SYNGRESS®

Phishing Exposed

Uncover Secrets from the Dark Side

- A "Must Read" for Programmers, Law Enforcement, and Security Professionals
- Detect and Defend against the Most Sophisticated Phishing Attacks
- Go Behind the Scenes of Highly Organized Phishing Gangs

Lance James, Secure Science Corporation

FOREWORD BY
JOE STEWART
LURHQ, INC.

Register for Free Membership to

solutions@syngress.com

Over the last few years, Syngress has published many best-selling and critically acclaimed books, including Tom Shinder's *Configuring ISA Server 2004*, Brian Caswell and Jay Beale's *Snort 2.1 Intrusion Detection*, and Angela Orebaugh and Gilbert Ramirez's *Ethereal Packet Sniffing*. One of the reasons for the success of these books has been our unique **solutions@syngress.com** program. Through this site, we've been able to provide readers a real time extension to the printed book.

As a registered owner of this book, you will qualify for free access to our members-only solutions@syngress.com program. Once you have registered, you will enjoy several benefits, including:

- Four downloadable e-booklets on topics related to the book. Each booklet is approximately 20-30 pages in Adobe PDF format. They have been selected by our editors from other best-selling Syngress books as providing topic coverage that is directly related to the coverage in this book.
- A comprehensive FAQ page that consolidates all of the key points of this book into an easy-to-search web page, providing you with the concise, easy-to-access data you need to perform your job.
- A "From the Author" Forum that allows the authors of this book to post timely updates and links to related sites, or additional topic coverage that may have been requested by readers.

Just visit us at **www.syngress.com/solutions** and follow the simple registration process. You will need to have this book with you when you register.

Thank you for giving us the opportunity to serve your needs. And be sure to let us know if there is anything else we can do to make your job easier.

SYNGRESS®

Phishing Exposed

Lance James, Secure Science Corporation

FOREWORD BY JOE STEWART

LURHQ, INC.

Syngress Publishing, Inc., the author(s), and any person or firm involved in the writing, editing, or production (collectively "Makers") of this book ("the Work") do not guarantee or warrant the results to be obtained from the Work.

There is no guarantee of any kind, expressed or implied, regarding the Work or its contents. The Work is sold AS IS and WITHOUT WARRANTY. You may have other legal rights, which vary from state to state.

In no event will Makers be liable to you for damages, including any loss of profits, lost savings, or other incidental or consequential damages arising out from the Work or its contents. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

You should always use reasonable care, including backup and other appropriate precautions, when working with computers, networks, data, and files.

Syngress Media®, Syngress®, "Career Advancement Through Skill Enhancement®," "Ask the Author UPDATE®," and "Hack Proofing®," are registered trademarks of Syngress Publishing, Inc. "Syngress: The Definition of a Serious Security Library"™, "Mission Critical™," and "The Only Way to Stop a Hacker is to Think Like One™" are trademarks of Syngress Publishing, Inc. Brands and product names mentioned in this book are trademarks or service marks of their respective companies.

KEY	**SERIAL NUMBER**
001	HJIRTCV764
002	PO9873D5FG
003	829KM8NJH2
004	HJ87623634
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

PUBLISHED BY
Syngress Publishing, Inc.
800 Hingham Street
Rockland, MA 02370

Phishing Exposed

Printed in the United States of America
1 2 3 4 5 6 7 8 9 0
ISBN: 159749030X

Publisher: Andrew Williams
Acquisitions Editor: Jaime Quigley
Technical Reviewer: George Spillman
Cover Designer: Michael Kavish

Page Layout and Art: Patricia Lupien
Copy Editor: Darlene Bordwell
Indexer: Richard Carlson

Distributed by O'Reilly Media, Inc. in the United States and Canada.
For information on rights and translations, contact Matt Pedersen, Director of Sales and Rights, at Syngress Publishing; email matt@syngress.com or fax to 781-681-3585.

Acknowledgments

Syngress would like to acknowledge the following people for their kindness and support in making this book possible.

