Phishing Attacks Diminish the Trust in Internet Channels

Online fraud scams continue to grow by 15% per quarter, targeting financial institutions of all sizes as well as e-commerce venues. Phishing attacks are growing in sophistication and often occur in sudden rashes over a several month period, unexpectedly hitting both large and small businesses. According to a leading industry analyst, the direct cost to the financial industry alone was nearly $2.8 billion in 2006. A more troubling consequence is the impact on consumer confidence in conducting financial transactions online. According to a recent Wall Street Journal/Harris Interactive poll, 24% of consumers limit their online banking due to threats such as identity theft. Financial institutions and e-commerce companies must aggressively combat these scams to avoid erosion of customer trust and protect online channel viability.

Five Tiers to Protect Consumers

MarkMonitor offers the industry’s most comprehensive AntiPhishing Solution. A multi-tiered security approach protects online consumers with several lines of defense that prevent them from reaching fraudulent sites. The solution is offered as a managed service, enabling companies to minimize operational costs and leverage the expertise of MarkMonitor’s antiphishing analysts, systems, and vast fraud data sets. MarkMonitor’s approach is the only industry solution with a focus on prevention rather than reactive measures. Financial customers can meet FFIEC and OCC guidelines for safeguarding customers with Antiphishing Solutions from MarkMonitor.

Features

- Detection of potential phish sites before they go live
- Real-time fraud detection, warning and blocking at the browser level
- World’s largest Fraud Broadcasting Network through major email and browser partners
- Dilution to render any information collected useless
- Global site shutdown services with a track record of disabling thousands of sites
- US-based 24x7 Security Operations Center (SOC) staffed with accessible and responsive antiphishing experts
- Customer portal for monitoring the status and investigating the details of phishing attacks

Benefits

- Multi-tiered system incorporates fraud prevention as well as reactive measures
- Fraud is prevented at the consumer desktop, drastically reducing the impact of any scam
- Regulatory compliance with consumer safeguard requirements may be achieved
- Higher online channel adoption rates and increased consumer confidence in conducting online transactions reduces overall marketing and operations costs
- Reduced fraud risk results in lower direct losses
- Leveraging MarkMonitor’s 24x7 SOC enables staff to focus on more strategic initiatives
First Tier of Defense: Pre-Attack Monitoring
MarkMonitor’s predictive Early Warning System™ uncovers potential phish sites before they become operational, thereby notifying customers in advance of an attack and allowing them to take appropriate action. Identity Tracker™ allows the client to investigate other attacks that may be launched by the same fraudster, sometimes before the phishing attacks have been initiated. Together, these tools provide customers early intelligence on potential threats.

Second Tier of Defense: ‘Zero Hour’ Protection
Consumers can be instantly prevented from visiting confirmed fraudulent Web sites, and warned about highly suspicious sites, with Trust Guard™, a small client-side application that applies real-time Web site heuristics for detection with proven 97% accuracy. Fraud intelligence from MarkMonitor’s world-class Security Operations Center (SOC) is continually broadcast to Trust Guard, providing the most up-to-date and comprehensive information on known phishing attacks. Real-time detection of suspect fraudulent sites is automatically fed back to the SOC for immediate analysis and verification by MarkMonitor’s antiphishing experts. This continuous intelligence feedback loop provides the most comprehensive and timely protection against Internet fraud available today.

Third Tier of Defense: 24x7 Detection and Email/Browser Blocking
Consumers are further protected when major ISPs block their access to thousands of fraudulent sites detected by MarkMonitor and delivered via MarkMonitor’s Fraud Broadcasting Network. The SOC administers 24x7 threat research and analysis of more than 16 million suspicious URLs and emails daily, detecting and verifying 15,000 phish attacks around the world each month. Customer abuse inboxes are also closely monitored. Blacklisted fraudulent sites are continually broadcast to the major ISPs for near real-time blocking of phishing emails. Confirmed phishing sites are also broadcast to leading browser toolbars. These efforts cover hundreds of millions of Internet users worldwide.

Fourth Tier of Defense: Dilution™
MarkMonitor dilutes the quality of any data received by phishers with an effective counterattack. False data is submitted to the fraudster’s Web server to effectively render useless any identity information collected during the scam. Several Dilution options are available.

Fifth Tier of Defense: Site Shutdown
MarkMonitor’s SOC leverages established protocols, procedures and relationships with ISPs to shut down fraudulent sites around the world, reducing the average uptime of a phish Web site from several days to typically less than 3 hours. To date, MarkMonitor has successfully shut down thousands of phish Web sites operating in more than 60 countries.

With a multi-layered approach, financial institutions and e-commerce companies can more effectively protect their customers from online identity theft. MarkMonitor’s AntiPhishing Solutions provide the industry’s most comprehensive, layered security solution for detecting, responding and preventing consumer access to online fraudulent attacks.

MarkMonitor Security Operations Center

- 24x7x365 antiphishing protection
- Highly-trained and experienced antiphishing experts
- Multilingual support for over 20 languages in 60 countries
- Relationships with major ISPs and domain registrars worldwide
- Confirmation and shutdown of thousands of phish sites monthly