BOOK REVIEW

DON'T FORGET TO WRITE

David Harley
ESET, UK

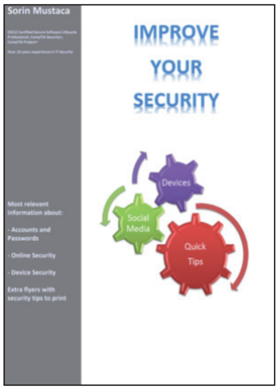
Industry veteran, prolific writer and educator David Harley reviews two recent published eBooks that aim to provide security guidance for consumers: Improve Your Security by Sorin Mustaca, and One Parent to Another by Tony Anscombe.

It sometimes seems that the security industry is still divided into the 'user education is vital' camp and the 'if education was going to work, it would have happened by now' camp [1]. Still, I doubt if even the most diehard proponent of the latter viewpoint really believes that matters would be no worse if we didn't make *any* attempt to teach the end-user anything about security.

There is, of course, no shortage of excellent user-oriented security blogs, white papers and conference papers relating to malware management (which I assume to be a major concern for readers of this publication). Good books are rather scarcer, and those of us in the industry who have attempted to write one have tended to find an audience either within the security industry itself, or among security administrators and managers. Books that have found a significant audience among end-users and home-users and that devote significant wordage to malware issues are less common. In fact, despite having either written or contributed to around a dozen security-oriented books myself, I've never managed to interest a mainstream publisher in a malware-oriented book that specifically targets consumers. Perhaps it's true, as it has been suggested, that Joe Average isn't interested enough in his own security to buy a book about it – though there are enough rather bad, consumer-facing books with a small amount of malware discussion to indicate that some publishers see a market there.

Nevertheless, from time to time, someone with real security knowledge does attempt to share that knowledge with the people who generally know the least. Regrettably, Eddy Willems' recent book *Cybergevaar* [2] (in Dutch) is beyond my linguistic skills (though hopefully there will be an English translation eventually). However, Sorin Mustaca's eBook *Improve Your Security: Everything you wanted to know about IT security and didn't know who to ask* [3] and Tony Anscombe's eBook *One Parent to Another: Managing technology and your teen* [4] *are* within my linguistic and technical competence, or so I'd like to believe. Both authors are well known in the security industry. Indeed, Anscombe's book is published under the aegis of his employer, *AVG*, as a free PDF download. Mustaca's book is published by *Leanpub*, though his employer, *Avira*, gets a mention on the Acknowledgements page and some of the advice given is *Avira*-centric. *Improve Your Security* is available in PDF, EPUB and MOBI formats with a recommended price of $4.99, but the actual sum is left to the buyer.

IMPROVE YOUR SECURITY



Mustaca's book, as its subtitle suggests, is wider in scope than Anscombe's, and in some areas has a more technical bias. It is divided into five main sections:

1. Accounts and Passwords
2. Online Security
3. Device Security
4. Tips that you can print to improving [*sic*] your security
5. Protect yourself against advertisements and tracking.

The first section, which deals with accounts and passwords, explains what a cryptographic hash function is and what salting is. It describes a few simple strategies for making a password harder to guess, and provides some useful advice on what *not* to do. There's some good advice here, but I suspect that some readers will find it a little scary and even confusing, visually. Mustaca also includes some thoughts on the deficiencies of password storage, advocating memorization as a better course of action. There is also some consideration of the high-level implications of password and account management, and the very sound recommendation to change default passwords. (Think that you don't need to worry about account management on a home computer? You might think differently when you read the story of the child who nearly bought a Harrier jump-jet.) Password strategies are a contentious subject, but this should at least start readers thinking beyond 'qwerty' and '123456'. This is a topic that could usefully be expanded in a future version of the book. It's true that there are many resources out there offering advice for password selection, but their quality is extraordinarily variable. I'd like to see a section on PIN selection strategies added at some point, too.

Networks and safety nets

The next section, 'Online Security', provides a simplified model of network security, then goes on to explain how to ‘harden your Facebook account’ with account settings. Next is a description of how to enable two-factor authentication for *Google*, *Facebook*, *Dropbox*, *Twitter* and *LinkedIn*, complete with screenshots. My guess is that the network security model will be slightly over the heads of much of the target audience, but many will appreciate the advice on improving their security on social network sites, and understanding just why it is that so many sites are now pressing them to go the two-factor route. Finally, there’s a consideration of ‘How to combat the brute force attacks on WordPress blogs’. This is aimed at self-hosted *WordPress* installations rather than bloggers using accounts on wordpress.com, and seems a little out of place in a collection of articles mostly aimed at consumers.

Our house (is a very, very, very safe house)

Section III, on device security, looks at setting up a laptop securely using ‘active’ authentication measures (BIOS, Power On, HDD and OS authentication), and ‘passive’ measures (data encryption with *TrueCrypt*, working as a non-privileged user, restricting booting from external devices and media, and deactivating ‘Autorun’). Next, there’s a discussion of software updates and an illustration of the process of securing a computer which draws an analogy with making your house secure. A section on password protection for smartphones is followed by a section on backups, then there’s a longer look at data encryption with *TrueCrypt*. The final parts of this section consist of a terse description of ‘What to do if your computer has a virus’ (unsurprisingly, including a brief and rather *Avira*-focused ‘How-To’), and notes on removing junk and freeing space. Some good advice, but I’d have liked to have seen a bit more guidance on avoiding the many all-but-useless registry cleaners and the like that are lurking out there.

Tip of the iceberg

The ‘Tips’ section includes ‘20 Tips to improve your security’; ‘5 signs you’ll notice if your social media account has been hacked’; ‘How to secure a new computer in 10 steps’; ‘How to protect your social media account’; ‘10 tips to improve your mobile devices security’; ‘Security tips for safe online shopping’ and ‘5 tips to keep your mobile devices safe while using 3/4G and LTE’. This kind of content is very useful to (and popular with) consumers.