Syngress books are now distributed in the United States and Canada by O'Reilly Media, Inc.The enthusiasm and work ethic at O'Reilly are incredible, and we would like to thank everyone there for their time and efforts to bring Syngress books to market:Tim O'Reilly, Laura Baldwin, Mark Brokering, Mike Leonard, Donna Selenko, Bonnie Sheehan, Cindy Davis, Grant Kikkert, Opol Matsutaro, Steve Hazelwood, Mark Wilson, Rick Brown, Leslie Becker, Jill Lothrop,Tim Hinton, Kyle Hart, Sara Winge, C. J. Rayhill, Peter Pardo, Leslie Crandell, Regina Aggio, Pascal Honscher, Preston Paull, Susan Thompson, Bruce Stewart, Laura Schmier, Sue Willing, Mark Jacobsen, Betsy Waliszewski, Dawn Mann, Kathryn Barrett,John Chodacki, Rob Bullington, and Aileen Berg.

The incredibly hardworking team at Elsevier Science, including Jonathan Bunkell, Ian Seager, Duncan Enright, David Burton, Rosanna Ramacciotti, Robert Fairbrother, Miguel Sanchez, Klaus Beran, Emma Wyatt, Chris Hossack, Krista Leppiko, Marcel Koppes,Judy Chappell, Radek Janousek, and Chris Reinders for making certain that our vision remains worldwide in scope.

David Buckland, Marie Chieng, Lucy Chong, Leslie Lim, Audrey Gan, Pang Ai Hua,Joseph Chan, and Siti Zuraidah Ahmad of STP Distributors for the enthusiasm with which they receive our books.

David Scott,Tricia Wilden, Marilla Burgess,Annette Scott,Andrew Swaffer, Stephen O'Donoghue, Bec Lowe, Mark Langley, and Anyo Geddes of Woodslane for distributing our books throughout Australia, New Zealand, Papua New Guinea, Fiji, Tonga, Solomon Islands, and the Cook Islands.

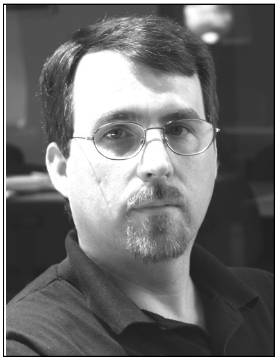
Author

Lance James has been heavily involved with the information security community for the past 10 years. With over a decade of experience with programming, network security, reverse engineering, cryptography design & cryptanalysis, attacking protocols and a detailed expertise in information security, Lance provides consultation to numerous businesses ranging from small start-ups, governments, both national and international, as well as Fortune 500's and America's top financial institutions. He has spent the last three years devising techniques to prevent, track, and detect phishing and online fraud. He is a lead scientist with Dachb0den Laboratories, a well-known Southern California "hacker" think-tank, creator of InvisibleNet, a prominent member of the local 2600 chapter, and the Chief Scientist with Secure Science Corporation, a security software company that is busy tracking over 53 phishing groups. As a regular speaker at numerous security conferences and being a consistent source of information by various news organizations, Lance James is recognized as a major asset in the information security community.

Technical Reviewer

George Spillman currently is a Director for Acadine Informatics, president of the computer consulting group PixelBlip Digital Services and one of the principals behind ToorCon, the highly respected computer security conference that draws in and educates some of the best hackers and security experts from around the globe. As such, he travels well in hacker circles and takes great pleasure in poking and prodding the deep dark underbelly of the internet. George is a frequent guest on television news programs for his expertise and his ability to communicate complex computer security and identity theft issues to non-technical audiences. His consulting clients include representatives from both the Fortune 100 and the Fortune 100,000,000. In the past he has been lured away from consulting by large wheelbarrows of stock options to serve as Director of IT for an international pharmaceutical R&D company, and would most likely do that again if the wheelbarrow was included to sweeten the deal.

Foreword Contributor



Joe Stewart (GGIH) As Senior Security Researcher with LURHQ, Joe researches unusual Internet activity to discover emerging threats, new attack techniques and the latest malicious code. Prior to this role, he was an Intrusion Analyst handling millions of security events for LURHQ clients while monitoring their corporate networks from the Secure Operations Center. He is a SANS Global Information Assurance Certified Incident Handler (GCIH) and has been in the information security field for five years. He is a frequent commentator on security issues for leading media organizations such as *The New York Times*, MSNBC, *Washington Post*, and *USA Today*. Additionally, Joe has published numerous security research papers on Sobig, Migmaf, Sinit, Phatbot and other cyber-threats and attack techniques.

Author Acknowledgements

I would like to take this page to say first and foremost, thank you to my amazing wife. Without her strength and support I would not be where I am today. Thanks for putting up with the @home Lance! I love you. Also, I would like to thank my two children for being themselves. You are truly my upgrades and even though you're all so young, you have taught me many wonderful lessons in life to date. I would like to dedicate this book to my entire family, the support system I could not live without. I love you all. Thanks so much Mom and Dad, you know why!

