Good guidance or mistaken misdirection: Assessing the quality of password advice

Steven Furnell
Security Research Institute, Edith Cowan University, Perth, Western Australia
Centre for Security, Communications and Network Research, University of Plymouth, Plymouth, United Kingdom
Centre for Research in Information and Cyber Security, Nelson Mandela University, Port Elizabeth, South Africa
steven.furnell@plymouth.ac.uk

Paul Haskell-Dowland
Security Research Institute, Edith Cowan University, Perth, Western Australia
p.haskelldowland@ecu.edu.au

Abstract

Modern websites often require users to create accounts in order to utilise services or store information. With password leaks appearing on an almost daily basis and being widely publicised, it is reasonable to assume that users should be adopting appropriate practices to secure their accounts and minimise their exposure to compromise. Despite the adoption of various password creation practices (e.g. password length and composition rules), appropriate guidance is often lacking. In order to bridge this gap, cybersecurity advice websites provide guidance to users to assist with the selection and use of appropriate passwords. This paper critically evaluates the advice provided by national-level guidance sites (often supported or implemented by government bodies). This guidance is likely to be a key source of reference for the populous of the respective countries and, as such, is worthy of examination to determine the effectiveness of the advice and the potential impact on individuals. As such, this paper presents a qualitative evaluation of the password guidance offered to end-users from a series of national cybersecurity advisory websites. The assessment is based upon a series of 11 criteria relating to password selection and management, with the guidance being rated as to whether it fully or partially addresses the related issues. This reveals that there is considerable variation in the scope and quality of the material, with some of the sources having areas of omission or even potential misdirection in the guidance being offered.

Introduction

Passwords are one of the most long-established cybersecurity technologies, in use across all manner of technology devices (from desktops and laptops to smartphones and tablets, plus extending into various IoT and smart devices), as well as providing the standard form of authentication for online sites and services. At the same time, they are amongst the most widely criticised forms of security, repeatedly shown to be poorly selected and managed by many of their users, and technologically dismissed as a relic of the past (Jobusch and Oldehoeft, 1989; Ives et al., 2004; Weber et al., 2008; Alomari and Thorpe, 2019). However, despite all the criticism, passwords are very much still in use, and extensively so. In all the time that they have been with us, successive new generations of users have continued to make the same mistakes and then fundamentals of good practice have failed to be learnt. As evidence of this, Table 1 summarises the top ten worst passwords from the most recent sets of results published by SplashData (TeamsID, 2016-2020). As can readily be seen, very little changes in the composition of the annual top ten, and there continues to be

significant use of passwords that ought to be dismissed out of hand. It is perhaps surprising that systems do not block their use, or that users are still making such poor choices. And it raises the question of why the situation does not improve, despite such readily recognised problems and with a wealth of publicised evidence demonstrating the common failings.

Table 1: Top ten worst passwords by year

Rank	2015	2016	2017	2018	2019
1	123456	123456	123456	123456	123456
2	password	password	password	password	123456789
3	12345678	12345	12345678	123456789	qwerty
4	qwerty	12345678	qwerty	12345678	password
5	12345	football	12345	12345	1234567
6	123456789	qwerty	123456789	111111	12345678
7	football	1234567890	letmein	1234567	12345
8	1234	1234567	1234567	sunshine	iloveyou
9	1234567	princess	football	qwerty	111111
10	baseball	1234	iloveyou	iloveyou	123123

Source: TeamsID (2016 – 2020)

While a common reaction here is to blame the users for making poor choices and suggest that they ought to know better, it is relevant to pause for thought and consider *why* such choices might be made. Indeed, it is all very well to suggest that users should know better, but on what basis might they be expected to do so? Where exactly are they getting the support to guide them? Prior assessments of the guidance provided by popular websites certainly serve to suggest that there is frequently little upfront support, and often a lack of credible enforcement of password policies to weed out poor choices (Furnell, 2018). In the most recent assessment of ten leading sites (including Facebook, Google, Instagram, Twitter, and Yahoo!) only one provided upfront password guidance at the point of user sign-up. All sites offered some level of feedback in response to password selection attempts, but in several cases it was not particularly informative, indicating a problem but not usefully guiding the user to understand how to solve it (e.g. offering a message such as "Your password needs to be stronger", which tells the user that their current choice is unsuitable, but without clearly defining what 'stronger' actually means)

