

## KEY BENEFITS

### Highest accuracy on phishing emails

Cloudmark's unique anti-phishing technology, coupled with the largest up-to-date threat database, ensures the highest accuracy on phishing attacks.

### Rapid response

Within moments of the first phishing sighting, Cloudmark propagates protection to all of its solutions, across its global network.

### Premium positioning for premium protection

Gain a competitive advantage, reduce churn, increase customer loyalty and maintain market leadership with the most effective phishing solution available.

### Automated response

The phishing detection-protection process is fully automated to offer 24x7 protection for the user.

## Cloudmark Anti-phishing Data Service Cloudmark Anti-phishing Engine

Cloudmark Collaborative Security Network™ provides the most effective, real-time, comprehensive phishing protection.

Phishing is a rapidly growing problem for service providers, enterprises and consumers. Phishers use social engineering tactics to send emails and pose as legitimate institutions requesting sensitive information from their customers. Phishing has eroded consumer confidence in conducting business over the Internet through diminished vendor credibility and subsequent brand erosion. Restored confidence is critical to the continued growth of e-commerce and e-banking, and to reduce churn by increasing confidence in service provider networks as consumers seek refuge with providers perceived to offer greater protection from personal threat.

A recent study by the Anti-Phishing Working Group (APWG) uncovered 9,765 phishing sites during the month of January, 2006, more than a 200% increase from levels just two months prior of 4,630. Attacks are becoming more sophisticated and are increasingly targeting service providers and e-commerce vendors as phishers look for convenient and less traceable ways to cash out.

Phishing differs from spam in that it is generated by a criminal element intent on stealing personal data for financial gain. Attacks are highly sophisticated, targeted, transient and dynamic, making it far more difficult to uncover and capture the perpetrators. Traditional methods of capturing spam do not work for phishing threats.

Phishers move very quickly. The Cloudmark Collaborative Security Network (CCSN) combines real-time live reporting with fully automated data collection, analysis and update cycles to ensure the fastest possible response time to phishing attacks.

Cloudmark offers two distinctive solutions to combat phishing and fraud:

### CLOUDMARK ANTI-PHISHING DATA SERVICE

An automated service that scans fraudulent email collected by the Cloudmark Collaborative Security Network (CCSN) and extracts the phishing URLs, using the collaborative reputation system to confirm that the URL is in actuality a phishing site and not a legitimate URL. The system collects live reports from millions of people around the world to provide real-time information about new attacks.

As soon as a URL has been confirmed as a phishing site, it is added to the phishing data feed that is obtained over HTTP as batches of URLs. Because phishing attacks are short-lived, these feeds include only those URLs that are live; URLs that have not been seen by CCSN for five days are automatically removed from the feed.

### CLOUDMARK ANTI-PHISHING ENGINE

An automated engine that is installed as part of a service provider's messaging infrastructure to provide filtering protection at the messaging gateway from fraudulent email. It scans each message and computes a set of fingerprints on the message, a process that is automatic, very lightweight and highly scalable for the large volumes of email typically seen by service providers. This approach combined to the data service provides a far more effective solution as the fingerprinting algorithms will analyze the structure of messages sent by phishers and block new attacks in advance of receiving URL reports.

The set of known phishing fingerprints is updated in real time and new fingerprints from the CCSN are available within moments of a new attack being identified.



### Cloudmark is a recognized spam and phishing protection industry leader

Cloudmark sponsors and leads industry standards organizations such as the Anti-Phishing Working Group, MAAWG and the Financial Services Technology Consortium. Cloudmark Gateway Edition is currently deployed in leading Service Provider environments worldwide.

### *Unmatched phishing intelligence*

Only Cloudmark has real-time data on phishing attacks through its fully automated data collection, analysis and update cycle.

### *Zero-hour/real-time phishing protection*

Phishing attacks are short-lived, often only occurring for a few hours before disappearing. In the most effective and intelligent combination of technology and human discretion, Cloudmark's massive installed base of human messaging-abuse reporters in the CCSN instantly responds to immediately stop phishing scams.

### *Blocks attacks while they are in progress*

Cloudmark blocks attacks while they are still in progress, unlike other vendors who employ static systems that cannot respond to the velocity of today's attacks.

### *Reputation-based*

Cloudmark's phishing architecture is modeled as a social solution to a social problem. It uses global, corroborated reputation to prevent the system from being poisoned by untrusted feedback. This ensures that only real phishing emails are being blocked.

### *Self-organizing*

The Cloudmark phishing service dynamically responds to a rapidly evolving model of good vs. bad, powered by the world's largest network of real-time users.

### *Self-correcting*

Within moments of the launch of a new phishing attack, phishing messages begin to be blocked. Conversely, if the system mistakenly begins blocking real emails, the CCSN will begin unblocking those emails and, within moments, the entire network will stop blocking those emails.

### *Low total cost of ownership*

Cloudmark's phishing engine is a maintenance-free solution that does not require IT administrator training or set up, freeing up valuable resources.

### *Maximum performance*

Cloudmark's phishing solutions require minimum overhead and integrate seamlessly into a network operator's messaging infrastructure.

*"Both eBay and PayPal have worked hard to build a community where its customers can make safe transactions. They partnered ... and can now deliver a system that not only protects customers from fraud before it reaches them, but goes a step further to protect their brand by ensuring the message is really from PayPal. ... the hope is that other e-commerce companies and financial institutions will follow suit."*

*— Howard Schmidt  
Chief Security Officer, eBay;  
Former Cyber Security Czar, White House;  
Former Chief Security Officer, Microsoft Corp.*

For more information visit us at  
[www.cloudmark.com](http://www.cloudmark.com)  
128 King Street, 2nd Floor  
San Francisco, CA 94107 USA  
Ph: +1.415.543.1220  
Fax: +1.415.543.1233

