of forgetting it. This assumes that the user would be retrieve the piece of paper physically each time they do forget their password. We consider this behavior to increase the risks associated with exposing the password..

3) *Character Mix:* As per the table below, a considerable percentage of respondents do not always use a mix of characters when they are not forced to do so. Further, this behavior is more pronounced in services like Facebook and LinkedIn which don't enforce such policies, and that are increasingly being used as identity providers for other online services leveraging the federated authentication method.

TABLE II. PERCENTAGE OF WILLINGNESS TO USE A MIX OF CHARACTERS WITHOUT BEING ASKED TO

	Yes, Always	Yes, Sometimes	No Never
Facebook	76	21	3
Gmail	81	18	2
LinkedIn	71	21	7
Online Video Games	67	30	3
Work/Studies	17	83	0
Twitter	3	24	74
Online Storage	83	17	0
Bank Account	82	14	5

4) *Password Change Frequency:* the respondents do not always exhibit a healthy pace of changing passwords when the policies do not enforce it.

TABLE III. PERCENTAGE OF HOW FREQUENT RESPONDENTS CHANGE PASSWORDS WILLINGLY

	monthly	6 months	yearly	rarely	When asked
Facebook	2	10	19	40	29
Gmail	2	8	24	34	32
LinkedIn	0	7	16	46	32
Online Game	3	3	12	41	21
Work/Studies	12	9	12	26	41
Twitter	0	5	16	45	34
Online Storage	2	10	16	36	36
Bank Account	3	8	17	42	30

TABLE IV. PERCENTAGE OF UNIQUENESS OF THE PASSWORD PER SERVICE

	Reused	Unique
Facebook	47	53
Gmail	42	58
LinkedIn	55	45
Online Games	60	40
Work/Studies	18	82
Twitter	42	58
Online Storage	45	55
Bank Account	17	83

5) *What IT Professionals Are Best at: So for,* for each one of the surveyed services, 97 percent of users reported password lengths greater than 6 characters.

Perception of the respondents about their password behavior *(*questions 24, 27 and 16):

- Sensitivity of the 8 services
- Perceived privacy concern
- Perceived confidence in the strength of the password used.

From the above we can note that:

- For each one of the 66 respondents: the study collected 9 individual pieces of information about their perceived password behavior.
- For each one of the 8 services: the study collected 132 pieces of information about how our respondents perceive their password usage behavior.
- Collectively, that is a total of 1056 pieces of information about how all of the respondents perceive their password interactions with all the services studied.

Similarly to the reported password behavior, the analysis first considers the results of the initial iteration of data analysis. Hence, the dataset is first analyzed as aggregated set. The resulting observations are as follows:

TABLE V. PERCEIVED SENSITIVITY OF A SERVICE

	High Sensitivity	Moderate Sensitivity	Low Sensitivity
Facebook	36	50	14
Gmail	58	31	11
LinkedIn	22	47	31
Online Video Games	13	30	57
Work/Studies	85	15	0
Twitter	11	37	53
Online Storage	68	30	2
Bank Account	95	5	0

TABLE VI. EXPRESSED CONFIDENCE IN THE PASSWORD STRENGTH

Expressed confidence level	Percentage
Totally Confident, 4	17
3	55
2	18
1	8
0	3

72 percent of the respondents reported a higher than average level of trust in their behavior. (Average refers to the average score as defined by the scale of choices given to the users to choose from: from 0 to 3).

6) *Reported Behavior Vs. Perceived Sensitivity:* From the aggregated analysis of the data above, we can already spot areas in which the password behavior of IT professional is less than satisfactory.

The first question the study would explore is "whether the observed passwords behavior for each user correlate with the perceived level of sensitivity for each service". As the data is categorical, the Chi square test will be used [10].

The Chi square test will be performed against the null hypothesis. The latter assumes that two categorical variables are completely independent. The Significance value the set for this study is 0.05.

The study aims not only to explore the statistical associations between the variables, but also to determine the specific pairs of combinations that have yielded the most significant results. To achieve this goal, the analysis of the data also comprises computations of the residual deviation for each pair. The significance range used is (-2,2) [10].The test is first run on all the services combined. The results are as follows:

TABLE VII. P TEST CHI SQUARE OF THE MEASURED PASSWORD BEHAVIOR VS. THE PERCEIVED SENSITIVITY LEVEL

	Sensitivity level	Interpretations/comments
Password Length	0.007	The null hypothesis does not hold. Strong derivative chi square between high sensitivity an increased password length
Password Character Mix	Less than 0.01	The null hypothesis does not hold Residual values of values of "yes, always" and "yes, sometimes" are the ones which are higher The residual values observation is confirmed by visualization of the data.
Password Change	P value could not be computed because of a high number of small count cells.	No conclusion about the association from the p value The residual margin analysis significance between(low sensitivity, only when prompted to do it) and (moderate sensitivity, every 6 months) Visualization of data are in sync with the residual margin observations.
Use of password Recovery option	0,06	Null hypothesis holds No significant residual margin values observed
Reuse	Less than 0.01	The hypothesis does not hold Residual margin values were significant for all pairs of value Closer look at the date needs to be done to infer the most relevant pairs for our study.

