Assessing password guidance and enforcement on leading websites

Steven Furnell, Centre for Security, Communications and Network Research, University of Plymouth, UK

For more than five decades, passwords have been the dominant means of user authentication for IT systems and are now used on a daily basis by millions of users worldwide.[1] Their significance is such that recent research has suggested 11% of people are now leaving (or planning to leave) details of Internet passwords in their wills so that they are able to pass on valuable online content to loved ones.[2] Meanwhile, in Italy the use of passwords has even become a matter of law, with privacy legislation laying down some minimum requirements (including that, where permitted by the system, they should be at least eight characters long, and be changed every six months).[3]

Moreover, in spite of recognised, long-standing limitations, the use of passwords appears to be ever-increasing, with online services now being among the most common scenarios in which people will be expected to use them. With this in mind, it is relevant to consider how well such sites are actually guiding and ensuring that they are used effectively. Here, we'll investigate the issue through examination of the password provision made by 10 leading websites.

This study builds upon earlier research conducted during the summer of 2007, which assessed the practices of Amazon, Bebo, eBay, Facebook, Friendster, Google, MSN, MySpace, Yahoo! and YouTube, and found them to be significantly variable.[4] The intervening period has seen significant developments in the online world, not least of which has been the massive growth of social networks (eg, Facebook has grown to over 800 million users, while Twitter – only a year old at the time of the previous study – now has 100 million active users), as well as continued expansion of online retail and overall Internet adoption.[5,6] It was therefore considered timely to repeat the assessment in order to determine the extent to which website authentication practices had evolved alongside the services they are supporting.

Methodology

As with the earlier study, the sites were selected from the Alexa 'Global Top Sites' list (see www.alexa.com/topsites) based on their traffic ranking. The sample was taken in mid-September 2011, with the assessment focused on sites presented in English and ignoring any regional variations of the same brands – eg, with Google.com already on the list, high-ranked sites such as Google UK were excluded. Also excluded were any sites that relied on the same login mechanisms as a site already benchmarked (eg, YouTube, ranked at number 3, and Blogspot.com, ranked at number 7, both used Google account login, while MSN and Bing, at numbers 11 and 24 respectively, both asked for the same credentials as Windows Live). As luck would have it, this yielded precisely 10 sites out of the top 25 that were eligible for further investigation, six of which were in common with the earlier 2007 study. The full set is listed in Table 1, and although this is not a high-volume sample, it still serves to capture a group of leading and well-recognised sites whose password practices are likely to influence a significant community of end-users. In addition, it is likely that other site providers will look towards them as a benchmark of the security that they ought to be providing on their own sites.

In each case, user accounts were created on the sites in order to determine the password selection requirements. With initial passwords having been set, these were then updated using the available password change and reset/recovery procedures. As with the original study,

Site	Alexa ranking	Description
Google	1	Web portal
Facebook	2	Social networking site
Yahoo!	4	Web portal
Wikipedia	6	Web-based collaborative encyclopaedia
Windows Live	8	Web portal
Twitter	9	Social networking and microblogging service
LinkedIn	13	Business/Professional networking site
Amazon	15	International online retailer
WordPress.com	18	Open source blog tool and publishing platform
eBay	21	Online auction site

Table 1: Ten popular websites selected for assessment.

each site was assessed against several key factors as part of this process:

- Whether the sites provided any guidance in relation to initial password selection, and (if so) the extent of the coverage.
- Whether any restrictions were imposed on permissible passwords, in order to reduce the user's potential for making poor choices.
- Whether a means was offered to reset or recover passwords, and (if so) the process involved.

In addition to repeating the original evaluations, the updated study also considered several further characteristics:

- Whether the site permitted the reuse of old passwords.
- Whether a password strength meter was provided, and if so, how it worked.
- Whether there was any means for users to supplement their passwords with additional protection (eg, via one-time access codes sent to their mobile device).

The specific findings in each of these areas are examined in the sections that follow.

Provision of password guidance

The extent of guidance provided to users was assessed during the initial registration process, as well as at the stages when users subsequently changed or reset their passwords. As in the earlier study, there was a significant disparity between the sites in terms of their attempts to inform and advise users about how and why to consider their password choices. One of the headline findings is basically that half of the sites provided little or no upfront guidance during account registration. Of those that did, eBay and Google were notable for providing clear links to comprehensive guidance pages (see Figure 1), which both included specific comments about how to select good passwords, as well as more general tips about how to use and protect them.

At the other end of the spectrum, some sites (eg, Amazon and Wikipedia) provided no password guidance at all at the point of registration. Most other sites were somewhere in between, providing an indication of the criteria for selection but no wider tips on protecting the password once chosen. As an example of the very limited guidance available in some cases, new users registering on Twitter are simply presented with a tip beside the password box saying "6 characters or more! Be tricky", but without any further indication of what 'being tricky' actually means. By contrast, if a user later elects to change their Twitter password, then they are given some slightly more useful information: "Be tricky! Your password should be at least 6 characters and not a dictionary word or common name. Change your password on occasion" (although there is still nothing to usefully explain 'tricky', nor indeed the frequency that qualifies as 'on occasion').