Even where it is provided, guidance can be significantly variable in terms of the focus and quality. Indeed users can sometimes get advice that is outright dangerous, such as the Italian online banking site that was advising its users to put their passwords into Google in order to determine if it was a suitable choice ("Insert it on Google: if it returns less than 10 results it means it's a good password.") (Franceschi-Bicchierai, 2019). Luckily, most password guidance is not this cavalier, but users could nonetheless be forgiven for getting mixed and confused messages.

Given the clear lack of guidance on many popular web sites, perhaps these providers assume that users can already get the advice elsewhere. While this is a poor excuse to avoid providing guidance (or linking to it), it does serve to raise the question of what users would find in such other sources. With this in mind, this paper seeks to examine the level and consistency of advice that users might receive if they were to go looking for password guidance from the recognised cybersecurity advice sites in their own country.

An assessment of password guidance

In order to perform a qualitative assessment, it is necessary to establish an idea of what we might be looking for users to be told in relation to their use of passwords. With this in mind, Table 2 suggests a series of issues that users can commonly receive guidance on, relating to both the selection/creation of passwords and the subsequent management of them. It should be noted that some of these are potentially *undesirable* criteria, depending on the advice being given (e.g. current advice around password change is not to do it unless compromise is suspected; advice on storing passwords is not helpful if it is saying not to do it at all

– but it should guide people against putting them in discoverable locations). In all cases, there are different levels of depth and coverage that can be provided, ranging from merely flagging an issue, through to more fully explaining it.

Table 2: Assessment criteria for coverage of password guidance

Issue		Description
Selection	Bad choices	Advice on the password choices that should be avoided, such as dictionary words, commonly used selections, and personal information.
	Composition	Advice to use multiple character types, such as alphabetic, numeric and punctuation symbols.
	Length	Guidance on the appropriate number of characters.
	Techniques	Suggestion of techniques that may help to create good passwords, such as use of passphrases, memorable acronyms, etc.
	Two-Factor	Guidance to supplement the password with two-factor authentication (2FA) where the option to do so is available.
	Uniqueness	Highlighting the importance of using different passwords to protect different accounts/devices.
Management	Changing	Advice on the frequency or regularity with which passwords should be changed (which may include guidance on *not* doing it, unless compromise is suspected).
	Reuse	Highlighting that previous password choices should not be reused.
	Sharing	Flagging the importance of not divulging passwords to colleagues, family or friends.
	Storage	Guidance on avoiding a discoverable record of passwords, such as writing them down or saving on devices in a plaintext format.
	Tools	Highlighting the potential to use tools such as password managers/vaults for support.

While the earlier research had looked at the password guidance and feedback on leading websites, these specific service-focused sites are arguably not the best candidates to assess in the current context, as they would potentially provide guidance that suits the needs of their site rather than good practice in general. Additionally, they are likely to focus on the password selection aspect (i.e. what the user needs to do in order to sign up to *their* site) rather than guiding on ongoing management or other aspects outside their own site. As such, the approach adopted for the current study was to examine national online security and safety websites that citizens in the countries concerned might naturally look toward as a primary source of official guidance. The selected sites are summarised in Table 3, noting also that (due to the authors' own linguistic limitations) only sites presented in English were considered.

