A practical usability evaluation of security features in end-user applications

S.M.Furnell, D.Katsabas, P.S.Dowland and F.Reid
Network Research Group, University of Plymouth, Plymouth, United Kingdom
info@network-research-group.org

Abstract. The presentation and usability of security features can represent a significant impediment to effective protection for end-user systems. In order to investigate the nature and level of problems that can be encountered during attempts to use security within standard end-user applications, this paper presents results from a series of hands-on user trials from web browsing, word-processing, and email activities. The results are based upon structured tests involving 15 participants (representing a mix of general and advanced users), revealing that in many cases users appear to have difficulties understanding and performing baseline security tasks within the applications concerned.

1 Introduction

Security-related software is now a standard provision in today's PCs, from specific tools such as anti-virus and anti-spyware utilities, through to the presence of protection features within more general applications. Although all can have a valuable role to play, the benefits can be significantly undermined if users cannot understand and make effective use of them – in some cases to the extent that they are effectively left unprotected as a result [1,2]. As such, the usability of security is a crucial factor in ensuring that it is able to serve its intended purpose. Although this requirement is now beginning to achieve much more widespread recognition [3,4], usable security remains an area in which current software is often notably lacking.

As part of a wider study into the nature of the usability problem, this paper presents the results of a hands-on trial involving the use of security-related features within a number of applications, in order to determine how well they can be understood and used by the intended end-users. Prior investigation has already established general evidence of problems, based upon the responses from over 340

users in a questionnaire-based study [5]. This survey revealed that respondents had significant difficulties understanding the language and appearance aspects of the user interfaces, suggesting that these would be an obstacle to practical usage. However, the survey had not been able to assess whether respondents would have been able to overcome their difficulties if they encountered such features in a practical context, and thus the next phase of the research aimed to get a deeper insight into users' ability to actually complete security-related tasks.

This paper begins by presenting an outline of the methodology adopted for the trial activities, followed by discussion of the results observed, with specific attention devoted to the findings from each of the applications assessed in this phase of the research. Brief conclusions and the outlook for future research are presented at the end of the paper.

2 Trial methodology

The trial involved 15 participants in a series of hands-on activities, using security features within a range of software applications. The trialists were a mixture of academic and administrative staff, and students from within the local university environment. All were regular users of IT, and familiar with the general operation of the Microsoft Windows environment in which the target applications were running. Within the group, eight participants were classed as general users, with a familiarity with using IT (and some of the applications concerned) on a regular basis, but with no specific knowledge about the detail of the technology. By contrast the other seven participants were advanced users, all with academic qualifications relating to IT and some prior knowledge in relation to security. Sampling in this study was purposeful rather than random, and was determined by the representativeness of trialists to the broader user population, the intensive nature of the think aloud methodology employed in this study, and the diminishing returns of using large samples for identifying usability problems using this method [6].

The activities were generally chosen to be representative of tasks that security-conscious users may wish to perform, as well as things that other users may find themselves needing to do as a result of the default security settings within the application, or settings that other users had applied. The required tasks were presented in writing and explained to the participants. Note that they were told what they needed to achieve, but not how to do it, and the aim of the trial was to determine whether they could understand and use the security features within the application sufficiently well to achieve the objectives. Participants were allowed to make use of any available 'help' features within the applications, as well as refer to online sources if the thought occurred to them to do so. In addition, the researcher conducting the trial was on hand to monitor their progress, provide any necessary help (as requested by participants), and to answer any questions regarding the progress of the tasks. Participants were also free to end the trial at any time.

Participants were encouraged to follow a 'think aloud' protocol, requiring them to explain their thought processes and decisions as they attempted to perform each of the tasks [7]. The intention here was to provide insights into how problem features

had been interpreted, which could hopefully help to inform improvements to future implementations. However, at the time of writing, these aspects have yet to be fully analyzed, and so the information conveyed here will be restricted to the results regarding success or failure of participants to complete the tasks. Consequently, the present paper offers summary statistics that are necessary to contextualise the protocol analysis that is currently underway

The full trial required security-related tasks to be performed within six software environments. Three of these were security-specific utilities (namely the Windows Firewall, the Zone Alarm firewall, and Norton Antivirus), whereas the others were general applications that included security-related features (namely Internet Explorer, Word, and Outlook Express). The findings presented here are restricted to those from the latter three applications, as these were common to the earlier survey exercise, and the findings in relation to the security-specific tools are not directly considered in this discussion. It should be noted that the significant focus upon Microsoft applications within the trial was in no way intended to imply that Microsoft's products were particularly at fault in terms of the usability of their security when compared to alternatives from other sources. The basis was rather that they were judged to be the applications that participants were most likely to use (as was borne out, in most cases, by the findings), and thus any difficulties encountered in the trials could be more directly related back to the usability of the security aspects rather than participants' unfamiliarity with the applications in general.

