



Identity Theft Attack Management

Identity Theft Attack Management Services

- Phishing, Vishing, SMSing Detection and Mitigation
- Malware Detection, Analysis and Mitigation
- Abuse Box Forwarding
- Secure interface for incident management
- Web-based phishing attack simulation for employee and customer education
- URL & DNS blocking

Identity Theft occurs when a user claims to be a legitimate entity in an attempt to scam private information. Cost to the enterprise includes financial losses by individual customers and loss of trust in the organization. According to Gartner Research, identity theft attacks increased 40% in 2009, and increasingly are targeting employees of companies and even their executives.

Identity theft includes: Phishing; the use of email scams. Vishing; the use of telephone and Voiceover IP (VOIP) scams, and SMSing which are SMS based Scams – and ever more sophisticated attempts by criminals to avoid detection. Pharming – the act of spoofing a legitimate website by compromising its legitimate DNS server. In addition to the above, there is the potential of scams including Malware. Malware is software designed to infiltrate or damage a computer system without the owner’s consent.

Best-in-class detection: BrandProtect continuously publishes thousands of email addresses in high-risk online environments to attract as many identity theft schemes as possible. As a result, our servers are inundated with emails every second of the day. Each time a new email is received our software conducts an automated analysis to determine the brand exposed and type of attack. Once a threat detected, our team is able to analyze it, including the re-engineering of Malware, to determine the level of threat that it poses and then transfers it to our Incident Response Team which is able to eliminate the threat.

Superior Mitigation: Our Incident Response Teams are based worldwide, with the assistance of more than 3500 Internet service providers, covering more than 90% of the web, have a perfect (100%) takedown record and have among the fastest takedown times in the industry.

A Multi-Pronged approach: Gartner Research advocates combining phishing e-mail blocking, safe browser surfing features, the use of site authentication, the detection of phishing attacks and the takedown of such attacks. They also stress the need for continued education of customers and employees.

BrandProtect’s Identity Theft Attack Management solution incorporates the following:

- A rapid response service to deal with all forms of identity theft attacks;
- Best in class detection practices including 24x7 response to abuse mail from customers;
- Support for employee and customer education: Incident response guidelines and simulated attack education;
- Browser plugins to help protect against attacks from fraudulent websites;
- Secure Portal with incident data details, trending and reporting capability;
- URL and DNS blocking
- Access to best practices from BrandProtect client base and partner community.