Table 3: National advisory sources included in the assessment

Country		Advisory source	Web address
AU	Australia	eSafetyCommissioner	www.esafety.gov.au/key-issues/how-to/protect-personal-information
CN	Canada	Get Cyber Safe	www.getcybersafe.gc.ca/cnt/prtct-yrslf/prtctn-dntty/usng-psswrds-en.aspx
IE	Ireland	webwise.ie	www.webwise.ie/uncategorized/creating-strong-passwords/
NZ	New Zealand	netsafe	www.netsafe.org.nz/passwords/
SG	Singapore	Gosafeonline	www.csa.gov.sg/gosafeonline/go-safe-for-me/homeinternetusers/use-strong-passwords

UK	United Kingdom	Get Safe Online	www.getsafeonline.org/protecting-your-computer/passwords/
US	United States	Stay Safe Online	staysafeonline.org/stay-safe-online/securing-key-accounts-devices/passwords-securing-accounts/
ZA	South Africa	Safer Internet South Africa	saferinternetsouthafrica.co.za/create-strong-password/

All of the sites were assessed in mid-January 2020. The resulting coverage against the criteria is summarised in Table 4 and further discussed in the paragraphs that follow.

Table 4: Assessment of advisory sources against password guidance criteria

		Country							
		AU	**CN**	**IE**	**NZ**	**SG**	**UK**	**US**	**ZA**
Selection	Bad choices	✓	✓	✓	✓	~	✓		✓
	Composition	✓	✓	~		✓	✓		✓
	Length	✓	✓	✓	✓	✓	✓	✓	✓
	Techniques	✓	✓	✓	✓	✓	✓	✓	✓
	Two-Factor	✓		✓	✓	✓	~	~	
	Uniqueness		✓	✓	✓	✓	✓	✓	~
Management	Changing		~				✓		
	Reuse						✓		
	Sharing	✓				✓	✓		
	Storage	✓	✓		✓	✓	✓	✓	✓
	Tools	~			✓		✓	✓	✓

Even from a casual inspection of the table, one can see from the varying presence and absence of tick marks that the guidance is far from uniform and consistent across the sites. At the extremes, the UK's Get Safe Online site ostensibly had the most comprehensive coverage, while the US Stay Safe Online was surprisingly sparse and included relatively little usable advice. Looking in more detail, there is then some variation in the type and level of advice. The sites do not offer the same sort of core advice, some discuss and explain things in more detail than others, and some offer useful tips that others omit. At the same time, there were relatively few cases in which the guidance actually felt like it was being *explained* to the users. They were being told *what* they ought to do, but not so much (if anything) about *why* it was relevant. As such, it would still seem to be missing the potential to help people more fully understand the basis of the advised good practice, and likely losing the opportunity to win some of the hearts and minds in the process.

Some of the sites were considered to have less direct coverage of some issues, and hence are denoted as partial guidance (~) in Table 4. For clarity, these instances are individually explained below:

- Password managers are mentioned in passing in the Australian guidelines, without offering a specific recommendation to use them (suggesting that users should not store passwords on their device "unless it's via a password manager which stores them in an encrypted database").
- The Canadian guidance advices users to change their password in specific scenarios but does not provide sufficient information for the user to determine which situation should trigger a change (as further discussed below).
- The Irish guidance makes repeated reference to the *potential* to use special characters, without directly suggesting that passwords must have multiple character types.

- The Singaporean guidance indicates that attackers can use dictionary-based attacks and that "the password 123456 can be hacked in less than one second", but does not more comprehensively explain the nature of bad password choices.
- The UK guidance makes reference to 2FA, but only in the context of protecting access to password vaults.
- The US guidance does not specifically name 2FA, but suggests that users should "Fortify your online accounts by enabling the strongest authentication tools available, such as biometrics, security keys or a unique one-time code through an app on your mobile device".
- The South African guidance makes passing reference to the fact that 'Password 101' would suggest having a unique password but stops short of specifically saying that this is what its own guidance is advising.

