2019-01-09

Aligning Security Practice with Policy: Guiding and Nudging towards Better Behavior

Furnell, SM

Aligning Security Practice with Policy: Guiding and Nudging towards Better Behavior

Steven M. Furnell
University of Plymouth, UK
Edith Cowan University, Australia
Nelson Mandela University, South Africa
steven.furnell@plymouth.ac.uk

Faisal Alotaibi
University of Plymouth, UK
faisal.alotaibi@plymouth.ac.uk

Rawan Esmael
University of Plymouth, UK

Abstract

Despite an abundance of policies being directed towards them, users often struggle to follow good cybersecurity practice. Recognizing that such behaviors do not come naturally, a logical approach is to ensure that users are guided and supported in knowing what to do and how to do it. Unfortunately, such support is often lacking. The paper uses the example of password authentication as a specific context in which cybersecurity behavior is frequently criticized, but where users are often left to manage without sufficient support (as evidenced by examining the lack of related guidance and enforcement of good practice on leading websites). The discussion then proceeds to look at the effect of actively supporting the user, drawing upon the results from two experimental studies (one looking at the practical impact of guidance and feedback upon users' password choices, and the other examining the effect of gamifying the password selection experience). The results collectively show that such efforts can have tangible positive effects upon user behaviors. While the specific findings are focused upon passwords, similar principles could also be applied to other aspects of user-facing security.

1. Introduction

Modern organizations are now characterized by a fundamental dependence upon information technology and knowledge management. This in turn introduces a fundamental reliance upon cybersecurity in order to ensure that related systems and data are available when needed and protected from harm. Unfortunately, however, those using the systems are often poor at cybersecurity, which tends to introduce resultant challenges when they are nonetheless required to use it.

The problem spans many domains, and even those working directly in the field, in areas such as information systems and knowledge management, cannot be relied upon to have the necessary skills by default [1]. As a result, we have environments which are geared towards extensive knowledge sharing, but with inadequate posture towards knowledge protection. Indeed, while security and protection have long been identified amongst the critical success factors for knowledge management systems [2,3], little is often done to position the people involved to become compliant. This is not to say that technology is not provided with the *potential* to enable security; it is rather a case that those at the receiving end are often not adequately equipped to use it. Similarly, policies can be set that require security to be maintained, but without a level of accompanying support this is less likely to become a feature of actual practice. Unfortunately, while there are some aspects of information technology that users often appear to take to without requiring much guidance, support, or instruction (with the use of social media and mobile apps being good examples), information security is rarely amongst them. As a result, while users may still be able to get by, doing so without suitable support often means that they develop and adopt bad practice in the process, which then becomes their default behavior across in other contexts.

This paper presents evidence of the problems that can result from a lack of security support and guidance, and then proceeds to examine how changes in users' awareness - and more particularly their resultant practices - can be achieved if tangible attention is directed towards assisting them (e.g. by providing guidance and nudges towards appropriate, safer behaviors). The problem of password usage is used as a specific focus for the discussion, with evidence drawn from a number of sources and experimental studies to demonstrate both the current challenge and the impact that more user-focused approaches may

have. Section 2 presents some background to the problem, looking at the weaknesses often seen in password usage and examining some evidence of why this may occur. Section 3 then proceeds to consider the impact of a more user-focused approach, examining the effect of supporting password use with baseline guidance and feedback. Section 4 then goes beyond this to examine how user awareness and understanding can be further enhanced via gamification of the security tasks that they otherwise find challenging. The paper concludes with section 5, which reflects upon the overall results and discusses the wider implications of the findings.

2. Evidencing a lack of user support

If security and protection are critical success factors for knowledge management systems, then in turn the people involved are critical success factors for security. Unfortunately, the two are not natural bedfellows and users are regularly cited as a weak link in cybersecurity, criticized for their lack of interest and attention in terms of protecting systems, devices and data. However, while users can certainly be held accountable in some contexts (most notably if they are actively ignoring clear advice), there are many scenarios in which their behavior becomes easier to explain if we look at the extent to which they have been guided or supported to do things any differently. To be clear on the definition here, guidance and support does *not* mean simply setting a policy and expecting users to follow it. What it actually refers to is taking the time and effort to ensure that there is a means for users to be made aware of what they are supposed to do, ensure that they understand how to do it, and ideally also appreciate *why* it is relevant, and have an opportunity to be reminded of it at the relevant time. Contrasting this to many so-called awareness-raising approaches (which often do little more than circulate a document by email and expect it to be adhered to), and there is often a gap to be bridged.