Each stage of the trial ended with the completion of a brief feedback questionnaire to record the participant's views about the application they had just used. Amongst the standard questions they were asked for each application were how easy it had been to use the available security, and how long it had taken to find and use the security features required. In terms of the ease of use rating, participants were offered the following options:

- Easy (Did not encounter any difficulties at all)
- OK (with minor difficulties)
- Hard (experienced several difficulties during the tasks)
- Unable to use

Meanwhile, the options for how long participants felt it had taken to locate and use the security were as follows:

- Very quick (it was obvious where to look for the available security and what to do)
- Quick (but I would expect the process to take less time)
- Slow (I worked around the application for some time before being able to find and use the available security)
- Very slow (it took a long time to find the security and determine how to use it)

The findings from these assessments are presented for each of the applications under discussion, alongside the actual results indicating how successfully the participants performed each of the required tasks.

3 Usability trial results

The sub-sections that follow present the results observed for each of the three applications. Although the size of the participant group was too small to yield truly meaningful percentages, some of the results are nonetheless presented in this format in order to enable an easier appreciation of the proportion of users that were able to complete each task (with the calculations for general, advanced and overall users being based upon 8, 7 and 15 participants respectively). The tables also present the overall time taken to complete the trial tasks for each application (although it should be noted that this includes the time taken to complete the aforementioned feedback questionnaire, and so the actual time spent completing the hands-on task was typically two minutes less than the values shown in the tables).

3.1 Trial activities involving Internet Explorer

For this stage of the trial, participants were asked to attempt a number of tasks in relation to these elements of browser security. The first was to simply determine the current security setting of the browser, requiring users to find and understand the related options interface via the Tools menu and then recognize the current setting of the slider shown in Fig. 1. The next task involved visiting a series of four websites, and determining whether participants could recognize which ones involved secure connections (i.e. recognizing the presence or absence of 'https' in the URL and/or the padlock icon in the browser status bar). Having completed these observational tasks, the next three activities involved making changes to the security configuration. Firstly, participants had to adjust settings to permit the downloading of a file – which involved reducing the security level shown in Fig. 1 from 'high' (which had been preset for the purposes of the trial) to 'medium'. The next adjustment involved a deeper level of configuration, via the 'Custom Level' settings, to get the browser to prompt before using ActiveX controls. The final tasks involved the use and concept of Web content zones, as shown at the top of the main security settings window. Participants were firstly asked to add a website address to the 'trusted' zone and another to the 'restricted' zone, and then asked to explain their understanding of what the zones actually meant in order to determine whether they knew what they were doing.

The majority of the participants (11 of 15) used Internet Explorer as their regular web browser, and thus (in theory) many of the tasks should not have posed a major problem. The actual levels of success observed for each of the tasks (overall, and split according to the experience levels), is shown in Table 1. It is notable that even with the baseline task (determining the current security settings), a quarter of the participants were unable to complete the actions required of them, and it was particularly surprising to find that only a third were able to determine whether or not the connection to a particular site was secure. Indeed, even where some tasks were completed successfully, some participants often took a fairly long time to do so. The other notable results in the table relate to the two tasks involving web content zones – which are the only findings from the three applications under discussion in which the 'general' users were found to out-perform the 'advanced' ones. One of the main

reasons for this seemed to be that some of the advanced users had pre-conceived ideas about what the 'trusted' and 'restricted' categories might mean, and consequently did not read the on-screen information closely enough (e.g. trying to add 'http' sites to the trusted list, when the browser default indicated that server verification was required, and therefore permitted only 'https' sites to be added for this zone).