The residual deviation significance does not always indicate a practically significant association. This, the analysis cross-compares the initial conclusions drawn from the residual deviations, to visualizations of the raw data before making any final conclusions. Such an approach is considered a good practice, because the Chi Square is a test of statistical association and not of linear correlation. The focus of this study is linear associations. The conclusions made as well as the interpretation of their implication are as follows:

- Character length is the feature that the respondents have shown the most ability to materialize from cognitive knowledge into practice. Indeed, more sensitive services exhibited lengthier passwords.
- An association exists between the character mix and the sensitivity level of services. There are strong evidences of a linear correlation in the data.
- Further analysis is needed for the reuse feature: the initial observations are not conclusive and did not initially reveal any significant linear correlations.
- The strong association between the pairs suggest that there is a consistency in the behavior of users who perform well. Specific pairs of combinations require further analysis.

The correlation value measured between different pairs on the reported password behavior yielded p values less than 0.001:

- This was an interesting result for us. Although it did not express what kind of correlation exists between these parameters, it made us think about investigating the behavior of single respondent across all the matrix parameters and see if we can spot consistent behavior of safe/unsafe password behavior.

At this point, we can already observe that our respondents are not exhibiting a strong correlation between the perceived sensitivity level and the password behavior. Suggesting that indeed, there is a disconnect between cognitive knowledge and practical behavior.

After having completed this round of analysis, we wanted to get a DEEPER understanding of our data, by looking at interesting combinations of responses that are hinted by the p values for Chi Square analysis.

*7) Respondents with an Across-the-board Satisfactory Password Behavior:*Indeed, and as hinted and highlighted in our previous conclusions, there was a strong suggested association between the parameters capturing the reported password behavior of users. One particular subset we focused on was the one of the respondents who exhibited satisfactory behavior across all metrics. We made interesting observations about this subgroup:

- 69 percent of passwords across all services satisfy all the parameters needed for a safe password at once.

That is a mere 12 percent of the whole of the passwords. The respondents of this subset exhibited the below behavior:

- 100 percent of the Respondents with a satisfactory password and who don't think they should improve their future password behavior have expressed a complete level of confidence in their behavior (4).
- 97 percent of the Respondents with a satisfactory password behavior and who are expressing the intention to improve their password habits in the future, expressed a level 3 confidence level in their password strength.
- 3 percent of the Respondents with a satisfactory password behavior and who are expressing the intention to improve their password habits in the future expressed a level 2 confidence level in their password strength.

There was one more observation which made us zoom more into this group of respondents and study a subset within it:

The Chi Square values revealed a tight association between 3 of the 5 parameters measuring the password behavior. Amongst the 69 passwords, more than 50 percent of the passwords mapped to 30 percent of the respondents that are part of this subset A.

Amongst A, the respondents who exhibited safe online password behavior across at least 50 percent of the services were further studied. These are the users exhibiting the most optimal password usage across all services:

- Interestingly, 75 percent of these respondents answered by yes to the question of whether or not they intent to improve their password habits in the future.
- 0 percent expressed a total confidence in their password strength.
- 100 percent expressed a level 3 confidence in their password strength.

8) Confidence Vs. Willingness to Change: The P value of the chi Square test revealed a strong correlation between the reported confidence level at the beginning of the survey and the expressed intent to improve ones password behavior at the end of the survey.Indeed, the P test value of 0.042 means that the null hypothesis does not hold. A second look at the the visualized dataset in light of this observation confirms it.

- 9 percent of the respondents who have expressed a total confidence in their password strength have expressed no intent to improve their password habits.
- 67 percent of the respondents who have expressed a level 3 confidence in their passwords behavior have expressed no intent to improve their password habits.

9) Perceived Privacy and Federated Login: Ever since their emergence, federated login mechanisms have sparked a lot of controversy in the security community. On one hand, they introduced a convenient way for end users to authenticate and alleviate their identity sprawl problem. On the other, they raised many privacy issues. In the context of this paper, we

will not discuss the other security requirements federated login put at risk [11].

One of the assumptions put forward to explain the growing adoption of federated login is the users' ignorance of its related privacy issues. This assumption pre-supposes, once more, that the lack of information is behind this behavior, and that in the presence of such knowledge, people will choose their privacy over convenience and usability.