As for the remaining entries in Table 4, it should be noted that having a tick in the box does not mean the sites offer consistent advice. For example, while all of them said *something* about password length, the specifics of *what* they say was rather variable:

- Australia - Suggests using 12-20 characters
- Canada – Suggests a minimum of 8 characters
- Ireland – Suggests a minimum of 10 characters
- New Zealand – Suggests using 15-20 characters
- Singapore - Suggests a minimum of 12 characters
- United Kingdom - Suggests a minimum of 8 characters
- United States - Suggests a minimum of 12 characters
- South Africa – Suggests a minimum of 8 characters

Looking at the list, there is clearly a lack of consensus on the appropriate minimum, and two of the sites are also suggesting maximum lengths. The latter is a curious aspect, insofar as it is unclear why it is *necessary* to provide a recommended upper limit if users are prepared to type more. In practice some websites and services will prevent longer passwords being used (or sometimes appear to accept longer entries when actually truncating the string at a certain length), but this is not a reason to give general advice to limit the size. As a related aside, the NIST guidelines suggest that user-selected 'memorized secrets' should be at least 8 characters in length, but also comment that users "should be encouraged to make their passwords as lengthy as they want, within reason. Since the size of a hashed password is independent of its length, there is no reason not to permit the use of lengthy passwords (or pass phrases) if the user wishes" (NIST, 2017).

It is not useful to cover the specifics of what each site said in detail (and interested readers are referred to the individual sources for further insight into how each of them treated the topics). However, it is perhaps useful to note some further aspects that emerged as useful themes in the coverage across multiple sites.

- Looking at the 'techniques' criterion, a commonly suggested approach was the use of passphrases (with, for example, Australian guidance recommending "seemingly random words" that can be "strung together along with numbers, symbols and upper and lower case letters" and Ireland suggesting users take the first letter of each word in a sentence). The 'random words' approach in particular is increasingly recommended by security agencies as a means of enabling long but memorable passwords (NCSC, 2016), and so it was encouraging to see some sites being up-to-date with this guidance.

- As is clear from Table 4, many sites had something to say about 2FA, which is again considered to be good advice in the context of safeguarding against password breaches that do not relate to the users' own selection or management practices (e.g. acquisition via keylogging, or as part of bulk compromise of accounts from a server or service provider).

- Some sites also present some specifics about how passwords can be set on different devices (e.g. the Australian site provides links to guidance for setting passwords on Windows and Macs; New Zealand's Netsafe provides brief steps for Android devices and iPhones).

At the same time, there were also some instances of advice that could actually be considered *unhelpful*:

- The Canadian site suggests that users "Try a mix of your pet's name, your favourite numbers, the street you grew up on or other combinations" – all of these are aspects that users would be advised to *avoid* on an individual basis as they are potentially known to others or susceptible to discovery via social engineering. Utilising a combination of them does not make the individual elements any more secret and only needs the attacker to discover the order in which they have been combined.

- Various sites advise on using combinations of characters, which the latest guidance from NIST and others has explicitly moved away from recommending.

- The Ireland site suggests that users "remember not to use the same password for more than two websites", but fails to identify the risks of a common password being compromised on a *single* site exposing the user to risk on the other (especially if one is the users' on-line banking).

- The New Zealand site advises: "avoid using the password storage options offered by web browser, as they are frequently targeted by hackers. Web browsers are targeted by hackers because if they can compromise the browser they can get access to the passwords you have stored in the browser". However, this advice may not be valid in all cases. For example, on the Safari browser on macOS, the password is stored in the user's Keychain and not by the browser, and is only auto-filled once the user re-authenticates themselves via their biometric or system password. As such, if the guidance is taken at face value then users could be denying themselves perfectly good usability-focused shortcuts.

Of the sites evaluated, the Canadian guidance offers a rather rich vein for criticism, as evidenced by the following quotes and consideration of their implications:

- "Commit your passwords to memory and don't store them on your computer or in your mobile phone" – this seems odd advice for managing potential password overload, and is rather at odds with various other sites that suggested using a password manager.

- "If you get an email that includes a password you've just set up, delete it" – while there is nothing wrong with this advice, it seems rather specific and ignores the fact that most users will be unaware of (or likely to overlook) the presence of a recovery function in the webmail service or email application being used. It would be more useful to advise users to delete *any* emails containing any of their passwords.

- "Change your passwords after implementing a fix or following being compromised" – this seems potentially confusing. Users may wonder what counts 'as implementing a fix'. For example, some may mistakenly conclude that it means they should change their password after installing operating system or application updates.

