

Symantec Online Fraud Protection Helps Businesses Combat Online Fraud, Protect Brand Equity

a comprehensive program that includes Symantec services, education and ongoing monitoring and management capabilities designed to protect businesses that conduct large volumes of financial transactions and their customers from losses due to online fraud.

Mumbai, Maharashtra, May 28, 2008 /[India PRwire](#)/ -- Symantec Corp. (Nasdaq: SYMC) today announced the availability of Symantec Online Fraud Protection, a comprehensive program that includes Symantec services, education and ongoing monitoring and management capabilities designed to protect businesses that conduct large volumes of financial transactions and their customers from losses due to online fraud. This offering helps businesses shield their customers from a variety of online threats, including phishing and pharming. By helping their customers safely conduct transactions online, businesses can boost customer loyalty, minimize financial loss and legal exposure, and reduce risks to their corporate brand.

Corporate brand erosion as a result of online fraud is a significant problem facing all organizations that conduct business online. Symantec's most recent Internet Security Threat Report, Volume XIII released in April 2008 indicates that threats from online fraud continue to plague both enterprise organizations and consumers. In the last six months of 2007, Symantec observed more than 85,000 phishing hosts – computers that can host one or more phishing Web sites – an increase of 167 percent from the first half of 2007.

Leveraging Symantec's broad footprint and position as a leader in security, Symantec Online Fraud Protection is a flexible program that combines a variety of offerings based on customer need. This offering is also backed by Symantec's Global Intelligence Network which provides the most comprehensive view of Internet attack activity based on security intelligence data gathered from around the world. Symantec's Global Intelligence Network includes 11 security response centers that analyze data from more than 2 million email accounts, 120 million systems and more than 40,000 devices in more than 200 countries. Symantec Online Fraud Protection includes:

- **Phishing Monitoring:** Watches for new phishing attacks and other attacks on the client's brand.
- **Transaction Monitoring:** Reviews transactions on back-end systems and blocks fraudulent activities.
- **Online Fraud Incident Response and Countermeasures:** Provides rapid response to attacks in order to minimize losses and protect brand reputation, including working with ISPs to curtail the activities of fraudsters.
- **Malware Intelligence and Analysis:** Provides monitoring of malware targeting a specific brand and analysis of new malware behavior.
- **Consumer Education and Protection:** Helps organizations educate and protect their end-user customers from online threats and minimize the risk of fraud.
- **Expert Resident:** The offering also includes an expert resident from Symantec, with access to a variety of security intelligence data sources, who works with in-house staff to provide security expertise and serve as the primary point of contact leading all online fraud protection efforts.

"Symantec's recent Internet Security Threat Report shows that 80 percent of brands targeted by phishing attacks were in the financial sector," said Anil Chakravarthy, senior vice president, worldwide, Enterprise Services, Symantec. "As online fraud continues to increase, Symantec is arming its customers with tools to protect against the brand erosion that can result from an attack. With Symantec's superior malware intelligence and analysis, monitoring and incident response services, customers can quickly respond to online fraud attacks, leverage expert command and control during incidents, and shift their approach to online fraud from reactive to proactive."

Symantec Online Fraud Protection provides a unique combination of products, services and education, leveraging Symantec's unparalleled scope and breadth of expertise in the security market. Symantec Global Services is a leader in providing expertise and resources for securing and managing the world's information. With more than 4,000 professionals worldwide, Symantec Global Services has worked with 99 percent of the Fortune 1,000.

Pricing and Availability

Symantec Online Fraud Protection is available in all regions globally. Pricing is based on the number of brands protected, the number of online users and the degree of onsite support required. For more information, visit [Symantec Online Fraud Protection](#).

Notes to Editor

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com

Supporting Relevant Industry Statistics and Research:

Information on phishing and social networking - specific to India - from Symantec's latest Internet Security Threat Report (ISTR), Volume XIII: Phishing was a major cause of concern in the Indian security threat landscape. In the last six months of 2007, Symantec observed 345 unique phishing URLs with IP addresses hosted in India. Symantec also observed more than 400 unique phishing attacks on reputable Indian banks. Out of these, some of the attacks involved the use of compromised '.gov' servers to launch phishing attacks on other brands.

According to the report, majority of phished Web sites that were detected globally during this reporting period spoofed social networking sites. This is a sign of caution for India too, since according to a recent industry report nearly 5-6 million Indians are actively involved in social networking and spend approximately 25-75 percent of their time online in social networking activities. They can become easy preys to 'abuse of trust' tactics. According to the Symantec report:

- Social networking sites are easy for criminals to spoof and because social networking pages are generally trusted by users, phishing attacks mimicking them may be more successful.
- Profiles on social networking sites often contain a significant amount of personal information about the user.
- Spoofed social networking pages can include links to false download that require users to enter confidential information such as authentication information or credit card information that can subsequently be used for fraudulent purposes.

NOTE TO EDITORS: If you would like additional information on Symantec Corporation and its products, please visit the Symantec News Room at <http://www.symantec.com/news>. All prices noted are in U.S. dollars and are valid only in the United States.

CONTACT:

Sagar Desai, Symantec India +91-98909 48706 sagar_desai@symantec.com
Melissa D'mello, 20:20 MEDIA, 98670 43485, melissa.dmello@2020india.com

Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

For more information, please contact:

David Vaz
MANAGER MEDIA RELATIONS
(L) 9322652611