

The increasing variety and growing sophistication of online threats demand an overwhelming response, says president of IDTheftSecurity.com

(BOSTON, Mass., Aug. 4, 2005 - IDTheftSecurity.com) Threats to computer and data security continue to increase in variety and grow in sophistication. Criminals such as identity thieves and computer hackers employ these tools along with social engineering techniques to lull unsuspecting Web surfers. According to Robert Siciliano, an identity theft expert based in Boston, Mass., the onslaught demands a coordinated, overwhelming response from industry.

“We must respond in a coordinated, overwhelming fashion to the threats presently endangering computers and databases,” said Robert Siciliano, a nationally televised and quoted authority on personal security and identity theft.

Siciliano is author of "The Safety Minute: 01" and an upcoming book, "Identity Theft Pandemic: Curing the Identity Theft Virus." He appeared on CNBC's "The Closing Bell" shortly after data breaches at ChoicePoint Inc. highlighted the problem of identity theft earlier this year.

“Without massive and intelligent retaliation from industry leaders and governments,” Siciliano said, “computer hackers, identity thieves, and the like will have gained the upper hand for a long time to come.”

Cons exploit the trusting sides of victims by using lies and ruses to gain proprietary information. This is “social engineering.” Hackers and identity thieves, technically adept, are adding social engineering to their tactics at an alarming rate. Social engineering is a tool to gain access to sensitive identifying and financial information stored on what may otherwise be properly secure individual and networked computers.

“Remain vigilant even if your computer system or network utilizes the very latest in security,” said Siciliano. “Anybody with nerve who studies sales techniques and psychology can socially engineer others. There is nothing high-tech about it. Social engineering applies tried-and-true, time-tested conning techniques to new circumstances, the information age.”

And the technical threats continue to mount as well. A July 25 press release from Websense, Inc. explores many, such as keyloggers, mobile malicious code (MMC), and others—all of which are increasing in their frequency, according to the release.

The August 2005 issue of *Entrepreneur* looks at another alarming ploy, the pharming technique, which essentially compromises the functioning of a domain name server (DNS). A pharming scam redirects Web surfers who type legitimate organizations' URLs. A user may have no idea she has been rerouted to a con site, which masquerades as the real thing. Those running the fake site typically steal the visitor's personal information.

“We cannot allow pharmerms to get away with taking hacking to a whole new level,” said Siciliano. “Pharming undermines users’ fundamental expectations for the online experience.”

“The response to online threats must be cooperative,” Siciliano continued. “Governments and industries such as banking and software firms should work together to combat the problem as a united front.”

“Stakeholders at all levels,” Siciliano added, “from the software firm’s boardroom to the personal computer user’s living room, need to aggregate threats as they learn of them. Only then will firms and individuals be able to easily obtain and deploy effective blocking software.”

“Companies’ security measures are woefully lacking,” Siciliano continued. “Just watch the news any night. The latest security breach tells you this.”

“The circumstances we find ourselves in could bring down the whole house of cards,” Siciliano concluded. “And a house of cards it truly is. Easy money for computer-savvy thieves abounds.”

###

Siciliano provides consumer education solutions to Fortune 500 companies and their clients. He has been featured on CNN, MSNBC, Fox News, "ABC News with Sam Donaldson," "The Montel Williams Show," "Maury Povich," "Sally Jesse Raphael" and "The Howard Stern Show." Siciliano also leads personal safety and security seminars nationwide.

Siciliano can be reached at 1 (888) SICILIANO (742-4542). The URL www.idtheftsecurity.com leads to his Web site. His blog is available at www.IDTheftSecurity.blogspot.com.

Siciliano's contact information follows:

Robert Siciliano
Personal Security Expert
PHONE: 888-SICILIANO (742-4542)
FAX: 877-2-FAX-NOW (232-9669)
E-MAIL: Robert@IDTheftSecurity.com

The media are encouraged to get in touch with Siciliano directly. They may also contact:

Brent W. Skinner, President
STETrevisions
PHONE: 617-875-4859
FAX: 866-663-6557

E-MAIL: BrentSkinner@STETrevisions.com
URL: www.STETrevisions.biz