Anti-Phishing Incident Response Service

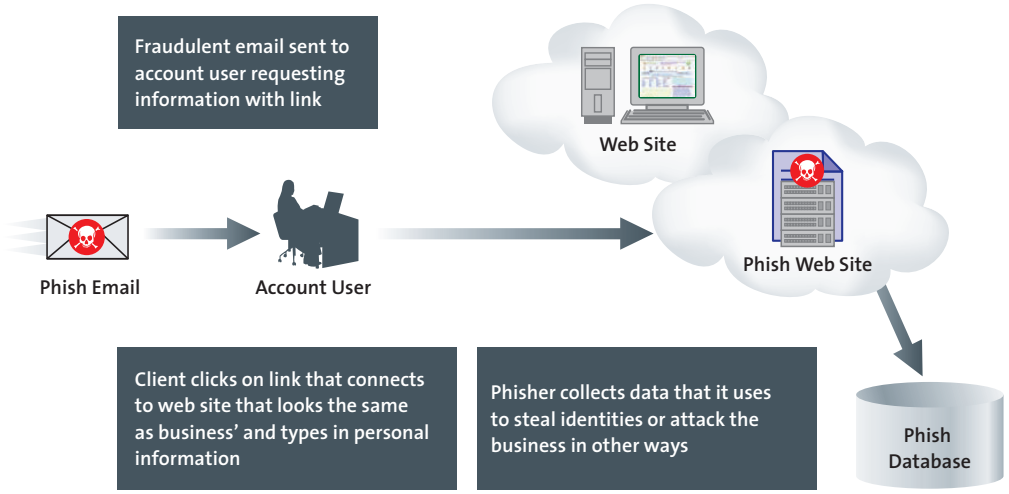
THE PROBLEM OVERVIEW:

- Inability of organizations to respond on a 24 x 7 basis
- Insufficient technical expertise and lack of technology tools
- Inability to collect complete forensic information
- Poor ability to escalate due to authority barriers

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 approximately $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℠ Phishing Incident Response Service provides our clients with the ability to identify phishing attacks and eliminate false web sites quickly.

PHISHING ATTACK



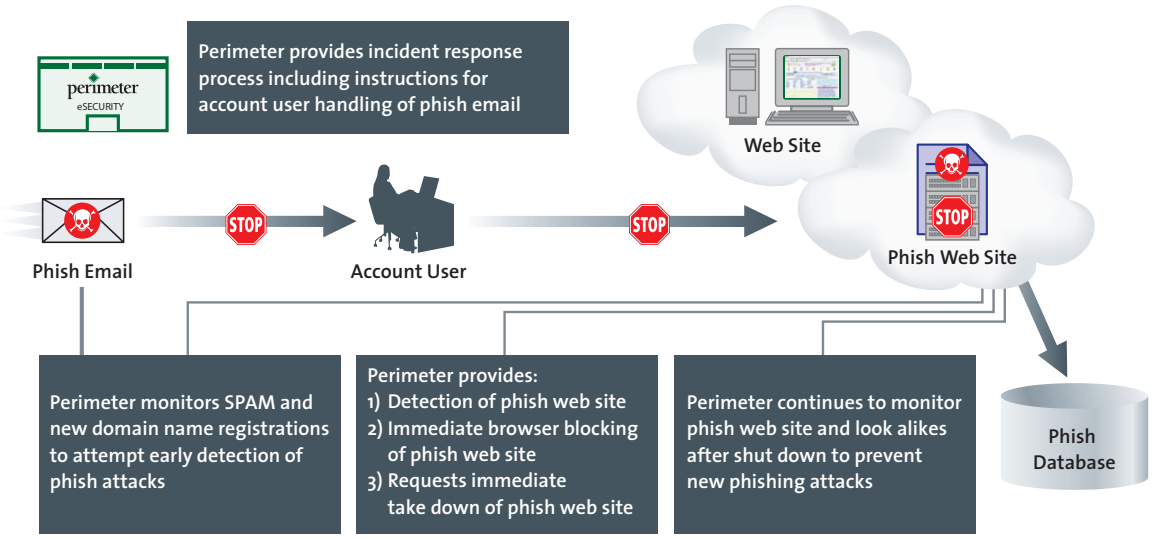
perimeter eSecurity™

Complete. On Demand. Affordable.

perimeter eSecurity™

Complete. On Demand. Affordable.

COUNTERPHISH℠ PHISHING INCIDENT RESPONSE SERVICE



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 multiple languages can be addressed, and the service averages take downs in less than 12 hours from time of validation. 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.

TECHNICAL OVERVIEW

CounterPhish℠ 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.

Key Features	Benefits
Detection	Early detection of phishing attacks mitigates reputational damage. Perimeter detects phishing attacks on a 24x7 basis through real time detection and a client portal that allows the customer to report a phishing attack.
Immediate Browser Blocking	IE 7.0 and Firefox 2.0 browser users enjoy an additional level of protection against identity theft. Databases at major search engines are updated to reflect the phished site and these URLs are blocked before your customer has a chance to click on it.
Site Take-down	On a 24x7 basis, fraudulent web sites can be validated and taken down on a timely basis protecting account user's personal information. The service provides a user portal for the client to submit their own take down URLs. These URLs are then monitored to make sure that they do not reappear.