To consider a specific example as a basis for discussion and evidence, we can look at password-based authentication. This is one of the most familiar aspects of day-to-day cybersecurity, and it is directly user-facing. Moreover, it is an aspect of security that has been with us for years, and while our devices (particularly smartphones) have now evolved to incorporate alternative options such as biometrics, passwords remain the dominant form of authentication across organizational systems and online services (and even the biometric-equipped devices still require passwords or PINs to be in place as underlying fallback methods). Thus, knowledge workers will not only be routinely familiar with using them on a daily basis but will typically have a multitude of devices and accounts that require them.

In spite of all this, passwords are regularly cited as a prime area in which users behave poorly and fail to follow basic good practice, and related research can be found dating back over many decades [4,5]. In more recent years the problem has been regularly evidenced by the widely-cited findings from SplashData, who publish an annual list of the worst passwords [6]. Table 1 lists the top-ten most frequently encountered passwords from the last three instances of their study, and clearly shows that bad choices readily persist from year to year with no obvious sign of improvement. Similarly, other findings can be easily located furthering highlight that – despite years of use as a standard security feature – passwords continue to be used badly [7]. As a result, they are estimated be implicated in more than 80% of breaches and to incur a significant management cost to organizations (with a single password reset estimated to cost over £50) [8]. At the same time, they have proven to be form of authentication this is difficult to replace, as no other approaches offer ideal alternatives in terms of usability, deployability and security [9].

Table 1. SplashData top-10 worst passwords

Rank	2016	2016	2017
1	123456	123456	123456
2	password	password	password
3	12345678	12345	12345678
4	qwerty	12345678	qwerty
5	12345	football	12345
6	123456789	qwerty	123456789
7	football	1234567890	letmein
8	1234	1234567	1234567
9	1234567	princess	football
10	baseball	1234	iloveyou

Of course, there is no shortage of guidance on how to choose and use passwords more effectively, with an example provided by [10]. A web search readily reveals numerous examples, and many organizations will themselves have taken the time to write password policies and may even have taken some steps to communicate them to staff. However, there is often a mismatch between the *existence* of security policies and guidance, and the effective provision and promotion of it at the time that related decisions are actually being made – which, in this case, refers to the point at which users choose their passwords in practice.

As a specific example, we can consider the results of a recent assessment of the password guidance and enforcement practices on a series of leading websites [11]. This examined the extent to which the sites provided users with password guidance at initial sign-up, as well as if they elected to change their password, or indeed were forced to change it because the original was forgotten. The assessment also considered the extent to which any restrictions on password choices were provided at the initial sign-up stage (recognizing this as the most crucial point, given that after this the users would have accounts – potentially holding further personal details – and these passwords might be the only things protecting them against impostor access).

The sites were selected from amongst the Alexa global list of 'The top 500 sites on the web' (see www.alexa.com/topsites), focusing upon the top ten sites presented in English and with distinct password processes (i.e. avoiding sites such as YouTube or Google.co.in, which used the same approach as the main Google site). The resulting sites and the key findings are presented in Tables 2 and 3. The former looks at the extent to which users were provided with guidance or feedback at initial sign-up, and it can clearly be seen that the majority of sites allowed users to proceed without any upfront information. As such, it would not be surprising to find users attempting to use weak or otherwise ill-advised password choices, which then places more emphasis on the ability of the site to prevent such options from being accepted.

Table 2. Provision of password guidance and meter at sign-up

Site	Guidance	Meter
Amazon	×	×
Facebook	×	×
Google	✓	×
Instagram	×	×
Microsoft Live	×	×
Netflix	×	×
Reddit	×	✓
Twitter	×	×
Wikipedia	×	×
Yahoo!	×	×

The fact that only one out ten of the sites offered users interactive feedback on their choices via a password meter (or strength ratings) was unexpected, as earlier runs of the study had found this to be more prominent. Indeed, the 2011 version of the assessment had found seven out of ten sites to be using password meters or ratings at the sign-up stage [12]. The decrease in use is somewhat surprising, given that it is not only serving to *remove* assistance, but also appears to overlook the positive effects that appropriately implemented meters have been found to deliver [13].

Meanwhile, Table 3 looks at the rules applied in order to see if the site will accept a given password choice. A total of six aspects were assessed:

- Is a minimum password length enforced?
- Does the site prevent the user from using their surname as the password (if this information is collected as part of registration)?
- Does the site prevent the user ID (login name) from being reused as the password (or the user ID part of their email address, if this is used as the login identity)?
- Does the site prevent the use of 'password'?
- Does the site require users to use more than one character type in the passwords (i.e. where types are upper and lower case letters, numeric characters and punctuation symbols)?
- Does the site prevent the use of dictionary words (with a series of test words being used as candidates – including 'diamonds', 'dictionary' and 'football' – the latter two of which were prominent in the SplashData lists, alongside 'letmein' and 'iloveyou' which were also tested as part of this criterion).