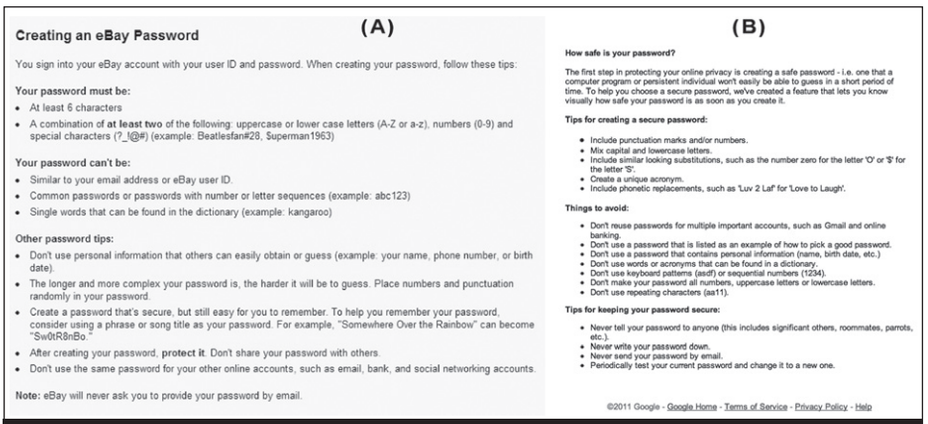

Figure 1: Examples of the more comprehensive password guidance available from (a) eBay and (b) Google.

A similar criticism can be levelled at the approaches used by Facebook and WordPress, with the former saying that "Your password should be more secure. Please try another.", but without giving any indication of how this can be achieved. Meanwhile, WordPress users receive a message to say, "Your password does not meet our security guidelines. Please try a more complex password", but without any further indication of what their security guidelines are or how to make a password that is more complex.

In common with the 2007 study, a potentially surprising finding was that while some sites provided no password

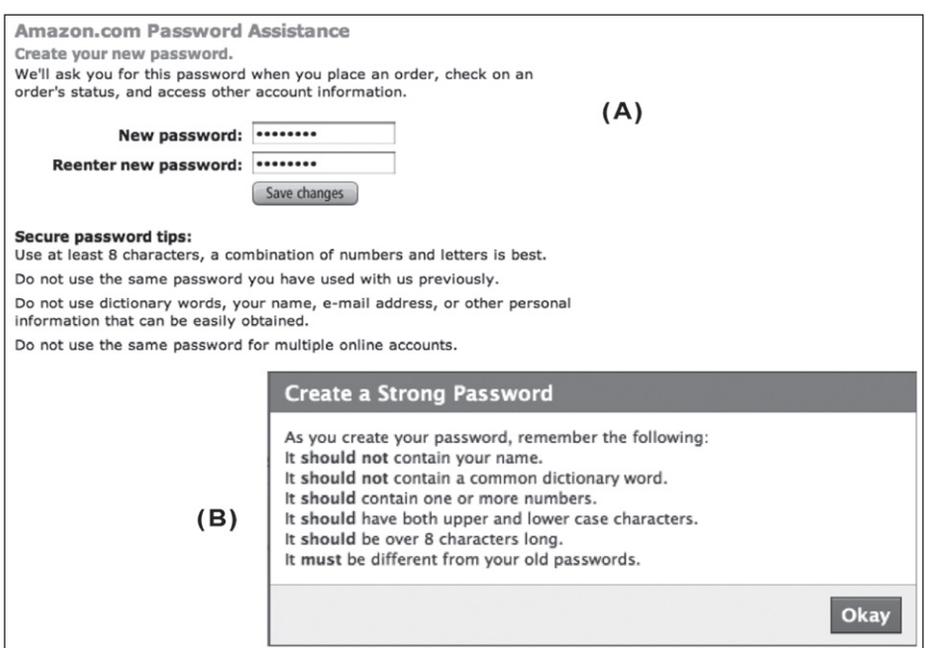

Figure 2: Password selection advice at reset from (a) Amazon and (b) Facebook.