I would like to send shout-outs to my grandmother-in-law, you have taught me so much more than you'll ever know, and I don't know if I would have made it to the last stretch of becoming a man just right if I hadn't met you. I want to thank my 100 year-old Poppa for hanging in there, and teaching me chess, gardening, and that life doesn't have to be so complicated—at 100 you still play a mean game of chess! I would like to thank Nana (may she rest in peace) for everything, you have a very big place in my heart and I know you're watching out for me up there. I would like to thank my mother-in-law for expecting me to go this far—and I know you know what I mean.

Above all, thank you God for blessing me every single day of my life with the opportunities! Big-ups to you God!

I would like to thank the entire Syngress team for having the patience and understanding of getting me through this book—you guys have been awesome and I look forward to many other Syngress published books with you all, specifically Jaime Quigley and Andrew Williams, thank you. Shout-outs to Dave Stephens, Adrian Younkins (the good always die young!), Dr. Rick Foreman, Kim, Geo, Jake, Josh, H1kari, Tim, and the whole San Diego 2600 crew!

A big thank you to the Anti-Phishing Working Group and the Digital Phishnet members, we'll get there, I promise.

Thanks to Joe Stewart for bailing us out at the last minute.

Anyone I may have forgot please forgive me, but that's always a good reason to talk to me, just to complain that I forgot!

Last, but not least, I would like to say thank you for picking up a copy of this book, as I believe it will be an informative read, and it gave me the opportunity to share some of the experiences I have had with the epidemic of phishing.

Contents

Foreword

In March 2003 one of our secure operations centers received a phishing e-mail that started a chain of events that ends with this page you are reading now. Phishing was almost unknown at the time; in fact, before that time it was generally used only in reference to stealing AOL users' credentials. Tracing that e-mail back to the source machine led us to the discovery that the recently released Sobig virus was facilitating the anonymity of the phishing e-mail we received; a proxy server made it impossible for us to trace the e-mail back any further and find the culprit. These proxy servers made it possible for spammers and phishers to begin a deluge of mail that hasn't stopped increasing to this day.

At the time, no one had made the connection between viruses and spam; viruses were just a nuisance propagated primarily by attention-seeking, smart, antisocial kids. We hoped that publishing a paper on how Sobig was connected to spam (and the phishing e-mail we received) would inspire law enforcement officials to track down the responsible party and introduce the person to some jail time. Instead, Sobig paved the way for what was to come: a plethora of criminal operations that has created an amazing amount of "background noise" on the Internet in terms of time and bandwidth wasted. Moreover, the author of Sobig is still at large, and as far as we know, is still running a spamming operation, even though the flood of Sobig variants stopped in late 2003. What's worse, however, is with each malicious creation, the noise level grows. The problem becomes worse, and other would-be criminals learn from those operations that went before them, adapting and then improving their methods.

Over the past two years, phishing has skyrocketed to staggering proportions. Each technical defensive measure deployed by the network security community and the financial organizations has been met with only an escalation in the complexity and cleverness of the phisher's methods. Even though phishing is nearly a household word these days, most of the general net population doesn't understand exactly how phishers ply their trade so successfully with hardly any risk of being caught. And if complexity weren't bad enough, the different phishing groups display a diverse range of techniques they use. Therefore, learning the specialized tactics of one phishing group isn't necessarily going to bring you any closer to understanding the next one. What is needed is a comprehensive study of the ways phishers operate—that is what I believe we now have with this book.

I've dealt with law enforcement officials working on the phishing problem, as well as individuals in the private industry, and I can say unequivocally that I have never met anyone so "clued" on the problem as Lance James. I can't think of a better qualified person to write this book, and I'm happy that Syngress also saw the need for such a tome. People who are tasked with handling the phishing problem either in their institutions or in terms of law enforcement should have a copy of this book on their shelves and should read it religiously.

Phishing isn't going to be solved by technical measures alone—at some point it has to become too risky for all but the most hardened criminals to operate in this space. And the only way that realistically will happen is when there are arrests occurring regularly all around the globe. I've often said that fighting Internet crime effectively requires a global task force of highly clued people who have a deep understanding of the technical issues involved as well as the authority to kick in doors and seize servers when necessary. Law enforcement is coming up to speed, but it is a slow, painful process to watch, especially as we see the Internet sink further and further into a quagmire of crime committed by those who would make a quick buck at the expense of everyone else. Hopefully, this book will help speed up the process of providing a "clue" to those people who need it and help stop the epidemic of phishing and identity theft that threatens to undermine the trust the public has left in doing business online.