As can be seen from the table, the level of enforcement is decidedly mixed, and various viable tests are excluded by some sites. If an option is found to be restricted, then at this point the user will get a feedback message to tell them that their password choice is not permitted. However, they notably have to determine this through a process of gradual discovery rather than having been advised upfront. In short, the sites clearly *have* policies, but most do not elect to tell the users what they are in a direct and upfront way. Discovering things in a piecemeal manner is likely to frustrate some users, especially if the feedback then received is still not specific enough to help them understand. Indeed, we can consider the following examples of messages offered by the sites assessed:

- Facebook – "Please choose a more secure password"
- Twitter – "Please enter a stronger password"
- Yahoo – "Please create a stronger password, the one that you submitted is too easy to guess"

Clearly the flaw in all three cases is that while they are arguably attempting to nudge the user by informing them that their current choice is not acceptable, the

messages are giving no useful insight into what would make it better. If users *knew* what 'stronger' and 'more secure' looked like, then they arguably might have avoided offering weak choices in the first place.

As mentioned above, this assessment of websites was actually a repeat of a study that was first conducted in 2007 [14], and half of the sites that were included in the top-10 list then remained there in 2018. However, in over a decade, there have been only marginal improvements in the related password practices, and even now only a small minority of the leading sites (specifically Google, and arguably Yahoo and Microsoft Live) are taking what could be seen as comprehensive stance in terms of enforcing baseline good practice. While Yahoo appears to accept shorter passwords and is indicated as not enforcing composition, there is actually a bit more too it in terms of the passwords that will be accepted. Specifically, a 7-character password is only permitted if it includes all four possible character types (i.e. upper and lower-case letters, numeric and punctuation). If fewer character types are used, then the password itself must be longer.

The most positive finding in the 2018 assessment was that eight out of ten sites now offered some form of additional login security, via two-step verification or two-factor authentication options. However, while they were *available*, these features were not enabled by default and were not prominently promoted. Instead, users typically had to go looking for them in their account security settings rather than having the opportunity highlighted to them.

A clear message arising from this assessment is therefore that, although passwords are widely-recognized as being used poorly, there is still a paucity of support to encourage them to be used better – even amongst the sites that others might regard as a benchmark of standard/acceptable practice (e.g. other providers looking to establish the authentication provisions on their own systems or online services might look at what these leading players are doing and consider this to be a suitable standard to follow). Of course, these sites may have various reasons for not doing more. For example, they may consider that users are not storing anything that warrants a greater level of protection (although users themselves may disagree with this, given that various personal and payment-related details can be held in several cases), or they may not want to introduce anything that may act as an impediment to getting users to sign-up. Indeed, looking at later stages, such as password change and (especially) reset, it is often apparent that several sites do then provide significantly more information. In addition, one other possible reason for not providing guidance and feedback may be the belief that users will ignore it anyway. Indeed, it may be reasoned that they must surely be familiar with passwords by now, and so telling them the rules again is hardly likely to have any impact. In practice, however, this can be far from the case, and the next sections proceed to examine the differences that supporting the user can actually make.

3. Examining the effect of guidance and feedback

As the website evaluation has consistently revealed over the years, there is a frequent tendency to provide users with security mechanisms, but then leave them to fend for themselves rather than provide effective guidance to support their use. This clearly increases the potential for users to make poor and ill-informed security decisions, which may actually increase risk.

Table 3. Password restriction applied at registration

Site	Restrictions enforced at sign-up					
	Min. length (+max if stated)	Prevents Surname	Prevents User ID	Prevents 'password'	Enforces composition	Prevents dictionary
Amazon	6	×	×	×	×	×
Facebook	6	✓	-	✓	×	✓
Google	8	✓	✓	✓	✓	✓
Instagram	6	×	✓	✓	×	~
Microsoft Live	8	-	✓	✓	✓	~
Netflix	4-60	-	×	×	×	×
Reddit	6	-	×	×	×	×
Twitter	6	×	×	✓	×	~
Wikipedia	×	×	✓	✓	×	~
Yahoo!	7	✓	✓	✓	×	✓

(✓ = enforced; × = not enforced; ~ = partially enforced; - = item not collected by site)

For example, poor decisions may result in users being left under-protected or even exposed as a consequence. The problem goes well beyond the realm of authentication and passwords, but this context can again be used to illustrate the positive effect of doing things differently. Far from being the lost cause that some may instinctively assume, user behavior is found to have significant potential to improve.