Site	Meter ratings and rules	Consistent at sign-up and change
eBay	Password rated against compliance with four 'password essentials': - 6-20 characters - Mix of letters, numbers or symbols - Not similar to your user ID or email - Not easily guessed, eg, abc123	Yes
Facebook	- Too short – fewer than 6 characters	
	- Weak – 6+ alphabetic-only characters or 6-7 numeric-only or symbol-only characters - Medium – 6+ characters of 2 different types - Medium – 6+ characters of 2 different types - Strong – 6+ characters of 4 different types Note: Medium and Strong ratings can be obtained using fewer character types if longer passwords are used.	No (only present for password change)
Google	Uses ratings of Weak, Fair, Good and Strong, but the basis for the ratings is not clear.	Yes
Twitter	When signing up, the system displays a meter and comments on the password (eg, 'Password is okay', 'Password is perfect') without a clear scale in use. When changing a password, the meter is replaced by a textual rating beside the password box: - Too short – fewer than 6 characters - Weak – 6-11 characters of the same type - Good – ~12+ characters of the same type - Strong – ~15+ characters of the same type - Very Strong – ~19+ characters of the same type or 6 characters if using 4 different types Note: The rating thresholds vary depending upon the variety of characters being used (eg, a varied range of lowercase letters gets the stronger ratings more quickly than a string that has repeated characters).	No (different versions)
Windows Live	- Strong – any 3 character types and at least 7 characters - Medium – any 2 types and at least 7 characters - otherwise rated 'weak'	No (different versions)
WordPress	Sign-up uses following ratings: - Too short – fewer than 4 characters - Bad – 4-7 characters of the same type - Good – At least 4 characters of 2 types - Strong – At least 4 characters of 3 types The higher ratings can also be achieved using longer passwords with fewer character types (eg, 8-13 characters of the same type can get rated 'Good', and 14+ characters can be rated 'Strong'). The meter for password change uses different ratings and applies different rules: - Very weak – fewer than 4 characters - Weak – 4-8 characters of the same type - Medium – 8+ characters of two types - Strong – 9+ characters of four types	No (different versions)
Yahoo!	- Invalid (if part of user's name, ID, or the word 'password') - Too short – fewer than 6 characters - Weak – 6-32 characters of the same type (either upper- or lowercase alphabetic or numeric) - Strong – 6-32 characters mixing at least two of upper- or lowercase alphabetic or numeric, or a string based solely on at least 6 special symbols (including a predictable sequence such as "!@£$%^" (ie, the shifted version of 123456). - Very Strong – 6-32 characters mixing at least 3 types of character. Can also get it for a very long string of special symbols (~25) plus a few alphabetic.	No (only present at sign-up)

Table 2: Password meter implementations.

guidance when users initially signed up, they did provide it at later stages of password change or reset. For example, both Amazon and Facebook only provide advice during the password reset process (see Figure 2), in the event that the user has forgotten their password (ie, nothing is available earlier when registering or electing to change the password voluntarily). Although there may be some degree of logic here (insofar as the user was unable to remember his or her previous choice and so may need tips to choose something more easily memorable), it is clear from the screenshots that none of the guidance is actually being presented from this perspective.

Even where guidance was offered, it is notable that none of the sites provided any explanation of why it was relevant to follow it (for example, rather than just saying that dictionary words should be avoided, explaining that this is because of the ease with which automated tools can discover them). It is considered that providing the 'why' in addition to the 'what' could be useful in getting buy-in from users, because they will then have a basis for understanding the basis of the rules rather than just being asked to obey them.

Use of password meters

One notable area of improvement compared to the earlier study was the proportion of sites offering password meters in order to give the user a visible measure of how strong their proposed password might be. Even in cases lacking guidance, a password meter can still provide users with a good indication of when they have 'got it right', and may indeed motivate them to go for a better rating and thus take them beyond the password choices that they might otherwise have settled for.

Back in 2007 only two of the 10 sites were doing this, but in the latest sample some form of meter was in use in a total of seven cases. However, there were some notable inconsistencies in how the sites implemented their approaches, with

some of them offering meters only during initial sign-up and others doing so only at registration, and some offering meters at both stages but with different appearance and/or rating behaviour.

Table 2 summarises the approaches used by the sites that offered meters at some stage, and it can quickly be seen that they had rather differing criteria for the ratings in use and the basis upon which they would be awarded. In terms of the rules, there are a couple of cases that merit some further comment. First, in Google's case, although four levels of rating were possible, it was quite easy to score higher ratings on the basis of what were actually rather poor choices. For example, both 'plokmonk' (a meaningless string, but using a fairly close collection of characters on the keyboard) and '77889912' were scored 'Strong', despite being composed from only one type of character. Meanwhile, just to give a flavour of how the other ratings could be obtained, various dictionary words (eg, 'dolphins', 'grapefruit' and 'melbourne',) were scored 'Weak', 'carrots1' was scored 'Fair', and 'farmyard' was scored 'Good'. Similarly, Facebook's approach to ratings (only available at password change or reset) was also rather curious. Specifically, while an alphabetic-only sequence would never get scored better than 'weak' (no matter how long it was), an eight-digit numeric sequence would get rated 'medium' (despite having a significantly reduced character space).

Although eBay is counted as having a meter, it was a little different from the others in use (see Figure 3). In this case, the assessment of the password was performed against a series of specific criteria rather than ratings on a meter. These items are then enforced before permitting the user to proceed (ie, they cannot select a password that does not satisfy all four of the rules).

To illustrate the inconsistency of the meter usage within the same site/service, we can consider the variety of examples presented by Windows Live. Figure 4a depicts the version encountered if you

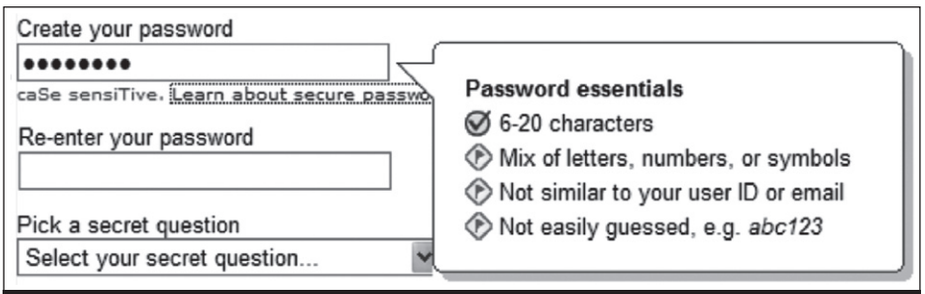

Figure 3: The eBay password assessment.

