Security Education: The Challenge beyond the Classroom

Steven M. Furnell

Security education: The challenge beyond the classroom

S.M.Furnell[1,2]

[1] Centre for Security, Communications and Network Research, Plymouth University,
Plymouth, United Kingdom
[2] Security Research Institute, Edith Cowan University, Perth, Western Australia

sfurnell@plymouth.ac.uk

Abstract. While it is easy to identify formal security education efforts directed towards professional programmes and academic curricula, it is arguable that the far larger population of end-users rarely benefit from such focused consideration. The paper discusses the nature of the challenge and presents survey evidence to illustrate that users are not coping with the technologies that they are expected to interact with, even when the threats concerned are relatively long-standing. Specific results are presented to show the persistence of bad practice with passwords, alongside the difference that can result if more effort were to be made to promote related guidance. Further evidence is then presented around end-user practices in relation to malware protection, suggesting that their limited understanding of the threats often leads to them protecting some devices but overlooking others. The discussion then concludes by recommending more proactive approach when targeting the end-users who may otherwise be unaware of their risks.

Keywords: Security education, End-user awareness, Passwords, Malware.

1 Introduction

As the importance of the domain has increased, there has been a corresponding growth in the range of academic programmes and professional accreditations that one can pursue in order to build and demonstrate a level of competence (e.g. see [1] for an indication of the range of available certifications). However, security issues are far more pervasive than the workplace environment, and so it is clearly not enough for efforts to focus solely upon the would-be security professionals. Indeed, the real security education challenge facing modern society goes beyond the issue of developing academic curricula and specifying appropriate bodies of knowledge from which to certify the industry practitioners, and actually represents a relevant issue for all IT users.

This paper begins by briefly evidencing the breadth and magnitude of the security awareness task that can now confront typical IT users. It then moves on to present evidence of difficulties that users can still face in dealing with long-standing security technologies when they have not been guided to use or regard them appropriately.

The discussion then concludes with thought towards the more proactive stance that ought to be taken in terms of promoting and requiring security practice amongst the end-user community.

2 Too much to know?

It is relevant to recognise the magnitude of the challenge that now faces users in terms of understanding the various security features that are placed before them. As an example, Figure 1 presents an illustration of this, taken from the Security-related Action Center settings within Windows 8. There are a total of nine distinct aspects that users apparently need to be aware of in order to know that their operating system's security features are configured and operating correctly. Of course, most users are likely to be fine in terms of taking reassurance that things are 'On' or 'OK', but they are likely to be rather less likely to understand what it all really means. Moreover, in cases where something is showing a different status (e.g. in the Figure it can be seen that Network Access Protection is currently 'Off'), they ideally need to be able to take a view as to whether that represents a problem for them.

The real challenge is that the situation depicted in Figure 1 is by no means atypical of those that can now be regularly encountered, and the observation applies across multiple operating system platforms and end-user applications. One positive aspect is that many aspects now come pre-configured with security enabled (e.g. with OS firewalls, automatic updates, and wireless encryption all being cases where the default settings have changed from security 'off' to 'on' in the last decade or so). However, default settings will not be appropriate for all scenarios, and so if they are to make effective and informed use of the security that is available to them, users need to have a tangible baseline of knowledge and understanding, and this in turn needs to be fostered through appropriate efforts towards awareness and education. The next section proceeds to present some related evidence for these claims.