Section V is a How-To: ‘Protect yourself from advertisements and tracking’. I’m sure we’d all like to know how to do this, but there is an awful lot more to say about telephone scams, and I’m not convinced that the softly-softly approach to requesting removal from contact lists is always effective. (And a four-letter word is sometimes more satisfying…)

Nevertheless, I like this book. It could, perhaps, benefit from some editing and expansion of some of its topics, but there are plenty of naïve and confused consumers around who would undoubtedly benefit from Mustaca’s advice, and I hope he gets enough response to encourage him to develop it further.

Improve Your Security is updated frequently: the version reviewed is from 20 December 2013.

ONE PARENT TO ANOTHER

Tony Anscombe’s book is more polished, and takes more of a ‘Guide for Dummies’ approach, going to some lengths to play down the use of technical terms and acronyms. It is divided into a number of chapters:

1. Who should read this book?
2. What are connected devices?
3. Connectivity and communications
4. The smartphone
5. Everyone on their best behavior
6. Parental controls
7. Cyberbullying

Finally, a concluding section reminds us of ‘the big things to keep in mind’.

While Anscombe summarizes: ‘everyone who is a parent or *in loco parentis* should read this book’, Chapter 1 is actually a well-argued high-level justification of the need for the book. I can’t help thinking, though, that the people who have gone to the trouble of downloading the book were probably already aware that they needed to be prepared to help young people to meet the challenges of somewhat scary new(-ish) technology.

Chapter 2 makes the point that a wide range of objects we don’t necessarily think of as computers have become capable of being connected to the Internet, but focuses mostly on the fairly current examples of smartphones and (other) photographic devices with geo-tagging capabilities.

Chapter 3 is a little more overtly technical, expounding on and explaining some acronyms that someone new to the technology and concerned about how it works needs to know. It also touches on some basic password strategies and gives a non-technical explanation of two-factor authentication. A look at the fundamentals of using email includes a brief consideration of spam and a fuller consideration of phishing that should go a fair way to educating both child and parent as regards the recognition of scam messages delivered by various media. That's followed by a look at the dangers of public Wi-Fi, especially when it comes to sensitive transactions.

The section that follows looks at the security implications of Internet transactions away from home, using public access points and hotel Wi-Fi networks. Considerations of privacy lead into a brief description of the risks of geo-tagging and a longer summary of the issues around social networking, in particular *Facebook* and *YouTube*.

Terms of engagement

Chapter 4 is entitled 'The Smartphone Chapter': it starts by detailing some problems that can arise with incautious use of a smartphone and considers the particular parenting issues that arise when setting the terms of engagement for the use of phones by children and teenagers. While the adoption of many of the guidelines that Anscombe provides will be considered highly subjective, the suggested discussions on the consequences of illegal or pirated downloads and budgeting for apps and music is one that most responsible adults will probably have with their children at some point.

Chapter 5, 'Everyone On Their Best Behavior', goes further into parent guidance territory, focusing on the perils of 'sharenting' [5], and makes an interesting but not altogether convincing suggestion for establishing your child's identity on the web by buying them a domain long before they become famous. Not an awful idea, but it doesn't seem to take into account all the long-term variables and uncertainties. It's hard to argue with the need to stay informed about what a child is *doing* on the Internet, though, or the need to take precautions against in-app marketplaces that may exploit the naïvety of younger people.

Parent-to-parent

Chapter 6 goes further along the same track, going into some detail in a discussion of parental controls, offering generic advice not only on selecting products and services, but also on augmenting technical solutions by interacting with the child. This very much exemplifies the 'parent-to-parent' approach: it may suggest a subjective 'one-size-fits-all' viewpoint, but the reader is, after all, able to make his or her own decision as to which suggestions to adopt, and which to reject. Chapter 7 covers the complex and sensitive topic of cyberbullying, and includes a handful of well-selected, useful resources.

Following a brief concluding section, there are two glossaries: one listing and defining the terms (emoticons, acronyms etc.) used in 'SMS and texts' (I guess the distinction here is between the SMS protocol and the use of 'texting' to describe other types of content covered by MMS), and one consisting of very simplified definitions of various moderately technical terms.

IN SUMMARY

While in some instances these two books cover similar ground, they approach it from different directions. Mustaca's book is wider in scope and sometimes reads a little more technical than was probably intended. Anscombe's parent-to-parent approach is sometimes more about parenting than security (not that there's anything wrong with that) and makes virtually no assumptions about the technical knowledge of the reader, sometimes being almost too simplistic. Nonetheless, both are way ahead of most of the 'lowest common denominator' guides I've seen, and I'd be happy to recommend either or both of them to their target audiences. It seems to me that there is still a need for a reliable but more comprehensive resource, in terms of scope, level of (non-technical) detail, and pointers to other reliable and independent resources. These books, however, are several steps in the right direction.

REFERENCES

[1] Abrams, R.; Harley, D. People Patching: Is User Education Of Any Use At All? AVAR Conference Proceedings, 2008. http://www.welivesecurity.com/media_files/white-papers/People_Patching.pdf.

[2] Willems, E. Cybergevaar. Lannoo, 2013. http://www.cybergevaar.be/.

[3] Mustaca, S. Improve your security: Everything you wanted to know about IT security and didn't know who to ask. https://leanpub.com/Improve_your_security.

[4] Anscombe, T. One parent to another: Managing technology and your teen. http://www.avg.com/ebooks/one-parent-to-another#.UqYiJ_RdUYN.

[5] Sharenting. Urban Dictionary. http://www.urbandictionary.com/define.php?term=Sharenting.