sign-up via live.com, with the meter and associated advice appearing interactively once the user reaches the 'create a password' field. By contrast, Figures 4b and 4c show what the user would see if they happened to route in through an MSN site (the differences between them being that Figure 4b is the version you get if you indicate that you have an existing email address, whereas Figure 4c is what you see if you also wish to sign up for a Hotmail account). Clearly, both the appearance of the meter and the level of immediate on-screen guidance vary in these cases, even though all three are cases in which the user is trying to do exactly the same task. Meanwhile, Figure 4d is the version seen when a Windows Live user elects to

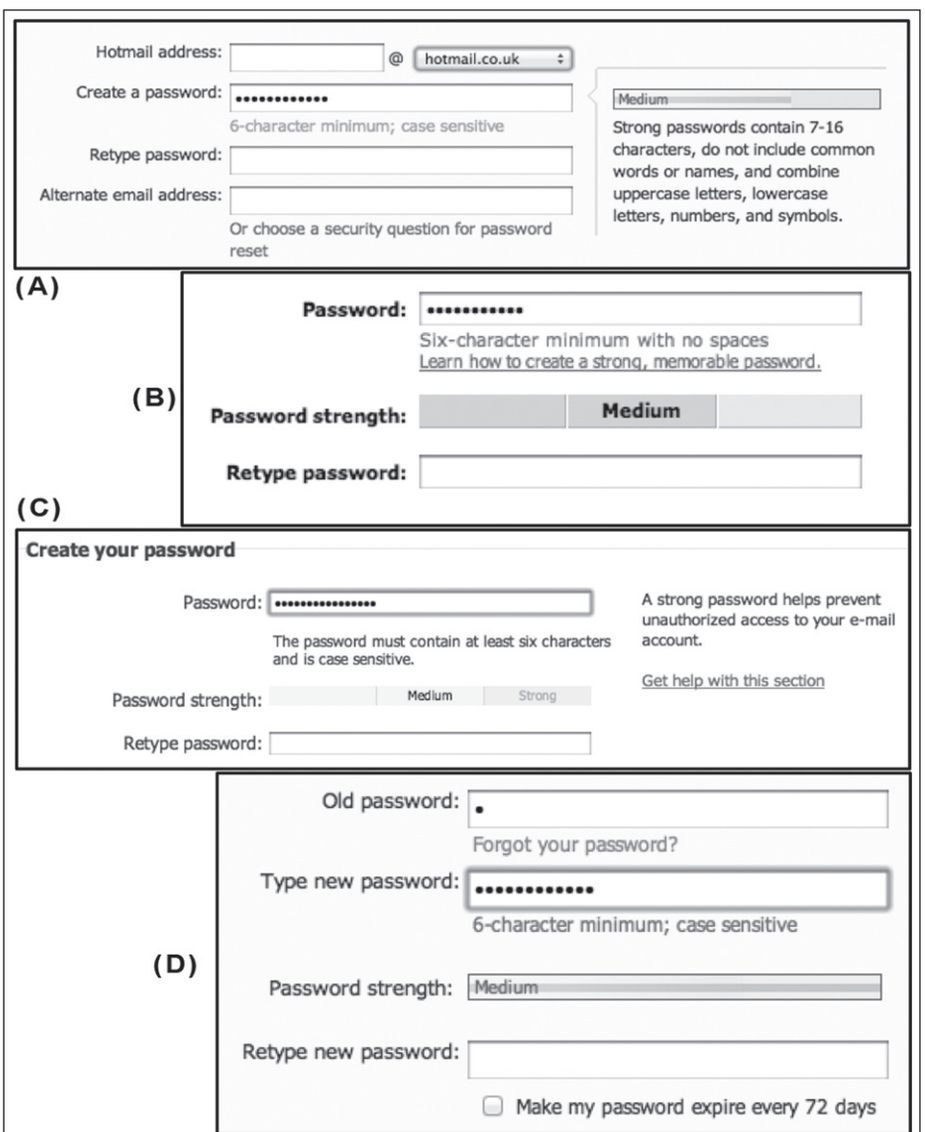

Figure 4: The varying appearance of Windows Live password selection.