As such, a more substantial study was conducted, with the aim of enabling more conclusive investigation, as well as exploring several parameters of potential influence (as opposed to simply a contrast between guided and unguided use).

In order to test the effect of guidance and feedback, a practical experiment was conducted in which a group of users were asked to perform a task involving password selection, but with differing levels of guidance and feedback to support them [16]. In order to ensure that the experiment was realistic, the participants were unaware that they were participating in a password-related study. From their perspective the primary task was to complete an online questionnaire about social media practices, and the creation of a password-based user account was an incidental activity required as part of the process (note that ethical approval was obtained in order to enable this mild deception). A total of 300 users were involved in the study, split into five equal-sized groups that then received differing levels of support in selecting their passwords. The characteristics in each case were as follows:

- **Scenario 1:** No guidance was provided, other than a request not to re-use a password already used on other systems.
- **Scenario 2:** Basic password guidance was provided alongside the password entry and confirmation boxes (as shown in Figure 1).
- **Scenario 3:** Basic guidance agsin, alongside the provision of a traditional password meter that rated choices as Weak, Medium or Strong.
- **Scenario 4:** Basic guidance combined with emoji-based feedback (a sad red-colored face for weak choices, a yellow neutral face for medium, and a smiling green face for strongly-rated choices).
- **Scenario 5:** As for group 4, but with emojis being accompanied by more emotive feedback messages ("This is not good enough!", "Ok, but you can still do better!", or "Well done!")

In all cases, the password choices themselves ultimately remained unrestricted – users could elect to use a single character password, a dictionary word, or anything else and the system would permit it. As such, the end results observed in terms of password choices were purely informed and differentiated on the basis of the guidance and feedback provided. The passwords themselves were all rated using the same scoring algorithm [17] and categorized as weak, medium or strong depending upon the score achieved. The algorithm scores passwords out of 100, awarding five points for each unique characters, two points for another instance of a character already used, and 15 points for each new character type (e.g. uppercase, lowercase, numeric or punctuation) *after* the type initially used. Scoring boundaries were then defined as weak for 40pts or less, 41-70pts for medium, and above this for strong (noting that any long passwords scoring over 100 were capped at that level). So, a password such as 'luke33' would score 37pts and be rated as weak, while 'foL34p!' (65pts) would be medium, and 'Lafe@9856!e' (82pts) would be strong. The results were then stored to enable comparison of the performance across the different scenarios.

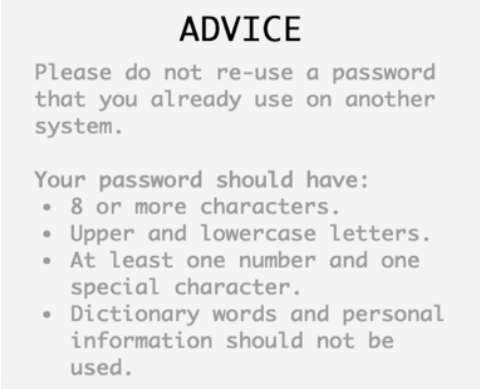

Figure 1. Baseline password selection guidance offered to participants

The resultant findings are presented in Figure 2, and the most striking aspect is the difference in the proportion of weak-rated passwords between scenario 1 and all of the others. This clearly suggests that the provision of guidance at the point of relevance can make a tangible difference to user decisions, and (in the case of passwords) shows that they do not have to be forced into making stronger choices solely by means of rules and restrictions. The more moderate further differences that were then made via the various feedback mechanisms (meter, emojis, messages) suggests that such nudges can also deliver further voluntary improvements.

One point that should be acknowledged here is that the difference observed between the meter and emoji-

based mechanisms may be as a result of the novelty value of the latter approach (i.e. users may have responded more to it because it was unusual, whereas many participants would have been likely to have been familiar with a traditional password meter approach from their experiences in other systems). Nonetheless, the findings as a whole clearly demonstrate positive impact from *any* of the additional provisions, and so the key lesson is that offering *something* can pay off.

