available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

An assessment of website password practices

*Steven Furnell**

Information Security & Network Research Group, School of Computing, Communications and Electronics, University of Plymouth, Plymouth, United Kingdom

ARTICLE INFO

Article history:
Received 31 July 2007
Revised 2 September 2007
Accepted 6 September 2007

Keywords:
Passwords
Authentication
Usability
Awareness
Websites

ABSTRACT

Password-based authentication is frequently criticised on the basis of the ways in which the approach can be compromised by end-users. However, a fundamental point in the defence of many users is that they may not know any better, and lack appropriate guidance and support when choosing their passwords and subsequently attempting to manage them. Given that such support could reasonably be expected to come from the systems upon which the passwords are used, this paper presents an assessment of password practices on 10 popular websites, examining the extent to which they provide guidance for password selection, enforce restrictions on password choices, and support easy and effective recovery or reset if passwords are forgotten. The findings reveal that the situation is extremely variable, with none of the assessed sites performing ideally across all of the assessed criteria. Better efforts are consequently required if password practices amongst the general populous are expected to improve.

1. Introduction

Although the theoretical view of user authentication argues that approaches may be based upon something the user knows (i.e. secret knowledge), something they have (e.g. a physical token) or something they are (e.g. a biometric), the practical reality is that there is typically no escaping the use of passwords. Indeed, in spite of the fact that their use has been roundly criticised on many occasions, passwords remain the de facto approach to user authentication and are used in the vast majority of cases (DTI, 2006). Having said this, it is notable that much of the criticism is not down to failings of passwords as a concept, but rather the fact of how they are used by the people that hold them. Indeed, there is a significant body of evidence to suggest that users have poor password practices and do not afford appropriate attention to safeguarding their secrets. For example, a variety of well-publicised studies have highlighted that users are willing to divulge the information far too easily, including to strangers in exchange for pens (Leyden, 2003) or sweets (BBC, 2004)! Aside from such indiscretions, other recognised problems may include (Furnell, 2005):

- Poor password choices (e.g. passwords that are too short, based upon dictionary words, related to personal information, etc.), leaving them vulnerable to cracking tools and social engineering.
- Writing the information down, and thus risking discovery by other people.
- Retaining the same password for long periods, increasing the window of opportunity for an impostor if the password has been discovered (or has previously been shared).
- Using the same password on multiple systems, with the consequence that a breach on one system potentially renders the others vulnerable.

However, before laying the blame entirely upon the users, it is worth considering how they are supposed to know how to

* Tel.: +44 1752 233521; fax: +44 1752 233520.
E-mail address: steven.furnell@plymouth.ac.uk
0167-4048/$ – see front matter © 2007 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2007.09.001

do things correctly, because it seems that, in many cases, they are expected to work things out for themselves. For example, in workplace contexts, there is ample evidence of security requirements not being adequately promoted, and awareness remaining low as a consequence (Ernst & Young, 2006). However, the importance of good password practice extends beyond this, and routinely applies to members of the general public when using web-based services. In this sense, it could be argued that the ability to select and maintain good passwords is one of the standard skills that an e-citizen ought to possess. However, the fact remains that they still need to get guidance from somewhere, and ideally be supported in handling the burden of password management. In the absence of appropriate help, prior research has suggested that users tend to make up their own rules, and end up choosing insecure passwords as a consequence (Adams and Sasse, 1999). With this in mind it is relevant to examine the extent to which websites can be relied upon to offer advice for selecting and using passwords, in order to see if they are helping to support good practice, as well as improving the usability of the approach.

2. Assessing password guidance and policy in practice

In order to investigate the situation, an assessment of password practices was conducted via an examination of 10 leading websites (listed in Table 1). All were selected from within the top 100 entries in the Alexa Global Top 500 websites (http://www.alexa.com/site/ds/top_500) during mid-July 2007, and were chosen to represent a range of popular online services that are likely to be used by the general public (i.e. rather than being specifically targeted towards a technical audience). Although not an extensive sample by volume, it nonetheless captures a number of the leading and most recognised online brands at the time of the study, whose password practices are therefore likely to influence the largest proportion of end-users (as well as potentially being used as a baseline to be followed by other sites).

The sites were assessed by creating user accounts and subsequently following the available processes for changing and recovering (or resetting) passwords. Three key aspects were then assessed in each case:

1. Whether the sites provided any guidance to users in relation to selecting passwords, and (if so) the extent of the coverage.
2. Whether any restrictions were imposed upon permissible passwords, in order to reduce the potential for users to make poor choices.
3. Whether a means was offered to assist users who had forgotten their password, and (if so) the process by which reset or recovery was achieved.

From this it can be seen that the first two points relate to encouraging good practice, while the third relates to helping the user. The findings from the assessment are presented and discussed in the sections that follow.

Table 1 – Ten popular websites selected for assessment

Site	Description
Amazon	Online retailer with over 40 categories of product.
Bebo	High school and college social networking site.
eBay	Online auction service.
Facebook	Social networking site.
Friendster	Social networking site.
Google	Search and content portal.
MSN	Search and content portal.
MySpace	Social networking site.
Yahoo!	Search and content portal.
YouTube	Online streaming service, to view and share video content.

3. Availability of password guidance

This aspect was assessed at initial registration, as well as at the stage when users subsequently changed their passwords (which, in some cases, revealed a curious situation in which no guidance was provided in the first instance, but was available later). The most notable finding is that majority of sites provided little or no guidance, leaving users to select passwords in a potentially ad hoc manner. In some cases, although no upfront advice was available, users would nonetheless receive guidance indirectly, as a result of warning messages that appeared if they attempted passwords that contravened the restrictions imposed by the system. The findings for each of the assessed sites are summarised in Table 2.

As the table clearly indicates, the general situation in relation to provision of password selection guidance was poor. When looking at the individual cases, both Amazon and eBay were surprising in the sense that although they provided some good password guidelines, these were only presented when a user *changed* their password (i.e. they are not made available when a user first registers with the site and the password is initially selected). Facebook also suffered a similar criticism, although its guidelines were less extensive, and were presented in an even more restricted context.

By far the best in terms of guidance were the Google and MSN sites, providing relevant advice to the user and a means of checking their choices via a password strength meter. By contrast the vast majority of sites provided no explanatory guidance at all. Thus, while they may still have imposed some restrictions upon the possible choices, users may not have understood *why* these constraints were required.

So, in spite of a few good examples, the overall findings here revealed the paucity of guidance that is actually provided on some of the most popular websites, and raises the question of how users can be expected to follow good practice if sites do not emphasise it to them. Of course, security-conscious users can easily locate suitable guidelines for themselves via a web search, but this requires extra effort that they should not be expected to make.

With the above comments in mind, it is worth considering the sort of guidelines that it would be useful to provide. A suggested baseline set is provided below (worded in a manner that could be presented to end-users), and it is notable that they include not only the statement about what the user is