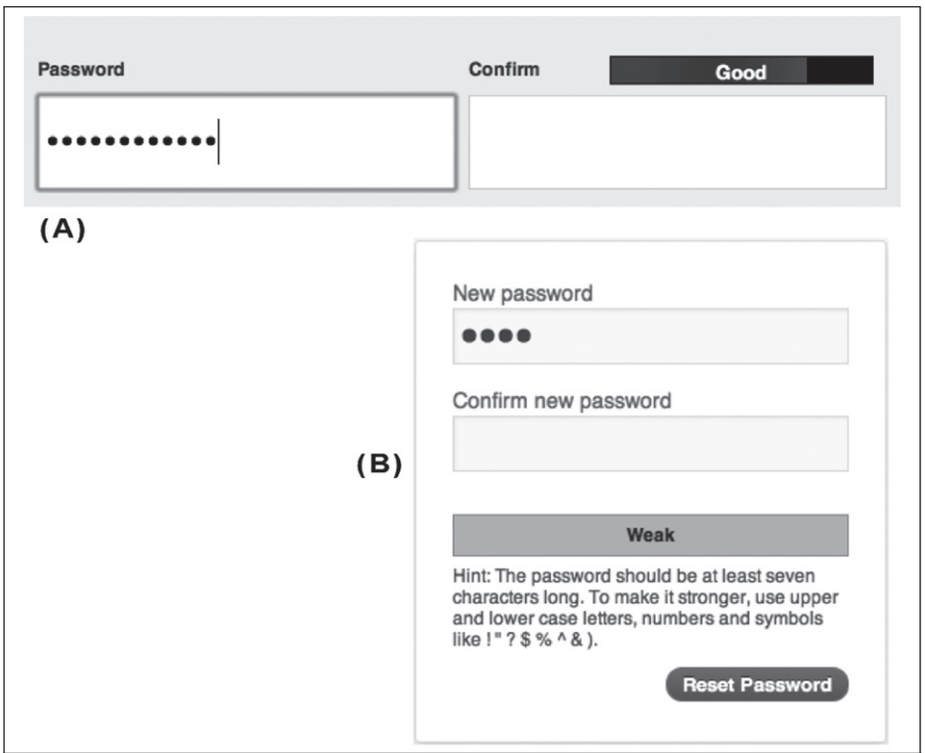

Figure 5: The WordPress password meter (a) for initial sign-up and (b) for password reset.

change their password, and is notably the only interface in which they also receive an option for the system to make their password expire after 72 days.

A further example of inconsistency is provided by WordPress, where not only is the appearance of the meter significantly different between sign-up and password reset (see Figure 5), but the actual ratings are also different. It is notable that the version in Figure 5b is accompanied by a small amount of password advice (which does not match the original password selection requirement), and choices that would previously have been rated as 'Bad' (including 'apples' and 'password') are all now accepted as valid. As an aside, another potential inconsistency with WordPress is that (depending on the route they take), users can find themselves changing the password via the Gravatar.com site rather than via the WordPress interface. If they do this, they will find some notable differences, including the total absence of a password meter and that fact that various choices that would previously have been rated as 'Bad' are again accepted as valid.

In some cases the basis of the rating would be far from obvious to the casual observer – in the absence of other password selection guidance, it would not be surprising if users were unclear about why their passwords were being rated at different levels. For example, Figure 6 shows the extent of feedback that users receive from Twitter's password meter, with a 12-character password here being rated as 'okay', but clearly falling well short of the possible full rating on the meter. However, the user is given no feedback about what they might do to improve the situation. Through experimentation they might discover that their rating improves as they just add more of the same type of characters (eg, going up to around 22 characters of the same type, the rating becomes 'perfect', but the meter bar is still not full), but this could leave them with a rather long password to type when, by contrast, they could have varied the character types and obtained a better score more quickly (eg, a 'perfect' rating can be achieved in six characters if it uses a full range of alphabetic, numeric and symbol character types).

Figure 6: The Twitter password meter at sign-up.

Also potentially confusing would be cases where there was actually a disconnect between the guidance provided and what users would then see from the password meter. For example, Google's tips clearly suggest that "a secure password" should contain mixed-case letters, punctuation symbols and/or numbers. However, in spite of this, it was still possible to get an eight-character password, all lowercase, to be rated as 'Strong'. The WordPress approach exhibited a different form of this disconnect. While it was encouraging to see that it did not allow users to proceed with a password rated as 'Bad', it was surprising to find that the same fate could befall some passwords rated as 'Good' on the meter. For example, an eight-character lowercase password was rated as 'Good', but attempting to use it met with the aforementioned message about guidelines and complexity. In this case, the message would arguably have been correct, but it would have been helpful for the password meter to better reflect the policy being enforced by the site. Interestingly, the password 'qw12', also rated 'Good' on the WordPress meter, was accepted for use.

Although all of the sites with meters were rating the passwords, they varied in terms of what they actually did with the information. While some (eBay, Google and WordPress) prevented users from proceeding with passwords that were rated too low, other meters (Twitter, Windows Live and Yahoo) advised that choices were weak but still accepted them for use.

As with the variation observed with availability of password guidance, there was again inconsistency in some cases over whether the password meter was available at registration and at later points when changing or resetting a password. These cases are highlighted in Table 2, and contribute to one of the

Site	Restrictions enforced							Support	
	Enforces min length (+max if approp)	Prevents surname	Prevents user ID	Prevents 'password'	Prevents dictionary words	Enforces composition	Prevents reuse	Password meter	Extra protection
Amazon	6	No	No	No	No	No	No	No	No
eBay	6-20	No	Yes	Yes	No	Yes	Yes	~	No
Facebook	6	Yes	No	Yes	~ (1)	No	No	~ (1)	Yes (2)
Google	8	No	Yes	Yes	Yes	No	Yes	Yes	Yes (2)
LinkedIn	6	No	No	Yes	No	No	No	No	No
Twitter	6	No	No	Yes	Yes	No	No	Yes	No
Wikipedia	No	No	Yes	No	No	No	No	No	No
Windows Live	6-16	Yes	Yes	Yes	No	Yes	No	Yes	Yes (2)
WordPress	4	No	Yes	Yes	No	No	No	Yes	No
Yahoo!	6-32	Yes	Yes	Yes	No	No	No	~ (3)	No

(1) Provision is only made when the user changes their password.
(2) Google allows two-step verification codes sent to or generated by a mobile device. Windows Live enables a 'single use code' to be sent to the user's registered mobile phone. Facebook can be configured to require login approval via an access code for an unrecognised device.
(3) Provision is only made during initial registration.

