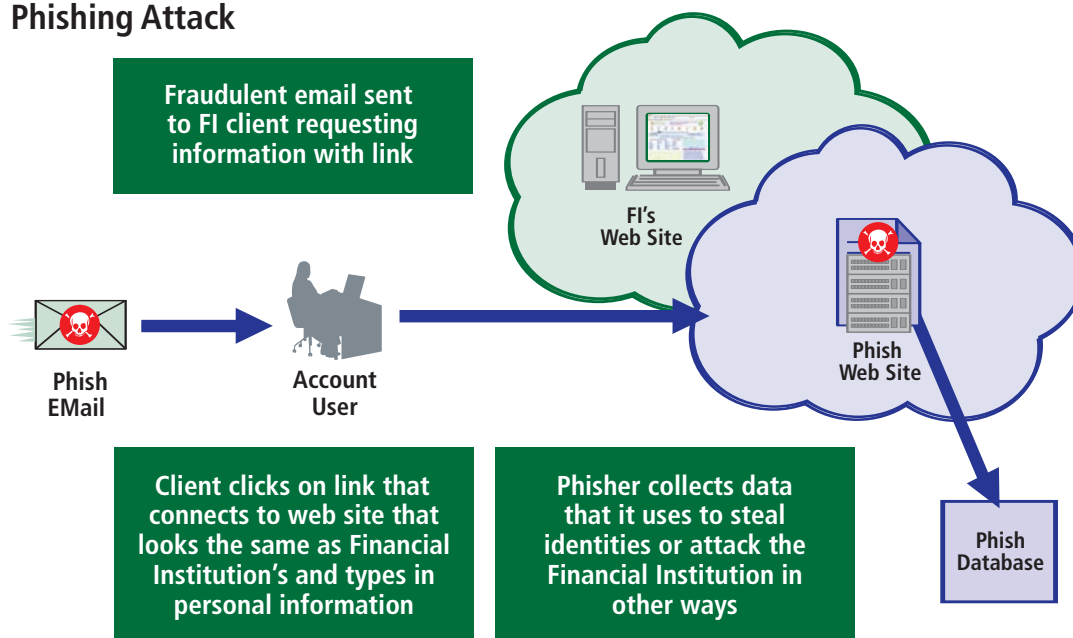


# CounterPhish<sup>SM</sup> Phishing Incident Response Service

## Service Overview

The corporate identity of any institution is fundamental to conducting business online. Your company name, logo, trademark and brand are valuable assets that drive revenues, establish trust and protect the customer experience. Phishing has become a popular and growing method of identity theft primarily through the creation of a web site that appears to represent a legitimate company. According to the Federal Trade Commission, identity theft through phishing attacks now affects more than 10 million people per year representing an annual cost to the economy of \$50 billion with ~\$50,000 in damages per incident for a financial institution. The Anti-Phishing Working Group reports that the frequency of these phishing attacks increases 24% every month and the research firm, Gartner, estimates that U.S. businesses lose an estimated \$2 billion a year as their clients become victims of phishing attacks. The growing trend of phishing attacks, and the inability of traditional security technologies to prevent these attacks, leaves many organizations vulnerable to substantial losses. Perimeter's CounterPhish<sup>SM</sup> Phishing Incident Response Service provides our clients with the ability to identify phishing attacks and eliminate false web sites quickly.

## Phishing Attack

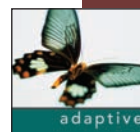


## Service Highlights

Perimeter deploys a well-defined incident management process that employees of clients can easily follow. The service includes escalation to CERT and other authorities and operates on a 24/7 basis in the U.S. and from three international locations. Phishing attacks on weekends and in 15 languages can be addressed, and the service averages a 3-hour take-down time for phishing sites in contrast to a nearly 6-day industry average. The service is priced and delivered with a small monthly fee plus a per incident charge, and the client does not need additional hardware, software or in-house technical expertise.

## Key Features & Benefits

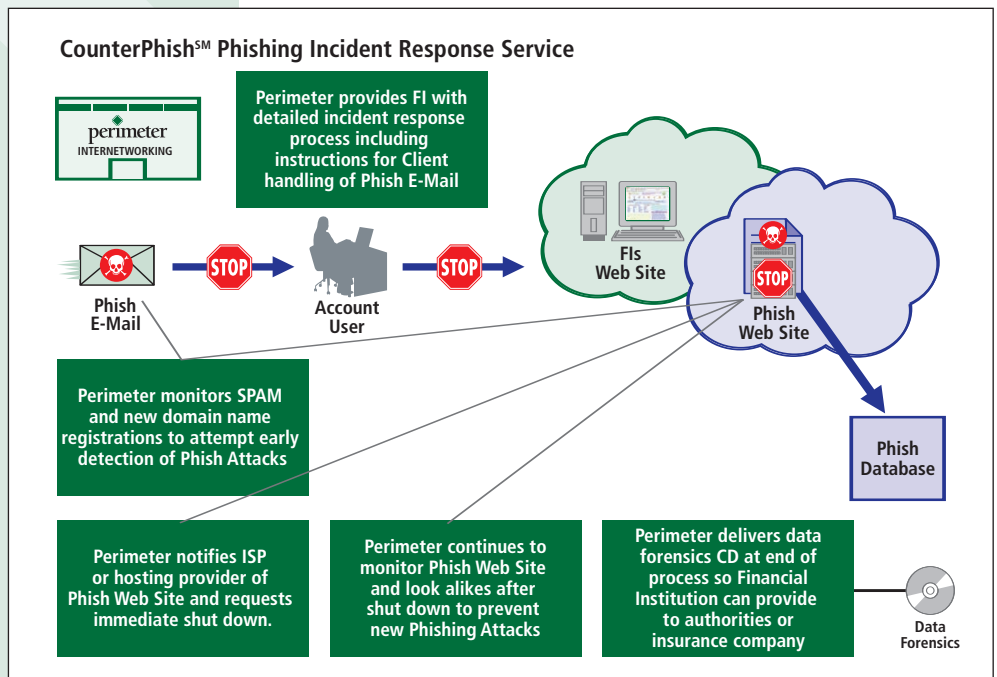
Feature	Benefit
Detailed process documentation.	Step-by-step instructions on what to do when a phishing attack has been launched including instructions for Account Users who report a phishy email
DNS monitoring	DNS servers monitored for newly-registered DNS names similar to that of the financial institution client.
Average 3-hour elapsed time to take down	Phishing site is quickly shut down mitigating damage to financial institution's client information and reputation.



## CounterPhish<sup>SM</sup> Phishing Incident Response Service

Small and medium-sized financial institutions exhibit several significant problems associated with responding to phishing attacks:

- Inability to respond on a 24x7 basis
- Insufficient technical expertise and lack of technology tools
- Inability to collect complete data forensic information
- Authority barriers that prevent escalation



## Technical Overview

CounterPhish<sup>SM</sup> will monitor the Internet for early signs of a phishing attack. Verification that a phishing attack is underway is quickly completed and notification, if necessary, is provided. The attack is traced, the ISP or hosting provider of the site and domain name services is contacted, and the site is shut down. Once the "false" site has been successfully shut down, the client will be notified, and the site will be monitored for changes continuously for 30 days. Once the case is closed, the collected information will be compiled including all of the data forensic information from the phishing attack. This information will be sent to the financial institution to forward it on to authorities and/or keep it for insurance purposes.

Perimeter's CounterPhish Incident Response Service is powered by Brandimensions. Perimeter reserves the right to change service benefits and features at any time.