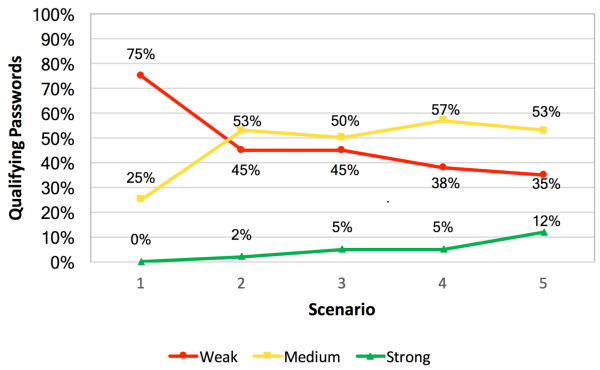

Figure 2. Distribution of the password strength ratings across five guidance-feedback scenarios

4. Gamification of security awareness

Beyond simply ensuring that guidance is provided, another step is to try to make it more engaging, so that it increases the chance of users (a) giving their attention and (b) internalizing the message. To some extent, this is what password meters already try to do, as there is a basic form of interaction going on between what the user chooses, what they receive as their rating, and what they might then do to improve it. However, taking this further, it is possible to explicitly gamify the awareness process, presenting the lessons and techniques in a context that engages users while also helping them to acquire and practice key knowledge and skills. The relevance and benefit of gamification is recognized in many situations [18], but its application is arguably well-suited to security given that this is certainly an aspect that users do not tend to enjoy by default and various examples of gamification can already be found in the security domain, addressing both the end-user audience and security professionals [19,20]

To this end, a further experimental study examined the potential to engage user interest in security – and enhance resulting awareness and understanding – via the use of gamification in mobile apps. A number of game concepts have been designed [21], and amongst those taken forward for proof-of-concept implementation by the authors was a game entitled Password Protector. This is intended to familiarize users with applying good password practices, as well as testing and developing their ability to generate and remember strong password choices.

The game was developed using C# and the Unity3D platform, and the basic premise is for players to create and remember suitably strong passwords, but working against the clock and with a restricted set of character choices to work from. The main interface is shown in Figure 3, and it can be seen that the player is presented with a set of letters in the top right (which can be alternated between upper and lower case using the control to the left), plus a set of numeric and punctuation characters (again, the onscreen interface requires them to alternate between these in order to both optimize the layout of the screen and also to increase the challenge in completing the task within the time limit). These characters are chosen at random for each new game/level, thereby requiring the user to make effective use of the characters available to them (and preventing them from relying upon pre-determined choices that they might otherwise plan to use if they had a full character set available).

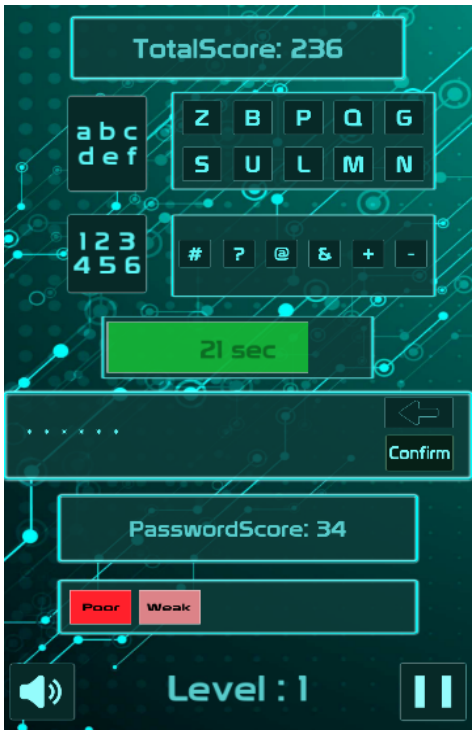

Figure 3. Password Protector game user interface

Table 4. Participants' responses to password-related statements before and after use of Password Protector

Statement		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
I understand the concept of password strength	Pre-study	18%	16%	20%	14%	32%
	Post-study	70%	26%	4%	0%	0%
Increasing the length increases the strength of the password	Pre-study	30%	18%	14%	18%	20%
	Post-study	64%	14%	14%	4%	4%
Use of different character types in my password increases its strength	Pre-study	38%	14%	20%	0%	16%
	Post-study	72%	24%	4%	0%	0%
I can remember passwords of more than 8 characters	Pre-study	12%	20%	22%	24%	22%
	Post-study	56%	22%	14%	2%	6%
I find password meters useful in checking if my password is strong or not	Pre-study	16%	22%	34%	12%	16%
	Post-study	64%	22%	12%	0%	2%

The player has a time limit within which to make their choice, and the available time decreases as the game proceeds to later levels (e.g. at Level 1 the limit is 90 seconds, then 70 at Level 2, 50 at Level 3, 40 at Level 4). However, the time they take also affects the time limit for re-entering the password a second time. For example, if a user enters their initial choice within 15 seconds, they will have 20 seconds to enter their verification attempt (i.e. the time they took to make the initial choice, plus a slight additional margin to ensure that they have some thinking time if required before having to re-enter their choice). This again adds to the challenge of the game, while at the same time aiming to avoid the impression that the game is trying to encourage choices to be made at speed. It also seeks to dissuade players from rushing to create a password without thinking about it, because they will still have to be able to re-enter it within a similar timeframe.