Table 3: The varying enforcement of password restrictions.

overall themes emerging from the study – namely that even where sites have got some elements of good practice, they cannot be relied upon to implement it in a consistent manner at all stages where they allow passwords to be set.

Enforcement of password restrictions

While the password meters monitored and advised on a number of aspects, including password length and composition, this did not necessarily mean that the sites actually enforced restrictions on the choices that could be made, as several allowed 'weak' passwords to be used. As such, all of the sites were tested against the following criteria to see which were actually enforced (with all but the last one having been common to the 2007 version of the study):

- **Enforces length:** indicates whether the site imposes restrictions over password length. Enforcement of a minimum length is of particular importance, given that longer passwords are more difficult to crack. But some sites also impose limits on the maximum length that can be used which, if too short, can also hamper user attempts to follow good practice.
- **Prevents surname:** determines whether the user is able to use their surname as the password. This is one of the obvious choices that may be used in order to make the password easy to remember. In cases where the site registration process includes collection of the user's name, it is possible to guard against this choice. In cases where the name is not obtained as part of registration (eg, Google, Wikipedia and WordPress), the user is implicitly unrestricted from using it as their password.
- **Prevents user ID:** tests whether the user's login or email identity can be used as the password. As with the surname, this would represent an obvious, easily guessable choice, which it would again be possible for the site to check and guard against.
- **Prevents 'password':** examines whether the site permits the word 'password' itself to be used as the password. This is known to be another common choice among users seeking to keep life simple for themselves.
- **Prevents dictionary words:** tests whether the site allows the use of dictionary words as passwords. This test is relevant on the basis that these are easier to crack using automated tools such as Ophcrack, and again standard password guidelines would recommend against their use. Sites failing the 'password' test will already have failed this one, but for completeness all sites were tested using words such as 'apples', 'secrets' and 'dictionary' as the dictionary words.
- **Enforces composition:** considers whether the site attempts to ensure that passwords incorporate a mix of character types (eg, upper- and lowercase alphabetic, numeric and/or punctuation symbols). This is again a standard recommendation in password guidelines, in order to increase the complexity (in terms of character space) of the password and force more permutations to be attempted in a brute force attack.
- **Prevents reuse:** tests whether the password change and reset processes allow users to choose passwords that they have already used in the past. This is another aspect of good password enforcement practice, in terms of preventing users from alternating between passwords or reverting back to previous ones if forced to change by the system.

Table 3 summarises the extent to which the different restrictions were enforced across the sample group (for completeness, it also lists the presence of support features discussed in other sections). Unless

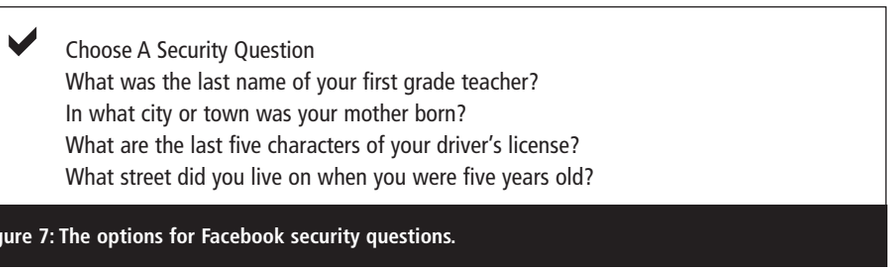

Figure 7: The options for Facebook security questions.

otherwise stated, these are the restrictions imposed on initial sign-up, and it is worth noting that this behaviour is not always consistent when it comes to later password change or reset (for example, at password change, WordPress went the way of Wikipedia and permitted a one-character password to be chosen).

One of the most immediate observations from Table 3 is the significant variation that can be seen across the group. Given that at least one of the sites does each of the things listed, it is clear that none of the criteria represents an unreasonable requirement. Even the enforcement of a minimum password length, perhaps one of the most readily recognised elements of password practice, is handled very variably. The modal value, a six-character minimum, seems rather low for sites that can store such sensitive details, and only Google's eight-character baseline seems aligned with more typical good practice guidance. Meanwhile, the decision of some sites to enforce a maximum length is not necessarily helpful. While Yahoo's upper limit of 32 seems unlikely to impede many users' choices, it is conceivable that users seeking more secure passwords might reasonably reach the 16 or even 20 character maximums imposed by Windows Live and eBay.

"Although some of the sites pass the basic tests, it does not take much to get past them. While Facebook prevented the use of the user's surname or 'password', adding a '1' to the end would be accepted as a valid choice"

It is worth noting that although some of the sites pass the basic tests, it does not take much to get past them. For example, using Facebook as an illustration, while it prevented the use of the user's surname or the word 'password', adding a '1' to the end of either of them would be accepted as a valid choice. As such, the validation is using specific string matching rather than more substantial parsing of the input.