The aggregated analysis showed that a significant number of respondents rely on federated login. The second iteration analysis did not find any significant statistical correlation between the expressed privacy concern, and the user's federated login behavior.

The above suggests that our respondents did not translate their expressed privacy concern into a corresponding usage pattern of federated login.

VI. Conclusions and Future Work

The above data and its analysis provide significant insights into the password habits of IT professionals. Although they possess enough cognitive knowledge to be fully aware of what constitutes an adequate password behavior, they fail to materialize it into practical habits in many instances. Evidently, the data analysis revealed no statistically significant correlation between the reported password behavior and the reported sensitivity level of the services. This strongly suggests that the ever more granular advice users get about adopting varying password behavior for each level of sensitivity, is not very efficient. Indeed, although cognitively convincing, the desired implications of such advice are not reflected in practice. This particular finding is in line with what Cormac Herley has highlighted in the "more is not the answer" paper [9]. More granular security advice is likely to be ignored due to other competing messages for users' attention.

While one might argue that IT professionals are scoring better than the general public in some metrics, the fact and matter is, the studied data is far from being satisfactory. Surely, we would be expecting a better return on investment for the educational efforts invested in end users. Furthermore, one is to remember that the respondents of this study do not only represent the profile of an ideal end user, but that they are also IT professionals within their organizations. Hence, they are likely to be handling security processes, or at least be holding privileged accounts within their organizations.

The aim of this research study was to explore the hypothesis that education is a necessary yet not by itself a satisfactory condition for ensuring a safe password behavior. The data of the survey supports the hypothesis. The data revealed interesting observations about the subset of respondents who exhibit satisfactory password habits for all services. As future work, we look forward to building upon this work and further investigating the characteristics which set apart this subset.

Further, the data revealed a significant proportion of respondents who had a shift in the expressed willingness to review their password habits between the beginning and the end of the survey. These respondents are also noted to have expressed a level 3 confidence in their password strength.

As a possible future work, we want to explore the following hypothesis: a healthy level of doubt in the strength of one's password habits and an expressed growing mind mentality, might yield a better correlation between cognitive knowledge and password practices. Being absolutely sure of the adequacy of your password habits, might make you more vulnerable, or at best, will not make you more secure

This study notes that over the last decade, there have been some voices presenting strong explanations for users' inadequate password habits. However, the desired implications of these studies have not materialized yet in the way IT professionals are designing solutions. The old mindset of "more education" is indeed still prevalent [9]. This study results are meant, hence, to confront IT professionals directly with their own password practices which fail to adhere to what they preach to end users through several educational channels. We would anticipate such a straightforward approach to fasten the mind shift of IT professionals. If their own solutions are failing them, then they would have more reasons to let go of their long held biases, and take mindful steps towards embracing the real reasons explaining end users' inadequate password habits. Implementing novel solutions in line with these studies would be the ultimate outcome.

Great insights have emerged as a result of significant research efforts targeted at resolving the online authentication challenge. However, given the urgency of the matter, we should strive to make the findings of these research studies relatable to the relevant people. This work subscribes to this philosophy. Indeed, this study targets in a straightforward manner IT professionals, gets them involved, and discusses findings that are very relatable to their concerns. IT professionals are a critical link in the security chain. The results of this study would be anticipated to increase the likelihood of IT professionals to let go of their old mindset, and fasten the pace at which they will start deploying new more appropriate solutions for their end users.

Lastly, as an IT community, we should open up to other disciplines, obtain a deeper understanding of the motivating factors for users' behavior, and become more humble in our perception of human capabilities. Knowing the right thing to do, does not necessarily mean that we will do the right thing. We must learn to practice what we preach.

Acknowledgments

We would like to thank the respondents for their time. We also thank our USEC 2015 anonymous reviewers, as well as our shepherd, Dr. Jens Grossklags for their valuable comments and guidance.

We, the authors, are funded by the informatics department of the University of Oslo, as well as COINS Research School of Computer and Information Security.

REFERENCES

[1] A. Adams and M. A. Sasse, "Users are not the enemy," Communications of the ACM, vol. 42, no. 12, 1999.

[2] R. J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd ed. Wiley Publishing, 2008.

[3] S. Anne and S. Lee, "Survey research and response bias," of the Survey Research Methods Section, ASA, 1993.

[4] H. Cavusoglu, B. Mishra, and S. Raghunathan, "The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers," Int. J. Electron. Commerce, vol. 9, no. 1, pp. 70–104, Oct. 2004.

[5] CSID. (2012) Consumer survey: Password habits: A study of password habits among american consumers.

