Pharming Shield

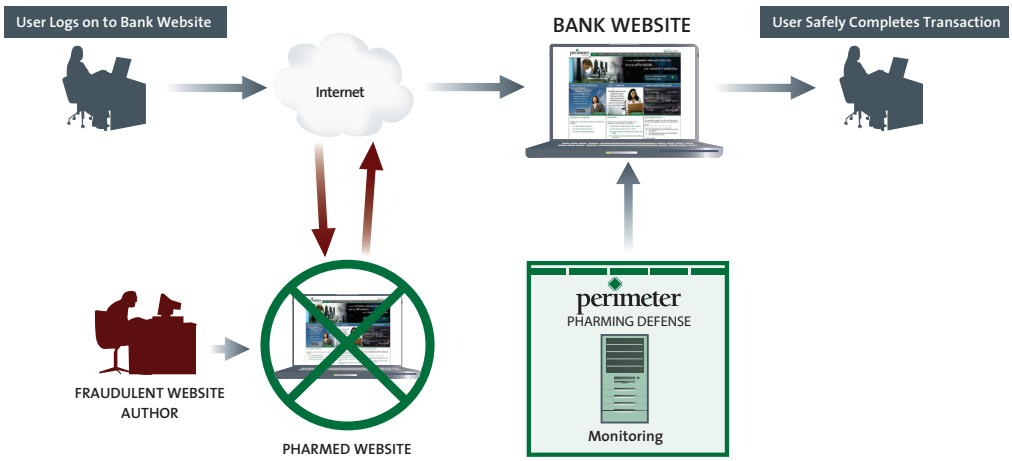
Advanced Web Site Protection

THE PROBLEM OVERVIEW

- Customers are asked to verify their personal and account information, and are redirected to a site that has been designed to look identical to yours. Because they trust you, they provide the requested information
- Organizations that are unable to validate changes to their web site have to deal with the impact to their customers and the negative publicity associated with it
- Many organizations aren't alerted that their site is being pharmed in time to alert and protect their customers
- Many organizations have no way to show their examiners and IT committee that their pharming defense solution is compliant

Pharming is one of the fastest-growing forms of identity theft on the Internet - and one of the hardest to defend against. In a pharming attack, a hacker has three ways that they can compromise your web site. They can insert malicious code or make an exact copy of your web site and capture customer user names and passwords as users try to access their account. They may also hijack your DNS and redirect traffic to their site or hijack your SSL certificate and redirect just the SSL portion to their site. In all of these situations an unsuspecting user enters ID, password and other confidential information which the hacker will "pharm" for illegal purposes. This is alarming because it usually goes undetected, both by the company and the user, until well after the damage has been done. These attacks can become both a liability and a reputation issue.

Perimeter's Pharming Shield continuously monitors your organization's web site for availability and code or page changes while verifying that your DNS and SSL certificate(s) have not been compromised. Real-time alerting and comprehensive reporting protects your online reputation. This is especially important if you are outsourcing to an independent third party, where validating an SLA can be challenging. Our solution continuously monitors your site for all varieties of pharming attacks every two minutes, 24 hours a day x 365 days a year.



perimeter eSecurity™

Complete. On Demand. Affordable.

perimeter eSecurity™

Complete. On Demand. Affordable.

THE PERIMETER SOLUTION

Perimeter's Anti-Pharming Service quickly detects a pharming attack so that a remedy can be initiated before any significant harm takes place. The service includes a DNS monitor, an SSL certificate monitor and a web defacement monitor that work together to insure the integrity of a web site and web transactions. This real-time service is non-intrusive, easy to install, and provides instant notification of attacks.

THE BENEFITS OF PERIMETER'S SOLUTION

Key Features	Benefits
Real Time Alert Notification	Our web of geographically-distributed sensors continuously monitors your web site and tests accuracy every two minutes
Secure Web Portal Reporting	Easily accessible compliance reporting with executive summaries to share with your IT committee and examiners
Web Page Performance Monitor	Performance security tests go beyond your web page, making sure it's running safely and optimally through quick diagnosis and correction of security and performance issues before they become incidents
Web Page Defacement Monitor	Validation that no unauthorized changes are made to your web page
SSL Certificate Monitor	We compare your SSL certificate to the one being used every 2 minutes, from multiple locations across the Internet
DNS Monitoring	Your DNS is monitored every two minutes to verify that your DNS has not been compromised.