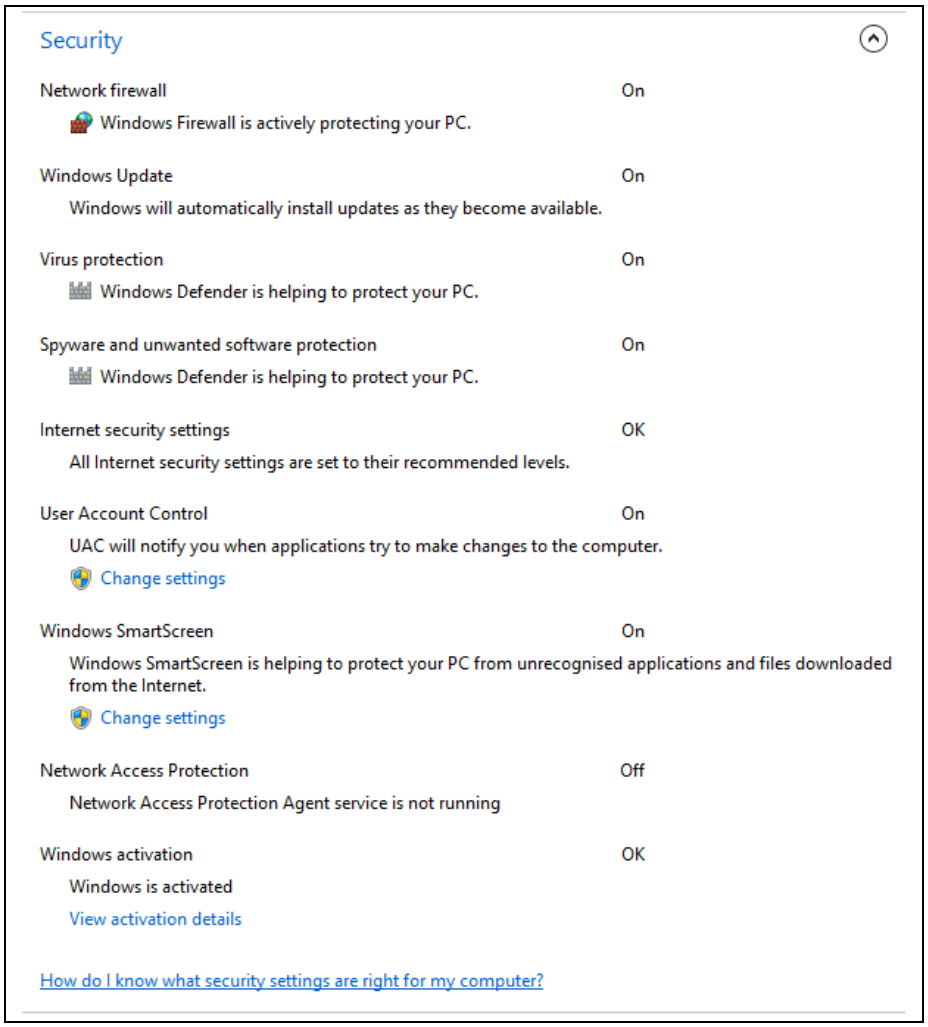

Fig. 1. Baseline security options facing end-users in Windows 8

3 Evidencing the impact of security education

While Figure 1 listed a range of features that can now be found on current systems, users have not even proven themselves to be competent at using the security technologies that have surrounded them for years. A classic, but nonetheless valid, example here can be provided in relation to passwords. A recent survey of 246 IT users, conducted by the author's research centre, revealed the limited extent to good password practice is actually followed. Respondents had been asked to consider the password used for their most important/valuable account, and Table 1 shows the

extent to which individual aspects of practice were reflected across the respondent group. Perhaps most significantly, only 25% of respondents were able to satisfy all five points [2].

Table 1. Responses to statements around password usage

Statement	Agreement (n=246)
It is at least 8 characters long	82%
It has alphabetic and numeric characters	84%
It includes other characters (e.g. punctuation symbols)	49%
It uses a word you would find in a dictionary	18%
It is based on personal information about me	26%

