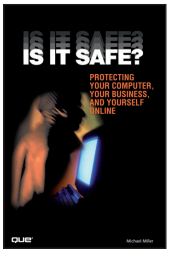
BOOK REVIEW

NEVER MIND HAVING FUN: ARE WE SAFE YET?

David Harley
Eset, UK



Title: Is it safe? Protecting your computer, your business, and yourself online
Publisher: Que
Author: Michael Miller
Cover price: US$24.99
ISBN-13: 978-0789737823

Michael Miller has, apparently, written more than 80 books in 20 years and, according to *Que*, has a reputation for 'clearly explaining technical topics to non-technical readers'. This suggests an author trying to teach the general public the least they need to know about issues they'd rather avoid knowing about at all, which is a laudable aim. When I reviewed another of Miller's books (elsewhere), the chapter on security (in *Vista*, as it happens) wasn't particularly strong and definitely not detailed, so my expectations were not particularly high when I picked up this book. However, Miller has apparently done some serious reading in the security arena since then.

This book is divided into seven parts, dealing respectively with identity theft, data theft, online fraud, email spam and scams, online surveillance, viruses and spyware, and computer hacks and attacks.

Identity theft

Chapter one is a sound summary of various forms of identity theft, while chapter two addresses some of the forms of technical and social engineering attack used to steal the information used as the basis for ID theft and impersonation. Chapter three is a useful, if somewhat US-centric, summary of steps to take and resources to make use of in the event of such a breach.

Data theft

Chapter four moves on to some well-known cases of customer data theft (such as the 2006 *TJX* breach), and touches on some other forms of data theft such as Intellectual Property (IP) and employee data theft. The details of how such attacks work are fairly sketchy, however, chapter five makes some useful suggestions as to how to reduce the risk – e.g. lockdown of laptops, Digital Rights Management (DRM), data encryption, discouraging copying to portable storage devices – without going into detail on the hows and wherefores. Chapter six is a short, but clear statement that could be used as the basis for a high-level corporate policy.

Online fraud

Chapter seven describes (briefly) some forms of online fraud (shopping fraud, auction fraud, *eBay* phishing – although phishing is described in depth later). Chapter eight has suggestions for protecting against shopping fraud that range from vague ('trust your instincts') to not so vague, e.g. safeguarding and hardening passwords. Chapter nine consists largely of a competent summary of the click fraud problem, though this is likely to have fairly limited interest for many everyday users.

Email spam and scams

Chapter ten covers a range of scams, from old-fashioned pyramid and multi-level marketing (MLM) schemes to mule recruitment, by way of stock fraud and 419s. There isn't much detailed analysis, but there are lots of examples. (I wouldn't have minded seeing more consideration of the generic psychological mechanisms here.) Phishing, unsurprisingly, gets a section to itself. Chapter 11 includes a range of rather basic and fallible scam recognition heuristics (misspellings and bad grammar are a pointer, but certainly not definitive!), suggestions for avoidance and remediation, and more about dealing with phishing. Chapter 12 focuses on spamming countermeasures. I'm not altogether happy about the separation of spam and scams ('Spam itself isn't dangerous') since nearly all spam is fraudulent to a greater or lesser extent, but this chapter does provide a summary of avoidance techniques that might be useful to home-users, (although less so to corporate organizations).

Online surveillance

The section on surveillance is the longest in the book. Chapter 13 summarizes many kinds of surveillance, from employee monitoring and government snooping to the activities of online predators. Chapter 14 provides a sound enough summary of the issues around surveillance in the workplace. Chapter 15 is a short, US-centric chapter with a pronounced libertarian flavour. Chapter 16 is largely focused on cookies and anonymous remailers. Chapter 17 deals at some length with cyberstalking, sexual predators and cyber-bullying. It takes seriously a topic that I'm sure is of great concern to many readers: however, given the legal complexities and muddy perceptions of the problems in this area, I'd have liked to have seen some analysis and clarification of some of those issues. Chapter 18 follows up with a discussion of 'tracking your children's online activity'.

Viruses and spyware

Chapter 19 describes various types of malware, from viruses, botnets and rootkits to spyware and rogue

anti-malware. The content is not particularly detailed, but is more accurate than we're used to seeing in general security books, especially those aimed partly or primarily at consumers and end-users. Chapter 20, on defending against viruses, is a little outdated – on the whole, infected attachments are much less of a problem nowadays, despite the occasional dramatic spike. The table of safe and unsafe file types is very short and potentially misleading even if it were safe to assume that file type and filename extension always match (I wouldn't describe PDFs as safe). Still, there isn't much here that's glaringly false. The range of anti-malware solutions listed (though not really described) does at least go further than the usual advice to use something free or one of the big three or four product ranges.

Books and articles that provide advice on recovering from malware tend to make me a little twitchy, as they tend to make large, simplistic assumptions. However, the advice here is fairly sound. The section on avoiding spyware is reasonably thorough and accurate. It's interesting to see null-routing suggested as a preventative measure in a book like this, but the audience will probably not know how to expand on this suggestion enough to make it really useful.

The final section goes back to backdoor attacks and social engineering, but also includes items such as website defacement and brief descriptions of various attacks on infrastructure. For example: DNS spoofing, race conditions, and Denial of Service attacks. Chapter 23 covers defending the home network, but isn't very specific, except about the desirability of using a personal firewall. There is a reasonably thorough summary of wireless security issues, but chapter 24, on defending corporate networks, is likely to benefit only the very rawest of newbie system administrators. Chapter 25, on defending the website, doesn't do much more than enumerate some common attacks, and needs more consideration of countermeasures.

CONCLUSION

I was pleasantly surprised by this book. To find a book that's largely accurate and well-written is rare enough in computing, even more so in the security field. Specialists aren't likely to learn anything dramatically new from it, though some of the brief case histories may prove a useful instant reference. In addition, the range of threats covered means that even the barebones enumeration of issues in many of these chapters could prove to be a useful aide-mémoire: probably more so for corporate managers with only a minimal grounding in security administration. Home-users and even corporate end-users are likely to find the book interesting and useful.