

# IM interoperability raises virus threat

30 January 2006



Interoperability of instant-messaging services will allow worms and viruses to propagate more easily, creating more risk in online security, according to Postini's annual Message Management and Threat Report.

The 42-page report, issued by messaging traffic processor Postini, details the types of threats to look for in 2006, as well as the new trends in data security to attempt to minimize those threats.

Among the predicted new security trends, the report said that message encryption will become standard, as companies find new ways to provide easy, policy-based encryption on demand.

The report also predicted an expansion in Internet service provider activity to place limits on the amount of messages subscribers can send out in an attempt to curtail the volume of spam on their networks.

As far as new threats, Postini forecasted the expanded use of images in spam as a substitute for text, to circumvent older text-based spam filters.

"We expect that the growth of more sophisticated and damaging threats, the proliferation of new

communication channels, and the archiving and compliance demands of new policies and regulations will converge in 2006 to produce a 'tidal wave' of demands that threaten to overwhelm messaging administrators and security managers," said Quentin Gallivan, president and chief executive officer of Postini.

Among the report's findings from 2005, small companies received almost 50 spam e-mail messages per day, four times as many as large companies received.

Ron Teixeira, executive director of the National Cyber Security Alliance, said that small businesses are at more of a risk because they simply aren't prepared for cyber threats.

Last week's FBI Cyber Crime Survey "showed that the small-business community doesn't have the resources and the education to put cyber security at the forefront of their priorities," Teixeira said.

It was also found that companies in the publishing and advertising industries received the most spam, averaging 70 and 50 per day respectively. Overall, Postini found spam e-mails to account for between 75 percent and 80 percent of all messages received.

Among spam, e-mails advertising discount drugs and software accounted for 28 percent, just beating out frauds, scams and phishing for most populous spam category. Special offers and pornography rounded out the top four most common types. Combined, those categories accounted for 90 percent of spam.

Postini's report also noted that attacks generated by instant messaging increased by 1,700 from 2004 to 2005. MSN Messenger was the most attacked, accounting for 54 percent of all instant-messaging attacks. AOL accounted for 34 percent.

Paul Kurtz, executive director of the Cyber Security Industry Alliance, said that the best defense from

cyber threats for small businesses is to worry about security from the start and "not have it be an afterthought."

"They need to adjust their thinking on how to protect information systems," Kurtz said.

He suggested companies hire someone to focus on company security, to look after the systems as well as security policy.

Last week's FBI survey found that less than 10 percent of the polled public and private institutions that suffered a computer security incident reported it to law enforcement, a fact that Kurtz found troubling.

"There are good sources to report the crime, and find out what you can do about it," he said, citing the Federal Trade Commission as an example.

Teixeira said there could be various reasons for a business not to report cyber crime.

"Small businesses will always fear the publicity surrounding a security intrusion," he said.

*Copyright 2006 by United Press International*

APA citation: IM interoperability raises virus threat (2006, January 30) retrieved 29 November 2021 from <https://phys.org/news/2006-01-im-interoperability-virus-threat.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.*