—Joe Stewart
Senior Security Researcher, LURHQ Corporation

Chapter 1

Banking On Phishing

Solutions in this chapter:

- Spam Classification
- Cyber-Crime Evolution
- What Is Phishing?
- Fraud, Forensics, and the Law

☑ Summary

☑ Solutions Fast Track

☑ Frequently Asked Questions

Introduction

During 2004, close to 2 million U.S. citizens had their checking accounts raided by cyber-criminals. With the average reported loss per incident estimated at $1200, total losses were close to $2 billion. The incidence of *phishing e-mails*—e-mails that attempt to steal a consumer's user name and password by imitating e-mail from a legitimate financial institution—has risen 4,000 percent over the past six months. The term *phishing* comes from the fact that cyber-attackers are fishing for data; the *ph* is derived from the sophisticated techniques they employ, to distinguish their activities from the more simplistic *fishing*.

Over the last few years, online banking, including online bill paying, has become very popular as more financial institutions begin to offer free online services. With the increase in online fraud and identity theft, financial crimes have changed from direct attacks to indirect attacks—in other words, rather than robbing a bank at gunpoint, the criminals target the bank's customers. This type of indirect attack significantly impacts the financial institutions themselves because their inability to adequately protect their customer assets tarnishes their reputations and overall trust.

Originally termed *carding* and carried out by *carders*, phishing e-mails are just another form of spam. Universally regarded as an intrusive side effect of our electronic age, spam continues to proliferate at an unbelievable rate each month. According to antispam technology vendor Symantec (Symantec Internet Threat Report, Volume VII, March 2005), 63 percent of the 2.93 billion e-mails filtered by the company's Brightmail AntiSpam software were spam. In mid-July 2004, Brightmail AntiSpam filters blocked 9 million phishing attempts per week, increasing to over 33 million blocked messages per week in December 2004.

Postini, an antispam service provider that provides real-time, online spam statistics, reports that during a 24-hour period in March 2005, 10 out of 12 e-mails were officially classified as spam, and 1 out of 82 messages were infected with a virus.

Since we universally agree that spam is bad, you may ask why it is still one of the fastest-growing industries? The answer is, as long as 1 in 100,000 recipients actually responds to the "Click here" come-on in spammers' e-mails, spammers will find sufficient financial incentive to send out another 5 million spamming messages.

[1] MSNBC, "Survey 2 Million Bank Accounts Robbed," Gartner Group, Anti-Phishing Working Group, June 2004.

Litigation against spammers has been hampered by several factors: tracking the source, identifying the source, and interpreting international laws in attempts to prosecute. Many industry experts believe that the majority of the phishing and spam e-mails originate outside the United States. However, antivirus software provider Sophos has reported that 60 percent of the spam received by its SophosLabs worldwide spam research center in 2004 originated in the United States. According to SophosLabs, over 1200 new viruses were reported during the first two months of 2005—a significant increase over 2004 stats. The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003 could be used to prosecute spammers, but over 60 percent of the spam sent from the United States was sent from computers infected with spam-relay Trojans and worms. These evil tools allow spammers from anywhere in the world to relay their messages through thousands of infected systems without the owners even knowing about it.

Spam Classification

Through the use of classification techniques and forensic data gathering, we can identify specific spam groups. In some cases the identification can include a specific individual; in other cases, groups of e-mails can be positively linked to the same unspecified group. Forensic tools and techniques can allow the identification of group attributes, such as nationality, left- or right-handedness, operating system preferences, and operational habits.

The identification techniques described in this book were developed for spam in general. However, these methods have shown an exceptional ability to identify some subsets of spam, including phishing, the focus of this book.

Spam Organization

There are two key items for identifying individual spammers or specific spam groups: the bulk mailing tool and the spammer's operational habits. People who send spam generally send millions of e-mails at a time. To maintain the high volume of e-mail generation, spammers use bulk-mailing tools. These tools generate unique e-mail headers and e-mail attributes that can be used to distinguish e-mail generated by different mailing tools. Although some bulk-mailing tools do permit randomized header values, field ordering, and the like, the set of items that can be randomized and the random value set are still limited to specific data subsets.