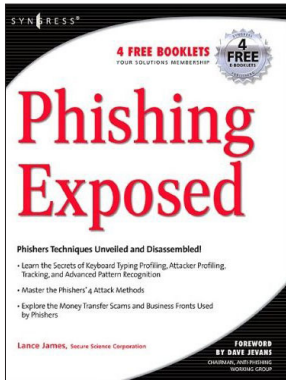


## BOOK REVIEW

### PHISH FINGERING

David Harley

Small Blue-Green World, UK



**Title:** Phishing Exposed

**Author:** Lance James

**Publisher:** Syngress

**ISBN:** 1-59749-030-X

**Cover Price:** \$49.95

There are several things that might put you off about this book. The back cover blurb ('Uncover secrets from the dark side'), the emphasis on attack code and a whiff of breathless, 133tspeak about

some of the prose all tend to grate on the sensibilities of an ageing AV researcher.

However, in this case it is worth looking past the abundance of exclamation marks. *Syngress* seems to prefer to publish books by IT professionals with hands-on expertise, rather than by career authors and journalists. Lance James is a prolific contributor to anti-phishing forums such as the Anti-Phishing Working Group, he represents a security software company that is active in the tracking of phishing groups, and he is certainly a hands-on kind of guy.

#### TARGET AUDIENCE

You shouldn't judge a book by its cover. But the cover may be the only selection criterion available to a prospective buyer. In this case the cover tells us that the reader can, among other things, uncover phishing servers, blind drops and CSS attacks, learn how email addresses are harvested, exploit SSL and 'untangle the intricate web of international money laundering'.

The choice of marketing hooks, the blurb and the foreword all seem to indicate that the book is aimed primarily at those concerned with phishing management at a technical level – particularly programmers, law enforcement professionals, and the security community. So I came to this review with two questions: does the book work for its target audience?, and is anyone else likely to benefit from it?

#### STRUCTURE

Following brief biographies (of the author, technical reviewer and foreword contributor), the author's acknowledgements and contents, the book is introduced by a short and to-the-point foreword by the estimable Joe

Stewart, another well-known name in phisher and botnet hunting circles.

*Phishing Exposed* uses a characteristic *Syngress* chapter format. Each chapter includes a short introduction. Main sections are referred to quaintly as 'solutions', even when they actually describe exploits, and are interspersed with boxed 'tricks of the trade', 'tools and traps' and 'notes from the underground'. There are also copious figures (mostly screenshots).

Each chapter ends with a summary, a 'solutions fast track' consisting of three or four main points, and an oddly named FAQ section. The questions are intended primarily to test comprehension of the preceding material, so probably aren't really asked frequently. However, they do serve as a useful summary of core concepts, and the reader can request from the author answers to specific questions by submitting a form on the *Syngress* website.

Chapter 1 ('Banking on phishing') covers spam classification, cyber-crime evolution, a definition of phishing, and finishes with a section on fraud, forensics and the law.

The section on spam classification doesn't, as you might expect, involve a detailed taxonomy: rather, it starts with a brief note on identifying spammers and gangs, and goes on to say that there are eight top-level spam classifications. Oddly, it lists only four of the top-level spam classifications: unsolicited and non-responsive commercial email (UCE, NCE), list makers and scams. If you already know what a hashbuster is, you probably won't learn much from this, and even neophytes won't learn all they need to know. While we are told that 419s and auction fraud are not phishing, we are not provided with an explanation as to why they are not included in this category.

The content of the next few pages is a generalist look at phishing with some statistical content. A box out and table compare phishing emails and phishing malware – a term used here to refer only to keyloggers. The legal section is focused entirely on the USA, though some of the more general discussion is relevant to all jurisdictions.

#### MORE PHISH TO PHRY

The author seems more comfortable with Chapter 2 ('Go phish!'), which focuses on three types of attack: impersonation, forwarding and popups. Readers of *VB* may be less comfortable with the level of detail provided in the attack descriptions and code, though only the most clueless of script kiddies will find much of this information new. End users who get through this section, on the other hand, will benefit in terms of an understanding of basic phishing mechanisms.