Users' choices are assessed in real time by a password meter, which rates them on a 5-point scale (Poor, Weak, Moderate, Good, Strong). Users must offer a password that is at least rated Moderate, but entering stronger choices increases the resulting score. So, while successfully completing a level basically requires users to choose, enter, remember and re-enter a qualifying password within the time limit, they can score differently according to the length and complexity of the passwords they attempt. The incentive to replay is therefore to go further and/or better their earlier score, and in the process they will be honing their password selection and memory abilities.

A practical evaluation was conducted that included 50 participants (34 male, 16 female), and involved the app being made available to them to use over a two-week period. Pre- and post-study surveys were then used to assess their attitudes and awareness on either side of the experience.

The pre- and post-study surveys asked participants to respond to a number of statements regarding their understanding and use of passwords. The related results are presented in Table 4, and it is very notable that attitudes have become more positive as a result of the exposure to the game. In most cases, the statements were related to areas of understanding and appreciation of password practice, but the 4th statement, around remembering passwords, relates to the participants' perception of their own *ability* to do perform the task, and it seems apparent that playing the game has increased confidence in the ability to do something that only a minority of users initially believed they were able to do (indeed, prior to playing the game, only a third believed that they could do it, but this subsequently rose to over three quarters).

In addition to requesting responses to the statements, the study also went beyond simply assessing what the users *claimed* and also evaluated their ability in practice. Specifically, a further task in both the pre- and post-study surveys asked the participants to provide an example of what they considered to be a strong password. These attempts were then evaluated by the research team, by feeding them into the same password scoring algorithm as used within the game. The notable finding here – and perhaps the most significant finding from this phase of the study – was that the average password strength score rose from 59% in the pre-study surveys to 80% in the post-study version. This suggests a genuine and tangible increase in users' *understanding* of what it takes to create a stronger password.

It should be noted that the game is *not* attempting to provide any evidence of the players' ability to remember and recall strong passwords in the longer-term. What it hopes to demonstrate to users is that they are able to create and re-enter better passwords

without requiring much additional time or effort. As such, the intent (and apparent effect based on the accompanying survey results) is to increase the user's *confidence* in their own ability to do this aspect of the wider security task.

As an aside, it should be noted that users were also asked to rate the game itself in terms of aspects such as design, ease use, interest, and fun (all of which are relevant if it is something the user is expected to enjoy playing and to come back to, rather than be asked to use but still regard as a chore). In these respects, the results were significantly positive, with all users indicating that the game was fun and provided an interesting means to learn about this aspect of cybersecurity.

The findings again contribute towards a wider view that the users can - and will - do better with password security if they are given a means of support to do so. As mentioned above, Password Protector was just one of several game concepts that were devised as part of this particular project, and others targeted different aspects of cybersecurity that have the potential to affect the general user community. Indeed, another game concept that was also implemented and evaluated in the same manner was titled Malware Guardian, which sought to increase players' awareness of malware threats by requiring them to act as the defender of a target system (while also emphasizing the importance of supporting actions such as system updates and backup in ensuring their overall protection). While a full examination of the related results is outside the scope of the current paper, it can be noted that this game was also met with a positive evaluation. This again helps to support the case that while passwords have been used as the specific focus in the current discussion, the underlying points around user awareness and support can be readily applied to other aspects of cybersecurity as well.

5. Conclusions

User behavior is often the downfall of what might otherwise be effective security mechanisms. However, this does not necessarily mean that the users themselves are at fault, as we cannot reasonably expect them to manage knowledge systems securely if they lack the knowledge of how to do so. It is not just a question of instructing them or enforcing restrictions upon them – the point is helping them to recognize and understand the security issues form themselves. Although setting and enforcing policy can have an effect, and may even succeed in getting users to do what is needed in a particular context, getting them to understand things stands a better chance of achieving acceptance and affecting their default behaviors (which in turn has clear links back to established theories, such as those relating to Reasoned Action [22] and Planned Behaviour [23]). Of course, a lack of awareness or understanding is not the barrier for *all* users; some simply do not care enough and lack the incentive or motivation to comply. However, while such users clearly exist, it is reasonable to believe that they are in the minority, and so the provision of appropriate support is still a fair expectation for the remainder that we have a chance of appealing to.