The eight sites were ultimately extremely variable in terms of both depth of advice (level of explanation) and styles of presentations. Guidance on what constitutes good practice *has* needed to change over time, particularly in terms of password length, as faster systems and distributed attacks make brute force more feasible, and rainbow tables exist for longer (and more complex) passwords. Indeed, it is worth recognising that whenever new recommendations are offered to users, tools will eventually be developed to target each new approach (Schneier, 2014), which in turn drives a need to change the guidance. However, it is apparent from many of the sites that their advice is still reflecting earlier versions of 'what good looked like', while current thinking has already moved on. Equally, while there is no definitive right or wrong way to present

the guidance, the authors' own recommendation would be toward clearly structured points, grouped either thematically or via sets of 'Do' and 'Don't' items, and using bullet lists to aid memorability.

From guidance to practice

Providing the guidance is arguably overcoming the first hurdle in supporting the user effectively. They now have a source of reference they can use in order to understand good practice. Unfortunately, the second hurdle is often the challenges that they can face when attempting to apply it.

In practice, users are increasingly able to invoke technology support when creating and managing passwords. For example, current web browsers can help via auto-generated strong password suggestions. However, as Figure 1 illustrates, individual websites can then undermine this as a result of imposing restrictions that the browser-created choices do not satisfy (the problem in this case being that the auto-generated password is too long). Similarly, attempting to follow advised good practice such as the oft-suggested notion of combining a series of random words, can fall foul of sites that still insist upon having multiple character types as a criterion. This is illustrated in Figure 2, where a 17-character password (wretchgravelgeese) is rejected because it does not contain upper and lowercase characters or a number. Such a password has entropy of 62 bits, thus making it far more resilient to brute force attach than a choice such as 'figRy$9a' – an 8-character option incorporating uppercase, lowercase and numeric characters (and hence meeting the requirements of the service in Figure 2), but having an entropy score of only 34.2 bits.

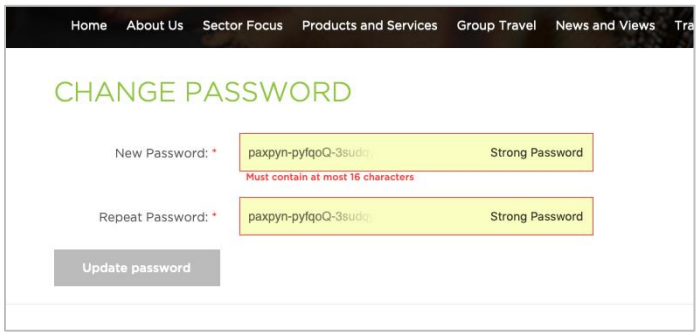

Figure 1: Browser-suggested password rejected by website rules

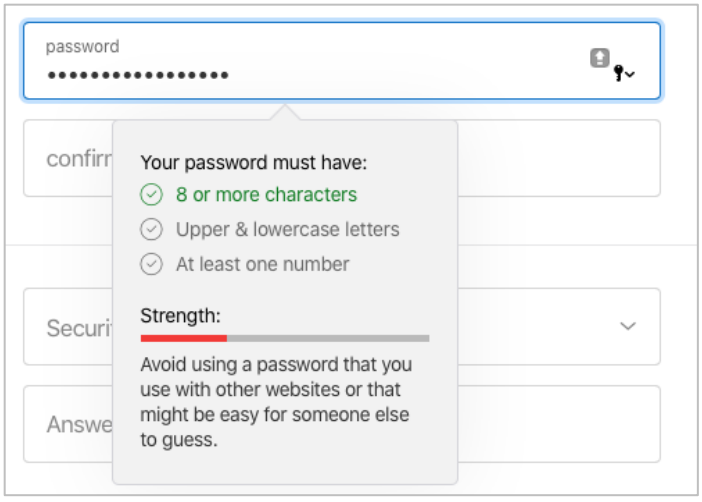

Figure 2: Three random words password rejected by website rules

Another common issue is encountered when password management applications or plugin utilities are used to generate dynamic/random passwords during account setup and subsequent login (making the process of creating and auto-populating password fields more user friendly, as well as facilitating the best-practice of unique passwords for each site). While these applications can usually generate a password that complies with the website requirements (meeting length and complexity requirements), some sites actively block attempts to insert the generated password (by preventing clipboard access or filtering input to limit to keypress events only). This has the effect of forcing the user to manually re-type the generated password, and, subsequently are likely to influence users to revert to less secure (but more convenient) password constructs.