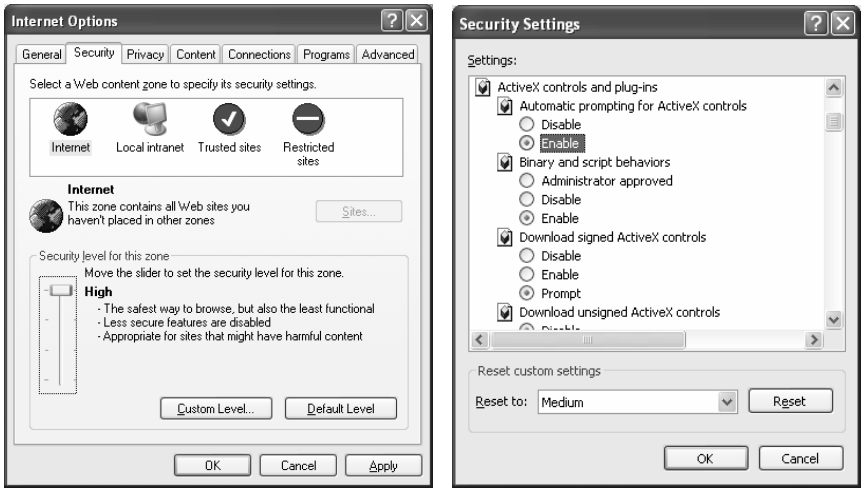

Fig. 1. Security options settings within Internet Explorer (main and custom level)

Table 1. Successful completion of user trial activities within Internet Explorer

Task	General users (%)	Advanced users (%)	Overall (%)
Determine the current security settings level within the browser	63	86	73
Determine whether communication with a specific webpage is using a secure connection	12	57	33
Customise security settings in order to permit download of a file	38	86	60
Customise security settings in order to be prompted before running ActiveX	12	71	40
Add websites to the 'trusted' and 'restricted' Web content zones	88	71	80
Explain the purpose of the Web content zones	88	43	67
Overall success	50%	69%	59%
Average time to complete all tasks	20m00s	15m50s	18m13s

Having completed the tasks, the participants were asked to express their views on how easy they had found it, and how long they felt the process had taken. The

related findings are illustrated in Figs. 2 and 3, and show that in spite of the fact that many participants had been unable to complete a number of the tasks, the overall feelings were generally positive from this stage of the trial.

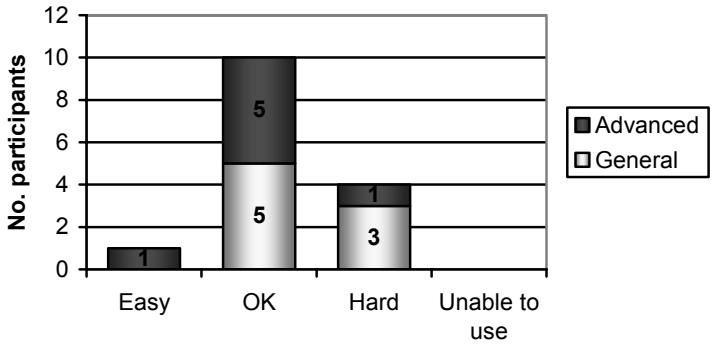

Fig. 2. Perceived ease of use of security within Internet Explorer

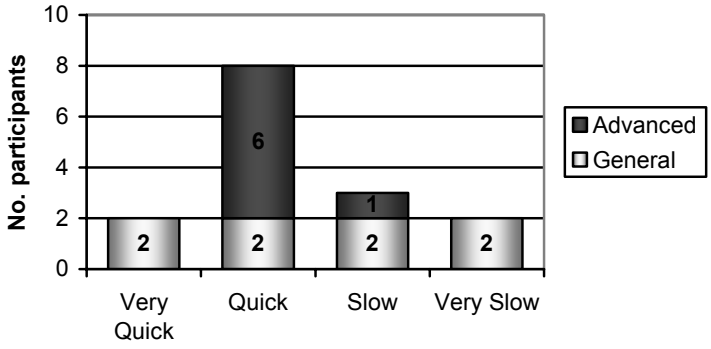

Fig. 3. Finding and using the required security features within Internet Explorer

3.2 Trial activities involving Word

As with Internet Explorer, the majority of participants were regular users of Word and so were familiar with the general interface and functionality. For the tasks in this phase, participants were provided with a sample Word document to work with and then asked to perform a number of security and privacy-related operations upon it. The first was to assign a password in order to restrict reading of the document.