Comments can also be made on the level of checking in some cases. For example, while Twitter gets a tick in the box for dictionary words, the extent in practice seems a little limited. For example, while 'apples', 'secret' and 'rabbit' (among others) are all rejected with the warning "Password is too obvious", the choice of 'rabbits' and 'secrets' were both accepted (albeit with the warning "Password could be more secure").

As indicated in the table, several of the sites are only marked as offering partial provision for the listed features, because they do not apply at all stages of the password process. For example, Facebook's enforcement of dictionary word restrictions only applies when changing the password (and indeed, guidance now appears if the password is rejected, informing the user that dictionary words cannot be used).

In several cases, the lack of enforcement was actually in contradiction to the advice being provided. For example, the Amazon guidance previously presented in Figure 2a advises use of an eight-character password, but the site still permits just six characters to be used, and also allows the reuse of previously used passwords. Similarly, while the Facebook guidance in Figure 2b clearly emphasises that the new password 'must' be different from old ones, this again is not enforced in practice (nor indeed are the composition requirements).

Password reset procedures

All of the sites provide functionality in the event of a forgotten password. Unlike the 2007 study, however, none of the sites do this by offering password recovery (ie, giving access to the current password) and instead require the password to be reset to a new one. As observed in the previous study, this is a good thing from a security perspective because if an impostor is at work then forcing them to set a new password will implicitly draw attention to the compromise of the account. Moreover, divulging the existing password could introduce risk to the legitimate user's other accounts (recognising the common end user practice of reusing the same passwords in multiple places).

The standard reset process across most of the sites was to send a link to the user's registered email address, which they would then follow in order to set a new password (in some cases, such as LinkedIn and Yahoo!, the link is only valid for a day in order to limit the potential for misuse). The exception was Wikipedia, which did things slightly differently by emailing a new, one-time password, which the user would then use to login and set a new password. In some cases (eg, Google and Facebook), if the user has added details of a mobile phone to their account, then they also have the option to receive a reset code as a text message rather than by email.

In terms of additional safeguards against abuse of this process, Twitter and Yahoo! require users to complete a Captcha in order to ensure that the reset request is originating from a human participant rather than an automated attack. Meanwhile, several of the sites also require the user to answer one or more security questions (the answers to which they would have provided during registration) in order to further authenticate their reset request. For example, eBay asks the user for any two of the following:

- Response to their secret question, with the question itself having been chosen from six available presets at sign-up.
- Postcode.
- Telephone number.
- Date of birth.

Meanwhile Windows Live and Yahoo! allow the user to answer the question(s) as an alternative to sending an email-based reset link (which is useful in the case that the user may have been using those services for email and thus, having forgotten the password, no longer has access to his or her account). In the case of Windows Live, only one question needs to be answered, whereas Yahoo! requires responses to two questions (which would have been selected from nine available at sign-up). Yahoo! required the answers to the questions to be at least four characters long, which might be problematic for some of the answers that people might otherwise want to give (eg, if 'your favourite uncle's name' was 'Tom'). Meanwhile, some of the questions may not be applicable to all users (eg, 'where you went for honeymoon' is no good if users are unmarried).

Finally, the Facebook case was interesting insofar as the password reset procedure was actually the stage at which users were asked to set their secret question, as shown in Figure 7. However, like Yahoo!, it starts to get picky over the responses. For example, if your first-grade teacher happened to have the last name 'Jones', then Facebook does not like it and responds with, "Sorry, but you can't use that answer. Please try another one that's harder to guess". Similarly, if your driving licence happens to end in '12345' then you cannot use it (although '67890' is apparently acceptable).

Going beyond passwords

While passwords still dominate the authentication methods of the market leaders, one difference since the earlier study is that they are no longer the complete story for the techniques on offer. As observed in Table 3, several of the sites offered users an opportunity to boost their authentication beyond this. The main options identified, and the extent to which they added protection, were as follows:

- Google allows the use of two-step verification, whereby the username and password must be followed up by a one-time code that can either be sent to the user's mobile phone by text or voice message, or generated using an app on an Android, BlackBerry or iOS device. Users can optionally remember a computer for up to 30 days so that they do not need to use the two-step verification every time they log in.
- Windows Live permits the user to request a 'single-use code', which can be used to log in instead of the password when accessing from someone else's computer. The code is sent to the user's registered mobile device.
- Facebook can be configured to require 'Login Approval' for access from an unrecognised device. This sends an access code to the legitimate user's mobile phone, and they will then have to enter this the first time they want to get access from the new device.

Of these, Google's approach is the only one that gives an option for true two-factor authentication to be used as a regular and routine part of the user's login process. The Windows Live approach replaces the password, and so if an impostor has acquired the user's mobile phone, then this is conceivably all they need in order to get access. The Facebook approach is just a one-off level of additional protection, the first time an unfamiliar device is used for access.

