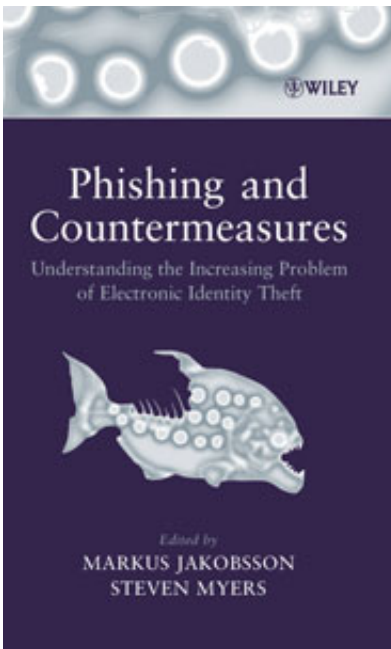


Phishing and pharming and fraud, oh my! Sleuthing the cyber swindlers

November 29 2006



Technology has transformed the Internet into an accessible and speedy superhighway, yet it also has paved slick paths for crooks to prey upon innocent online travelers.

That's the focus of *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft* (John Wiley & Sons Inc.), a new book written and edited by scientists at the Indiana University

School of Informatics. The book -- one of the first of its kind to cover such issues -- explores and explains the sophisticated methods cyber crooks use to steal financial and other personal information from consumers, and conduct corporate and military espionage.

The book describes likely trends in online fraud, and possible countermeasures that can benefit corporations, administrators and developers using the Internet.

The 736-page tome delves into the technology behind phishing, pharming, spam and click-fraud. As the title of the book suggests, the focus is on phishing (using e-mail or instant messages to direct the recipient to a fraudulent Website that appears legitimate), but the coverage goes far beyond the common attacks and countermeasures of today.

"I have been asked by many whether it is ethical to publish a book that may help the bad guys as well as the good guys," said Markus Jakobsson, associate professor, who co-edited the book with Steven Myers, assistant professor. "It's a textbook about cyber crime, its likely trends and what to do to counter it. In many ways the bad guys already have a lead, and it's our goal that *Phishing and Countermeasures* will help level the playing field for the good guys."

Myers said the book draws from a broad range of disciplines, including computer science, human-computer interaction design, psychology and law, and that it reflects the School of Informatics' goal of advancing research on a global scale.

"Apart from describing phishing in North America, the book addresses phishing scenarios in Germany, China and Japan, as well as other types of cyber attacks in those countries," Myers said.

Among the IU contributors to the book are Distinguished Professor of Law Fred Cate, who is internationally known as an expert in privacy issues and the Internet and directs the IU-based Center for Applied Cybersecurity Research; and Peter Finn, professor of psychological and brain sciences and chair of the Institutional Review Board at IU-Bloomington.

External contributors include computer and network security experts Ron Rivest, Massachusetts Institute of Technology; Dan Boneh, Stanford University; and J.D. Tygar, University of California-Berkeley.

"Because there is at least one sucker born every minute, and the Internet puts them all into a huge convenient circus tent, phishing, pharming and other spoofing attacks have risen to the top as the most dangerous computer security risks," said Gary McGraw, chief technology officer of Cigital Inc., and author of *Software Security*.

"The writers and editors of this book go far beyond the basics of problem exposition, covering solutions, legal status and advanced research," McGraw added. "They help Internet users gird themselves for battle against the identity thieves."

Details about *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*, are at phishing-and-countermeasures.info .

More information about anti-phishing research activities at Indiana University is at www.stop-phishing.com .

Source: Indiana University

Citation: Phishing and pharming and fraud, oh my! Sleuthing the cyber swindlers (2006, November 29) retrieved 27 April 2024 from <https://phys.org/news/2006-11-phishing-pharming-fraud-sleuthing-cyber.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.