This required users to locate the password protection facilities within Word (located again within options under the Tools menu), and then determine which of the two password possibilities they were meant to be setting. The two choices here are illustrated in the uppermost portion of Fig. 4, and our previous work [8] has commented upon the potential confusion that this presentation can generate. The next task required users to click on the 'Advanced' button and determine whether they could understand how the options they were then presented with (see Fig. 5) actually related to the password they had specified on the previous screen. The next task involved utilizing other features from Fig. 4 to ensure maximum privacy for their document, and then to assign a second password to prevent unauthorized changes to its content. The final activity involved inspecting and adjusting the macro security settings in order to ensure that a warning would be displayed when opening a document containing a macro. To test their decision, participants were then required to determine which document, from a pair pre-stored on the trial system, had macro content in it.

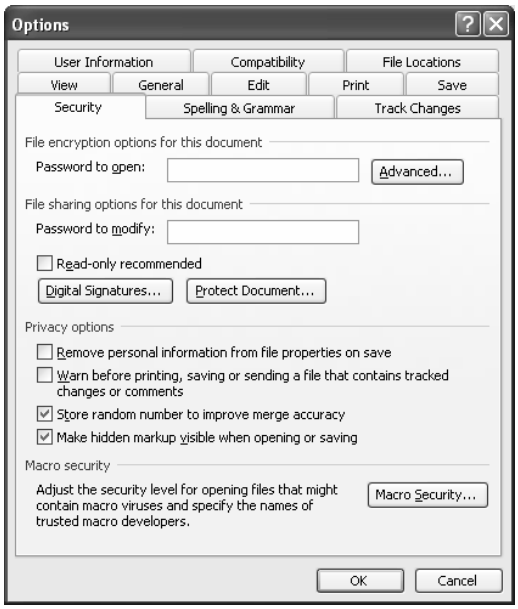

Fig. 4. Alternative password options in Microsoft Word

As the results in Table 2 illustrate, the overall findings for the Word tasks were not greatly positive, and exhibited a pronounced difference between the general and advanced users. While some of the areas of difficulty (e.g. in relation to encryption options) were anticipated, it is notable that only a third of the participants were able to successfully complete the baseline task of adding password protection to prevent a document from being read. This very much confirmed the earlier suspicions that this

interface presents particular challenges for users to understand a security feature (i.e. passwords) that they would normally consider themselves familiar with.

Fig. 5. The advanced encryption options in Word

Table 2. Successful completion of user trial activities within Word

Task	General users (%)	Advanced users (%)	Overall (%)
Password protect a document to prevent it being read	25	43	33
Understand how the 'advanced' (encryption-related) options relate to the password	12	43	27
Protect the privacy of the document.	75	100	87
Password protect a document to prevent changes	25	57	40
Configure the macro security settings in order to be warned when opening a document with a potentially unsafe macro	12	57	33
Overall success	30	60	44
Average time to complete all tasks	11m30s	11m50s	11m39s

Having completed the tasks, the participants' views were as shown in Figs 6 and 7. Compared to the IE findings, we can now observe a more significant split between those who found the tasks fairly straightforward and those who encountered difficulties (with the 'general' users clearly faring worse overall). Additionally, most respondents had even more negative views about the time required to find the features in the first place.