Of course, some might argue that these findings actually reflect the failing of password *technology*, which users find difficult to use properly and therefore find means to simplify in order to aid their own ease of use. However, this potentially overlooks the fact that there is often a massive weakness in the password education efforts to which such users are exposed. Not only do many organisations still do little or nothing about it (other than perhaps having a few rules, which they may *enforce* but do not *explain*), but the websites on which many users are likely to be most regularly encountering passwords also do far less than they could in order to promote and encourage good practice. For example, in an assessment of ten leading websites against their enforcement of six possible aspects of good practice (namely *enforcing* a minimum length of 8 characters and the use of multiple character types, alongside *preventing* the password choice from being the user's surname, user id the word 'password' or wider dictionary words) the overall enforcement rate was just 42% [3]. Moreover, the sites concerned were extremely inconsistent in the level of guidance that they provided to users, and while there were some cases in which comprehensive and explanatory guidance was offered, most sites seemed content with warning messages for which the underlying rationale was not explained (e.g. a Facebook message at the time would advise users that 'Your password should be more secure. Please try another.', without giving any indication of how more security might be achieved). Looking again to more recent research, we have sought to investigate whether better guidance may yield better behaviour, and the initial indications suggest that it does. Using the five points from Table 1 as a basis for good practice, 27 users were asked to created password-protected accounts as the starting point for participation in a study of website usability. Unbeknownst to the participants, there were two variants of the site – one in which password guidance was provided, and the other in which they were left to select passwords unaided (with neither case actually *enforcing* any password rules). There were notable differences in the results, with the guided group (n=13) scoring an average of 3.8/5, against just 1.9/5 from the unaided (n=14) group [2]. Analysis revealed that areas such as password length, use of other characters, and avoidance of personal information were the ones most likely to be improved by the provision of the guidance. Thus, what this can arguably be shown to illustrate is that education and awareness can have a tangible effect upon the users' behaviour with a technology that they would otherwise be inclined to use badly.

4 Knowing a little, but not enough

While it would be rare these days to find users that are totally ignorant of the risks to be faced online, it would be equally fair to say that while users often have an awareness of certain threats that can affect them, the *extent* of their knowledge does not stretch very far. A very good example here relates to the threat of malware, which (like passwords) can now be regarded as a long-standing aspect of the user-facing security landscape. Indeed, antivirus protection is now a very commonplace safeguard on PCs in both home and workplace contexts. However, there is again evidence that users' real understanding of the threat has not kept pace with the technology that they are using, and this is particularly apparent in relation to mobile devices such as smartphones and tablets, where recent years have seen a sizeable increase in the actual threat). For example, while the problem had been largely theoretical for many years (but with predictions having been made by antivirus vendors since the mid-2000s), the period around 2011/12 saw the market conditions become such malware writers began to take a more active interest. Key aspects were the emergence of a sizeable population of device owners, and the fact that sufficient of them was using an OS platform that could be targeted. As a consequence, according to figures from Kaspersky Lab, 2012 saw a massive rise in the number of malicious programs on the Android platform, rising from less than 6,000 at the start of the year to over 43,000 by the end [4]. Android was consequently playing host to over 99% of the malicious programs identified on mobile platforms (which is in part thanks to its more open app distribution process when compared to its main competitor, iOS, where apps have to pass an approval process before being placed on the platform's official App Store), and thus attracting a significantly disproportionate share of the mobile malware when compared to its share of the mobile device market.

The clear message here is an increasing threat to the associated user population, but returning again to the survey of 246 end users, it would appear to be a message that is not naturally getting through. From this group, 28 of them had an Android-based mobile device, but only 19% of these had antivirus protection for it. While it could be argued that this small sample might just be an unrepresentative group of security-resistant users, an interesting point to note was that 82% of the same sub-group had antivirus protection on their traditional PC. As such, it seems likely that lack of awareness rather than lack of regard for security may have been the main reason for so many more mobile devices going unprotected. This situation suggests that if the risks of new platforms are not overtly communicated, users currently seem to have little ability to take the lessons learned in one context (e.g. the desktop PC) and apply them to another (e.g. the mobile device).

5 Recommendations and Conclusions

The evidence above points towards a clear need for security education in the wider context, as there is enough evidence from successive and sustained cases of bad practice to show that they are not skills that users can be relied upon to naturally possess or develop as part of their wider IT development. If the situation is to improve, then the obvious answer is that something more proactive needs to be done about it. However, this is again an area in which attempts have historically been poor, even within workplace contexts. For example, findings from Ernst & Young's Global Information Security Survey 2012 revealed that while the top-rated area of risk-exposure was 'careless or unaware employees' (ranked first out of 16 threats/vulnerabilities, and rated first choice by 37% of respondents), the issue of 'Security awareness and training' was ranked as a top security priority by only 9% (placing it 17th out of twenty possible areas), thus showing a clear disconnect between the problem and what organisations are prepared to do about it [5]. Without a tangible uplift in terms of attention and investment, it seems unlikely that the issue will heal itself automatically.