The password-related findings help to support these beliefs. By default, systems and services often do very little to present upfront guidance and support (even though users may ultimately be prevented from doing some of the wrong things via underlying restrictions). As a result, we continue to see users gravitating towards bad practice when the opportunity arises (as illustrated by the SplashData findings). However, it clearly does not have to be this way. The use of password guidance and feedback had clear effects upon the users within the experimental study, and a significant proportion moved away from weak passwords simply as a result of information being provided to them. They still had the option to make weak choices, but the provision of guidance and nudges at the appropriate point (i.e. while they were making the security decision concerned) had a positive effect without resorting to any enforcement of rules and restrictions. Similarly, the findings from the Password Protector game suggested that if users are shown the effects of different behaviors, they may be inclined to choose the better ones. Moreover, the experience of playing the game appeared to changed users' perceptions of what they could do (e.g. some may previously have avoided choosing longer passwords on the mistaken belief that they would not remember them), and post-testing suggested that this had actually changed behaviors. Given that the study was not longitudinal, it could clearly be questioned whether such changes might be transient, but the collective findings suggest that, with appropriate reminders and reinforcement, the effect could become longer term.

For the avoidance of doubt, these findings should not be mistaken for an argument towards maintaining passwords over other forms of authentication. Passwords themselves are *still* an inadequate and unfriendly approach, and simply do not scale to the number of systems that now expect us to use them. No matter what guidance and nudges are given, most users will find it impossible to choose strong passwords for all the devices, sites and services that they use without resorting to duplication and/or the use of some form of password management solution. Moreover, there are still going to be categories of attack against passwords

(e.g. keylogging and backend breaches) in which the strength will have no impact anyway, plus it has also been argued that (past a certain point) pushing for better password composition is not worth the additional user effort required to achieve it [24]. However, passwords continue to be used, and thus the point remains that we could support people better in using them.

In terms of how to take the lessons into practice, the findings should not be regarded as a script that is expected to be followed exactly. For example, it is not proposed that all users should be *required* to play the Password Protector before choosing passwords on other systems – the point is rather that doing so has been shown to have a positive impact, and so has likely value within a wider arsenal of approaches to password education (which would also include providing guidance and feedback during actual password selection). Indeed, no single technique is being advocated as the answer in its own right, and over-emphasis of any particular approach would in any case be likely to lead to diminishing returns over time and lead to the risk of user fatigue. The hope is to promote understanding that judicious availability and usage of a *range* of interventions has the likelihood of improving matters over the typical level of success that has traditionally been seen with passwords. Moreover, even passwords are just being used as an example context here; the wider point is that better understanding, use and acceptance of security more generally could be achieved by promoting it to users in more effective ways.

The fact that users struggle with passwords and would benefit from support in using them is not a new finding. Indeed, [25] had flagged the need for instruction, training and constructive online feedback back in 1999. The disappointing fact is that we not only seem no closer to addressing the situation with passwords, but we now also suffer the same problems with other forms of user-facing security as well. Illustrative examples of further security tasks and responsibilities that users might be encouraged to enact better would include:

- Anti-malware scanning and updating
- Backup
- Data leakage/loss prevention (including avoidance of phishing and other forms of social engineering)
- Privacy management (relating to their own data and that of the organization)
- Vulnerability management (i.e. patching)

All of these represent contexts in which users are again prone to making choices borne out of ignorance or geared towards serving their own convenience, but where their decisions might arguably change if they were better informed. Added to this, there are many cases in which knowledge workers are basically at the mercy of technology provided, and so even if they want to be security-conscious their efforts may be frustrated by tools that are not sufficiently intuitive or usable [26]. With all of these factors in play, it is certainly not appropriate or fair to simply shrug and blame the users for the situation. Only if reasonable attempts have been made to guide and support them can they be viewed as being at fault for the cybersecurity issues that they may introduce. This in turn links back into the overall provision of an effective knowledge management structure [27], with governance mechanisms being used to ensure that policies and guidance are promoted to staff in an appropriate manner.

6. References

[1] M. Jennex and A. Durcikova, “Integrating IS Security with Knowledge Management: Are We Doing Enough?”, International Journal of Knowledge Management, vol. 10, no. 2, 2014, pp1-12.

[2] Y. Malhotra, “Why knowledge management systems fail: enablers and constraints of knowledge management in human enterprises”, in Holsapple C.W. (eds) Handbook on Knowledge Management, Springer, Berlin, 2004, pp. 577-599.

[3] M. Jennex and L Olfman, “A Model of Knowledge Management Success”, International Journal of Knowledge Management, vol. 2, no. 3, 2006, pp51-68.

[4] R. Morris and K. Thompson, “Password security: a case history”. Communications of the ACM vol. 22, no. 11, 1979, pp594–7.