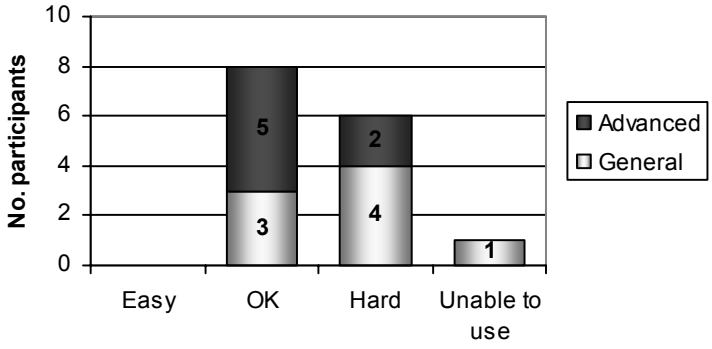

Fig. 6. Perceived ease of use of security within Word

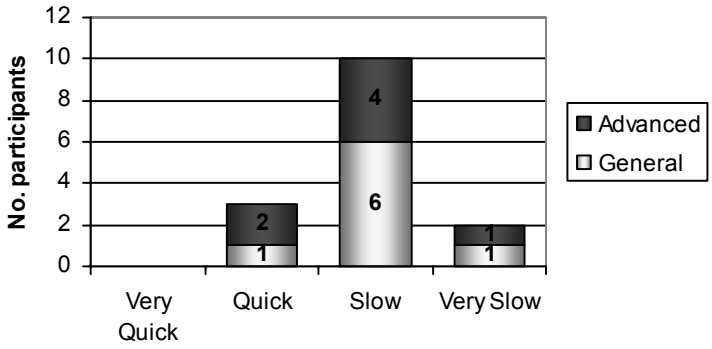

Fig. 7. Finding and using the required security features within Word

3.3 Trial activities involving Outlook Express

Whereas the other two applications were generally well-known to the participants, only four (all from the 'general' user category) indicated that they used Outlook Express as their default email client, and so in this set of tasks the participants were generally using an application that they were less familiar with. Having said this, many of the participants used the full version of Outlook and/or Outlook Web Access on a regular basis, and so were not totally unfamiliar with the general style of the interface.

For this stage of the trial, participants were asked to attempt four tasks. The first was to send an encrypted email to a given recipient, and the challenge here was for them to realize why it ultimately was not possible. Although the 'New Message'

window in Outlook Express offers the apparent option to 'Encrypt' a message (see Fig. 8), to do so requires the sender and receiver to have established a DigitalID beforehand. The next task reflected the fact that, by default, Outlook Express removes access to 71 potentially unsafe categories of attachment (e.g. .exe, .mdb, and .vbs files) [9]. However, in some contexts, a user may have a genuine requirement to receive such a file from a trusted source. In this situation, they would need to determine how to configure the settings to allow access to the attachment to be regained, and this was the scenario presented to the participants. The final pair of tasks related to blocking email senders – initially requiring the user to block the receipt of email messages from a particular address, and then to locate and check the 'Blocked Senders' list to ensure that another address had not been blocked by accident.

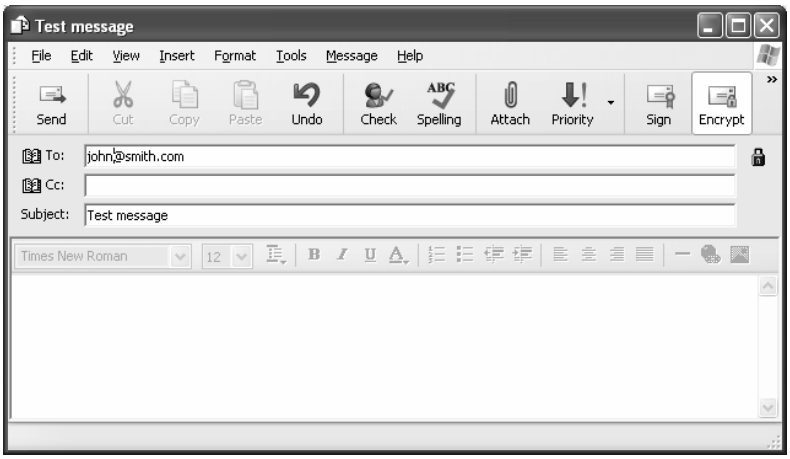

Fig. 8. Message encryption option within Outlook Express

The findings from this phase are presented in Table 3, and are notably the only set described in this paper in which less than half of the participants were able to complete any of the associated tasks. In view of the results from the table, it is perhaps unsurprising to find that the participants viewed Outlook Express as the most difficult of the three applications under discussion here (see Fig. 9). Although it could be argued that this reflects the fact that most participants did not normally use the application, it can be noted that two out of the four that *did* use it still indicated that they found it hard to use the security.