While all of these represent a level of advancement, they are not the only options to be found in the current market. Although they were not represented in the sample group, clear indications are emerging elsewhere that some providers are no longer content to rely on password-based approaches. For example, many online banks have now moved towards issuing physical card readers or one-time code devices to their customers, thus ensuring that two-factor authentication can be reliably incorporated into the standard login procedures and/or the authorisation required for particular types of transaction. These, combined with login approaches that involve more cognitively demanding, multi-stage procedures, mean that users tend to see a more visible barrier in place between an impostor and their accounts.[7] However, it also means that the process is not necessarily the sort of thing that would easily scale to other contexts, and the idea of all providers issuing their own dedicated card readers or tokens is not one that would be likely to be welcomed once people found themselves having to manage a multitude of them. As such, a solution for the wider market would seem to more reasonably lie with the approaches that Google and others have followed in leveraging the mobile devices that users are already likely to own.

Conclusions

Comparing the results of this study with the 2007 original, it is fair to say that the intervening period has not seen an improvement in password practices that feels commensurate with the increased use of online services or the breaches observed. The key finding essentially remains the same, insofar as one really could expect to see a greater degree of good practice being promoted and enforced. In addition, one might reasonably hope to see a greater level of consistency between the practices of leading sites. With a couple of honourable exceptions, all of the mainstream sites assessed are offering nothing beyond standard password protection, and even then are not implementing it as well as they could do. Meanwhile, many have neither evolved their practices nor their advice to users. For example, given what the other sites are able to provide, Amazon's offer still remains surprisingly weak for a site that allows the user to lodge payment card details and other

personal information with the service – although it has at least advanced beyond allowing the one-character password that it permitted four years ago.

"When it comes to helping their users to protect themselves, the market leaders are generally missing an opportunity to take the lead"

It is also surprising to see such a significant difference between the two Alexa-ranked leaders (Google and Facebook). While Google is pushing the envelope through the option to use two-step verification, Facebook seems content to enforce a password policy that ignores several decades of password advice. And despite the wealth of sensitive personal information that it can store, its approach is among the weaker of those surveyed.

Of course, sites might argue that they consider the checks to be commensurate with the data at risk, and that users are not prevented from using stronger passwords – and indeed, other than having potentially restrictive maximum length limitations in a couple of cases, the sites allow users to select as strong a choice as they wish. However, what this overlooks is the missed opportunity to help users learn and acquire good practice, and the fact that they may consequently take these weaker practices as their benchmark for choosing passwords elsewhere. In short, when it comes to helping their users to protect themselves, the market leaders are generally missing an opportunity to take the lead.

About the author

Prof Steven Furnell is the head of the Centre for Security, Communications & Network Research at Plymouth University in the UK, and an adjunct professor with Edith Cowan University in Western Australia. His interests include security management and culture, computer crime, user authentication and security usability. Furnell is active within three working groups of the International Federation for Information Processing (IFIP) – namely Information Security Management, Information Security Education, and Human Aspects of Information Security & Assurance. He is the author of over 210 papers in refereed international journals and conference proceedings, as well as books including Cybercrime: Vandalizing the Information Society (2001) and Computer Insecurity: Risking the System (2005). Further details can be found at www.plymouth.ac.uk/cscan.

References

1. Denning, PJ. 'Passwords'. American Scientist 80 (Mar-Apr 1992), pp117-120.
2. 'Generation Cloud'. Rackspace Hosting, 2011. <http://www.rackspace.co.uk/uploads/involve/user_all/generation_cloud.pdf>.
3. See Technical Specifications Concerning Minimum Security Measures (Annex B) in Italian Personal Data Protection Code, Legislative Decree no. 196 of 30 June 2003. http://www.privacy.it/privacycode-en.html.
4. Furnell, S. 'An assessment of website password practices'. Computers & Security, 2007, vol. 26, nos. 7-8, pp445-451.
5. Facebook. 2011. Statistics. Accessed 16 October 2011. <http://www.facebook.com/press/info.php?statistics>.
6. 'One hundred million active voices'. Twitter Blog, 8 Sep 2011. <http://blog.twitter.com/2011/09/one-hundred-million-voices.html>.
7. Furnell, S. 'A comparison of website user authentication mechanisms'. Computer Fraud & Security, September 2007, pp5-9.

Interview: Todd Krautkremer, Red Lambda

Steve Mansfield-Devine

It's becoming trendy to talk about big data, however you care to define it. But security practitioners are all too aware of the problems of drowning in data. Mention 'logs' to network managers and watch them twitch. That reaction has one of two causes: guilt, because they haven't been monitoring their system logs nearly as much as they should; or exhaustion, because they have.

Security Incident and Event Management (SIEM) tools were supposed to put an end to all that. By applying rules to the data, they alert managers to the presence of anomalous behaviour. Or not, as Todd Krautkremer, COO at Red Lambda, explains: "Many of the current technologies that use signatures in the rules are, by definition, looking for threats that have, in one way, shape or form, been seen before." Red Lambda, he explains, has come up with another way of going about this. "The advantage of what we're doing is to find the unknown-unknown," he claims. "You don't know what they are, where they're coming from or what they're going to attack. But the idea is that every threat, every attack, leaves some trail."

Red Lambda has recently launched its MetaGrid solution, built on top of the AppIron grid platform, which is all about handling big data. On top of