[5] D. Klein, “Foiling the Cracker: A Survey of, and Improvements to, Password Security”, Proceedings of the Second USENIX Security Workshop, Portland, Oregon, August 1990, pp.5-14.

[6] SplashData, “Worst Passwords of 2017 – Top 100”. https://www.teamsid.com/worst-passwords-2017-full-list/ (accessed 15 June 2018).

[7] LastPass, Psychology of Passwords: Neglect is Helping Hackers Win, LogMeIn Inc, 2018, https://www.lastpass.com/psychology-of-passwords (accessed 15 June 2018).

[8] S. Palfy, “How Much do Passwords Cost your Business?”, InfoSecurity Magazine, 14 June 2018, https://www.infosecurity-magazine.com/opinions/how-much-passwords-cost/ (accessed 15 June 2018).

[9] J. Bonneau, C. Herley, P.C. van Oorschot, and F. Stajano, “The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes”, in Proceedings of the IEEE Symposium on Security and Privacy 2012, pp553-567.

[10] NCSC, “Password Guidance: Simplifying Your Approach”, National Cyber-security Centre, 7 Jan 2016. www.ncsc.gov.uk/guidance/password- guidance-simplifying-your-approach (accessed 15 June 2018).

[11] S. Furnell, “Assessing website password practices – Over a decade of progress?”, Computer Fraud & Security, July 2018.

[12] S. Furnell, “Assessing password guidance and enforcement on leading websites’. Computer Fraud & Security, Dec 2011, pp.10-18.

[13] B. Ur, P.G. Kelley, S. Komanduri, J. Lee, M. Maass, M.L. Mazurek, T. Passaro, R. Shay, T. Vidas, L. Bauer, N. Christin and L.F. Cranor, “How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation”, Proceedings of the 21st USENIX conference on Security symposium, USENIX Association Berkeley, CA, 2012.

[14] S. Furnell, “An assessment of website password practices”, Computers & Security, vol. 26, nos. 7-8, 2007, pp.445-451.

[15] S. Furnell and N. Bar, "Essential Lessons Still Not Learned? Examining the Password Practices of End-Users and Service Providers", International Conference on Human Aspects of Information Security, Privacy, and Trust, Las Vegas, USA, 21-26 July 2013, pp217--225.

[16] S. Furnell, W. Khern-am-nuai, R. Esmael, W. Yang, and N. Li, “Enhancing security behaviour by supporting the user”, Computers & Security, vol. 75, 2018, pp1-9.

[17] K.Mohamed, *password-meter-tutorial. 19 September 2014.* https://github.com/lifeentity/password-meter-tutorial (accessed 31 August 2018).

[18] A, Pandey, “6 Killer Examples Of Gamification In eLearning”, 6 October 2015, https://elearningindustry.com/6-killer-examples-gamification-in-elearning (accessed 15 June 2018).

[19] T. Denning, Z.N. Peterson and M. Gondree, "Security through play”, *IEEE Security & Privacy*, vol. 11, no. 3, 2013, pp.64-67.

[20] W. Ashford, “Automation and gamification key to cyber security”, ComputerWeekly.com, 3 April 2018, https://www.computerweekly.com/news/252437833/Automation-and-gamification-key-to-cyber-security (accessed 15 June 2018).

[21] F. Alotaibi, S. Furnell, I. Stengel and M. Papadaki, “Enhancing cyber security awareness with mobile games”, 12th International Conference for Internet Technology and Secured Transactions (ICITST), Cambridge, UK, 11-14 December 2017, pp129-134.

[22] M. Fishbein and I. Ajzen, Belief, attitude, intention and behavior: An introduction to theory and research. Reading, MA: Addison-Wesley, 1975.

[23] I. Ajzen, “The theory of planned behavior,” Organizational Behavior and Human Decision Processes, vol. 50, no. 2, 1991, pp179–211.

[24] D. Florencio, C. Herley and P.C. Van Oorschot, “Pushing on String - The 'Don't Care' Region of Password Strength”, Communications of the ACM, vol. 59, no. 11, Nov. 2016, pp66-74.

[25] A. Adams and M.A. Sasse, “Users are not the enemy”, Communications of the ACM, vol. 42, no. 12, Dec. 1999, pp40-46.

[26] J.R.C. Nurse, S. Creese, M. Goldsmith and K. Lamberts, "Guidelines for usable cybersecurity: Past and present," *2011 Third International Workshop on Cyberspace Safety and Security (CSS)*, Milan, 2011, pp21-26.

[27] M. Jennex, “Re-Examining the Jennex Olfman Knowledge Management Success Model,” 50th Hawaii International Conference on System Sciences, HICSS50, IEEE Computer Society, January 2017.