Table 3. Successful completion of user trial activities within Outlook Express

Task	General users (%)	Advanced users (%)	Overall (%)
Determine why they could not send an encrypted message.	25	71	47
Recover access to a blocked attachment	25	71	47
Block a sender who has been generating spam	12	57	33
Find the list of blocked senders	25	57	40
Overall success	22	64	42
Average time to complete all tasks	10m07s	9m20s	9m47s

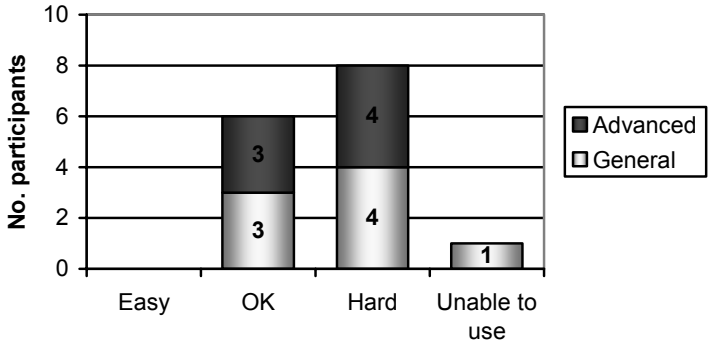

Fig. 9. Perceived ease of use of security within Outlook Express

In addition to finding it hard to complete the required tasks, the vast majority of participants clearly felt that it took too long to locate the security features and determine how to use them, as shown in Fig. 10.

4 Conclusion

The discussion here has illustrated the problems that can be encountered by users when attempting to perform security-related tasks within a number of standard PC applications. The difficulties that were encountered in the trials are particularly notable in view of the fact that all of the tests involved applications that are aimed at the general user community rather than specialists. Although it could be argued that there are other aspects of security for which usability is more critical (e.g. the ability to use authentication methods), and that some of the tasks involved in the trials would only be relevant for a subset of users, they still represent aspects of protection that some users could have a genuine desire to use.

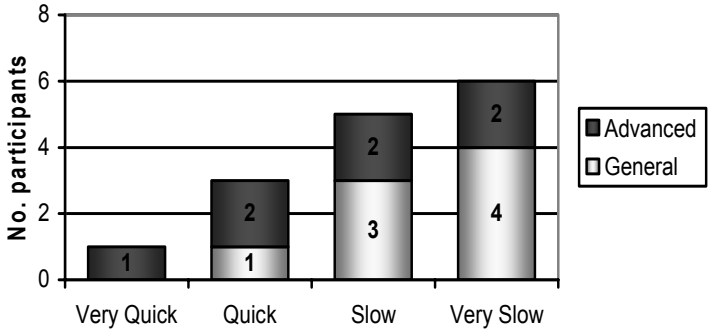

Fig. 10. Finding and using the required security features within Outlook Express

The ongoing research will use the results reported here, along with further findings from the trials, as a means of informing enhanced approaches to security interfaces and interactions. By establishing the areas in which users currently have difficulties, and more importantly the factors that contribute towards them, it is intended that enhanced alternatives can be devised and trialed in order to assess the potential for improvement.

References

1. Whitten, A. and Tygar, J. D. 1999. "Why Johnny can't Encrypt: A usability Evaluation of PGP 5.0", *Proceedings of the 8th USENIX Security Symposium*, Washington, D.C., USA, August 23–26, pp169-184.
2. DeWitt, A.J. and Kuljis, J. 2006. "Aligning usability and security: a usability study of Polaris", *Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS '06)*, Pittsburgh, Pennsylvania, USA, July 12-14, pp1-7.
3. Cranor, L.F. and Garfinkel, S. 2005. *Security and Usability: Designing Secure Systems That People Can Use*. O'Reilly. ISBN 0596008279.
4. CRA. 2003. *Grand Research Challenges in Information Systems*, Computing Research Association, Washington DC, September 2003. http://www.cra.org/reports/gc.systems.pdf.
5. Furnell, S.M., Jusoh, A. and Katsabas, D. 2006. "The challenges of understanding and using security: A survey of end-users", *Computers & Security*, vol. 25, no. 1, pp27-35.
6. Nielson, J. 1994. "Estimating the number of subjects needed for a thinking aloud test", International Journal of Human-Computer Studies, vol. 41, no. 3, pp385–397.
7. Lewis, C. and Rieman, J. 1993/1994. Chapter 5 in *Task-Centred User Inferface Design – A Practical Introduction*. See http://hcibib.org/tcuid/
8. Furnell, S.M. 2005. "Why users cannot use security", *Computers & Security*, vol. 24, no. 4, pp274-279.
9. Koch, T. 2004. "Outlook Express and Windows XP Service Pack 2: Several Problems or Superior Protection?", 21 October 2004, www.microsoft.com/windows/ie/community/columns/oeandsp2.mspx.