Conclusions

One of the foundations for achieving effective cybersecurity amongst end-users must surely be for them to receive clear and comprehensive advice on how to fulfil their responsibilities. If this is the case, then the results of this investigation in the context of passwords does not paint an encouraging picture.

The key finding of the study is not what any particular site did or did not say, but rather that they collectively gave such a varied (and therefore inconsistent) account of good practice around a technology that we have been using and criticising for years. With so much negativity surrounding passwords as a security method, it might at least be reasonably for us to have got our story straight over how to use them as effectively as possible. If we cannot manage a clear, consistent and robust message here, it does not bode well for other aspects of cybersecurity where users will be in equal need of support.

In terms of the findings from the sets of guidance, it is of course easy to criticise and highlight omissions or aspects that could be improved. However, given the patchy nature of some of the guidance, and the potentially misleading items of advice in others, it is relevant to wonder how some of it was arrived at, and whether it was created with reference to other sources and/or validated by experts. Again, recognising the established nature of passwords and the resultant volume of advice that is already available, the extent of omissions and potential misdirection in some of the sources is surprising.

Finally, and as a potential area for future investigation, it would be relevant to determine whether the guidance has been evaluated – in terms of the target users' ability to understand and apply it, as well as any practical effect it has upon their password practices.

References

Alomari, R. and Thorpe. J. (2019) On password behaviours and attitudes in different populations. *Journal of Information Security and Applications Vol. 45. Pg. [79-89]*

Franceschi-Bicchierai, L. (2019) This Bank Had the Worst Password Policy We've Ever Seen, *VICE*, 14 November 2019. https://www.vice.com/en_us/article/kz4jjv/this-bank-had-the-worst-password-policy-weve-ever-seen

Furnell, S. (2018) Assessing website password practices – over a decade of progress?, *Computer Fraud & Security*, July 2018, pp6-13.

Ives B., Walsh, K.R. and Schneider, H. (2004) The domino effect of password reuse. *Communications of the ACM. Vol. 47. No. 4.*

Jobusch, D.L. and Oldehoeft, A.E. (1989) A survey of password mechanisms: Weaknesses and potential improvements. Part 1. *Computers and Security. Vol. 8. Is. 7. Pg. [587-604]*

NCSC (2016) Three random words or #thinkrandom. https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0

NIST (2017) Digital Identity Guidelines - Authentication and Lifecycle Management. *NIST Special Publication 800-63B*. National Institute of Standards and Technology, June 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

Schneier, B. (2014) Choosing Secure Passwords, *Schneier on Security*, 3 March 2014, https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html

TeamsID (2016) Announcing our Worst Passwords of 2015. https://www.teamsid.com/worst-passwords-2015/

TeamsID (2017) Announcing our Worst Passwords of 2016. https://www.teamsid.com/worst-passwords-2016/

TeamsID (2018) 100 Worst Passwords of 2017! The Full List. https://www.teamsid.com/worst-passwords-2017-full-list/

TeamsID (2019) SplashData's Top 100 Worst Passwords of 2018. https://www.teamsid.com/splashdatas-top-100-worst-passwords-of-2018/

TeamsID (2020) The Top 50 Worst Passwords of 2019. https://www.teamsid.com/1-50-worst-passwords-2019/

Weber, J.E., Guster. D., Safonov, P. and Schmidt, M.B. (2008) Weak Password Security: An Empirical Study. *Information Security Journal: A Global Perspective. Vol. 17. Is. 1. Pg. [45-54]*