The onus is to increase threat awareness for private individuals and staff within organisations. While much of the responsibility for the latter must still rest with employers (and so can also be seen to be within their control), the issue of wider public awareness requires necessarily broader steps to be taken. Recent years have already seen some notable activities in this direction, with a European example being the introduction of a Cyber Security Month [6], which took place for the first time in October 2012. However, one of the main findings documented from this was the need to "Better define the specific audience that is targeted by the awareness initiative in order to tailor the message content to the target group's knowledge or technical aptitude" [7], which serves to illustrate the ongoing challenge that awareness-raising is likely to pose.

In many ways, the way in which users are encouraged to think about their IT devices is still based around the wrong model. While they are routinely purchased in the same manner as other consumer electronics devices, a more appropriate parallel can be made to the purchase of a car. With a car there is an upfront recognition that the driver needs to be competent in order to use it safely, and that the car itself is expected to be fitted with a range of safety and protection features, and that the vehicle needs to be appropriately maintained if it is to continue to operate correctly. While it would not be realistic to regulate IT usage to quite this degree, there are nonetheless some steps that could be taken to alter the mindset around it. As an example, here are a few related thoughts:

- There needs to be something that clearly highlights and explains the key issues for new users as they take product home. While there is often plenty of material to be found for those inclined to go looking for it (e.g. in the UK a good user-facing resource is provided by GetSafeOnline,org), many people will not be aware enough to look for this in the first place. Even the provision of a leaflet in the box with the product could go a long way to raising upfront awareness.

- Users need to be encouraged to be aware of security issues and practices from their early encounters with IT. Inclusion of security education as a 'key skill' within school and university curricula would be a relevant contribution here, thus ensuring that relevant baseline exposure is provided for all users, rather than just those that have chosen to study the topic as the basis for a career. This does not equate to turning everyone into security experts, but rather to ensure that protection issues are given an effective level of emphasis as part of any wider introduction to IT usage.
- Increase the expectation (and perhaps obligation) to use appropriate safeguards. While many devices will now be provided with software such as antivirus or wider Internet Security suites as part of the bundle, it is still perfectly possible to purchase and use PCs without this being in place. Clearly there still needs to be a place for consumer choice over products, and competition between associated vendors, but it ought to become a question of *what* product to have rather than *whether* to have one). Moreover, looking at the wider context of online devices, there is currently far less of an established culture of bundling protection with smartphones and tablets, but they (and their users) are becoming equally in need of protection.

While the paper is unable to report the results of putting such ideas into practice, this is clearly no basis to accept the status quo. Indeed, what we *can* see from the findings of the earlier studies is the result of the current approach. In the meantime, security educators should take the opportunity to push their messages to as wide an audience as possible, in order to raise awareness and support a more effective security culture amongst the public at large.

6 References

[1] Goodchild, J. 2012. "The Security Certification Directory", *CSO Online*, 24 October 2012. http://www.csoonline.com/article/485071/the-security-certification-directory (accessed 25 April 2012).

[2] Furnell, S. and Bär N. 2013. "Essential lessons still not learned? Examining the password practices of end-users and service providers", to appear in *Proceedings of HCI International 2013*, Las Vegas, Nevada, 21-26 July 2013.

[3] Furnell, S. 2011. "Assessing password guidance and enforcement on leading websites", *Computer Fraud & Security*, December 2011, pp10-18.

[4] Kaspersky Lab. 2013. "Today's Mobile Threatscape: Android-Centric, Booming, Espionage-friendly", Virus News, 28 February 2013. http://www.kaspersky.com/about/news/virus/2013/Todays_Mobile_Threatscape_Android_Centric_Booming_Espionage_friendly.

[5] Ernst & Young. 2012. *Fighting to close the gap – Ernst & Young's Global Information Security Survey 2012*. EYG no. AU1311. www.ey.com/giss2012.

[6] ENISA. 2011. *European Month of Network and Information Security for All - A feasibility study*. 14 December 2011. ISBN-13 978-92-9204-056-7.

[7] ENISA. 2012. Be Aware, Be Secure. Synthesis of the results of the first European Cyber Security Month. 17 December 2012. ISBN 978-92-9204-063-5.