Chapter 3 ('E-mail: the weapon of mass delivery') is divided into sections on email basics, anonymous email, address harvesting, and sending spam. Much of the content is quite general. This could be a useful introduction to spam technology, discussing such issues as header forgery, open relays and proxies, though the general reader's eyes might glaze slightly at the liberal (and largely unexplained) use of regular expressions in command lines. The same reader might, however, benefit from the short descriptions of some spammers' tools and of *Spam Assassin* that follow. SPIM is mentioned in the Fast Track, but not considered in depth.

### POACHERS VS. GAMEKEEPERS

Chapter 4 ('Crossing the phishing line') starts with a fairly high-level description of the Web, dealing with DHTML and HTTP, including a brief note on request methods, one of those topics 'everyone knows about' and no-one ever explains.

The section on misplaced trust looks at the issue of 'consumer misdirection', or the ways in which the marketing departments of banks and other organizations make the phishers' jobs easier by continuing to use long, complex links, 'click here' links, misadvertised links, arbitrary redirects and unpersonalized message text. This section (or at least a summary with less jargon and exploit code) should be used to wrap the sandwiches of many a financial marketroid. CSS attacks are alluded to, but not considered in depth.

On the *SecureScience* website ([www.securescience.com](http://www.securescience.com)), the book is described as a 'view from both sides of the phishing playing field'. It is in Chapter 5 ('The dark side of the web') that the book comes nearest to meeting that description. This chapter considers Dynamic HTML and DOM in depth, and includes information on URL poisoning, filter evasion, SSL misuse, frame attacks and session hijacking.

### YOU MAY GROW UP TO BE A MULE

Chapter 6 ('Malware, money movers, and ma bell mayhem!') starts with a good section on mule recruitment and money laundering. Given the very variable quality of available information on these issues, any general reader might benefit from the information here. The size of the mule recruitment problem is largely underestimated and often goes unmentioned in security books and on informational websites.

James then goes on to consider telephony issues such as Caller ID spoofing and anonymous VoIP, mostly in the context of mule driving. The section on malware is a

reasonably accurate introduction to the subject (at least as far as the past two to three years are concerned), and makes some valid points about changing patterns in malware technology and the consequent difficulties for anti-virus technology.

For Chapter 7, the author was unable to resist the title 'So long, and thanks for all the phish!'. The chapter includes some more US-centric legal observations, a fairly superficial survey of anti-phishing vendors, and some statistical observations.

### DOES THE BOOK KEEP ITS PROMISES?

While the book is more detailed (and accurate) than the average *Dummies Guide*, it doesn't really constitute a complete toolkit either for the skiddie or for the anti-phishing professional. Newbies will come away with more idea of how it all works and what it all means than they had before, but won't be fully equipped for a forensic career.

*Phishing Exposed* is a competent, largely accurate introduction to some of the more technical aspects of phishing. Lance James writes clearly, and has a good reputation in the anti-phishing circles. There are some editing and proofing anomalies which should really have been picked up during the editing process. The industry professionals working directly in this area will not learn a great deal, although non-specialists working in other areas of security may get more out of it.

Businesses targeted by phishing sites will want to look at this book. Phish-management professionals will certainly want a copy, if only to see what people further down the food chain might be reading. Most end users will probably be too intimidated by the technical detail to consider buying it, which is a pity. There is a lot of detail, though most of it takes the form of exhaustive code and historical data rather than copious explanations. However, a general user who is prepared to sift for nuggets could learn a great deal about Internet safety, fraud and email abuse.

The book would benefit from establishing clearer differentiation between old and new threats (the same could be said of many security books). It would also benefit from a glossary and a references/further reading section.

In fact, this could have been one of two very different books: a much more detailed book on the mechanics of phishing and anti-phishing technologies for aspiring specialists, or a short book for the non-specialist, shorn of some of the less useful detail, including some fairly dated attack code. The book that we actually have is not as useful as it might be to either group. Nonetheless, for now it is certainly the best book on the subject to have come my way.