[6] EVRY. (2013) Poor password security among norwegians.2013. [Online]. Available: https://www.evry.no/bedrift/investor/bors-ogpressemeldinger/evry-darlig- passordsikkerhet-hos-nordmenn-1867810/

[7] D. Florencio and C. Herley, "A large-scale study of web password habits," in Proceedings of the 16th international conference on the World Wide Web. Association for Computing Machinery, Inc., May 2007, pp. 657–666.

[8] C. Herley, "So long, and no thanks for the externalities: The rational rejection of security advice by users," in Proceedings of the 2009 Workshop on New Security Paradigms Workshop, ser. NSPW '09. New York, NY, USA: ACM, 2009, pp. 133–144.

[9] C. Herley, "More is not the answer," IEEE Security and Privacy magazine, 2014.

[10] W. Jennifer, "How to perform and interpret chi-square and t-tests," SAS Global Forum, 2012.

[11] S. Landau, H. Gong, and R. Wilton, "Financial cryptography and data security," in Financial Cryptography and Data Security, R. Dingledine and P. Golle, Eds. Berlin, Heidelberg: Springer-Verlag, 2009, ch. Achieving Privacy in a Federated Identity Management System, pp. 51–70.

[12] H. Mark, "The human side of security," Security Week, 2013.

[13] D. Prabhu, M. Adimoolam, and P. Saravannan, "Article: A novel dna based encrypted text compression," IJCA Special Issue on Network Security and Cryptography, vol. NSC, no. 2, pp. 36–41, December 2011, full text available.

[14] pwnedlist. (2012) Proactive credential monitoring. [Online]. Available: www.pwnedlist.com

[15] I. SafeNet. (2005) 2004annual password survey results.

[16] E. Stobert and R. Biddle, "The password life cycle: User behaviour in managing passwords," in Symposium On Usable Privacy and Security (SOUPS 2014). Menlo Park, CA: USENIX Association, Jul. 2014, pp. 243–255.

[17] V. R. Team. (2013) 2013 data breach investigations report.

[18] Verizon (2009) Comtrol computer crime news.

[19] T. William KM. (2006) In research method knowledge base.

APPENDIX 1: OVERVIEW OF THE SURVEY QUESTIONS

For questions 19─24, answers were required for each one of the below online services:

- Facebook
- Gmail/Google+/YouTube
- LinkedIn
- Online Video Games
- Work Studies Account
- Twitter.

TABLE VIII. OVERVIEW OF THE SURVEY QUESTIONS

Q1	Are you male or female?
Q2	What is your age?
Q3	What is your ethnic background?
Q4	Where are you currently living?
Q5	Which of the following best describes your current status?
Q6	Which of the following best describes your current occupation?
Q7	What is the highest degree you have received/working towards completing?
Q8	How would you describe your mood today?
Q9	How strongly do you agree/disagree with the below statement "People are inherently bad".
Q10	How Would you describe yourself?
Q11	How often do you log into social media networks (e.g. Facebook, Google+, etc.)?
Q12	How would you rate your computer Skills?
Q13	Have you ever been the victim of online theft...(stolen password, unauthorized transactions in your name)
Q14	How many web accounts do you currently have
Q15	In which year did you get your first email address?
Q16	What is the typical length of the password you use for the below?
Q17	How confident are you in the strength of the passwords you use to access your online accounts?
Q18	How do you store passwords?
Q19	What is the typical length of the password you use for the below?
Q20	For each of the below, do you by your own choice use mixes of different character types?
Q21	For each of the below, do you Ever change your password because you decide you do it?
Q22	For each of the below, how often do you forget your password then use the recovery option?
Q23	For each of the below, do you use a Unique password or is it reused with another account?
Q24	How sensitive do you consider the below online service are to you?
Q25	Do you use an online password Manager to store/manage your credentials?
Q26	Social login is the option to use your profile from one service to register/login into another online service
Q27	Do you worry about the privacy of your online presence?
Q28	Do you think you should improve your password habits?
Q29	Do you have further comments about your web password and online identities that you would like to share?

APPENDIX 2: SAMPLE OF AGGREGATED RESULTS

Below are the answers collected from the questions which define the profile of our respondents:

TABLE IX. THE RESPONDENTS' PROFILE

Answer Options for gender	**Response Percent**
Male	84.8%
Female	15.2%
17 or younger	0.0%
18-20	1.5%
21-29	43.9%
30-39	22.7%
40-49	13.6%
50-59	13.6%
60 or older	4.5%
Primary School	0.0%
High school degree or equivalent	1.5%
Professional training	0.0%
Bachelor's degree or equivalent	12.1%
Master's degree or equivalent	68.2%
PhD	18.2%
1 online account	0.0%
2-5 online accounts	22.7%
6-10 online accounts	16.7%
11-20 online accounts	9.1%
21-50 online accounts	24.2%
>50 online accounts	27.3%