



SecureWorks



Anti-Phishing Services

Service benefits

- Respond quickly and decisively to attacks
- Provide timely communications to your customers to keep them informed
- Minimize the impact on your business
- Protect employees and customers

Expert anti-phishing assistance

Phishing attacks, in which electronic thieves deceive people into revealing account information in order to steal, are complex in nature, and attack methods are evolving rapidly. Phishing is not only a threat to consumers but also to the businesses these consumers trust. A phishing attack can lead to consumers losing confidence in their financial institutions and ecommerce vendors, resulting in lost sales, unwanted publicity, increased costs and, potentially, even legal action.

Dell SecureWorks® helps protect financial institutions and other organizations vulnerable to phishing attacks. When organizations are attacked, they often lack the processes, knowledge and dedicated resources to respond quickly and effectively. Phishers know to attack after hours and on weekends – when you are least able to respond. Twenty-four hours a day, 365 days a year, Dell SecureWorks provides the tools and expertise to restore your customers' confidence and turn the tables on the attackers.

Dell SecureWorks provides several services to help organizations prepare for and respond to phishing attacks.

Phishing incident preparation

Phishing incident response planning

When an attack hits, response time is critical. Having an incident handling plan in hand when that time comes is very important. The incident handling plan provides a blueprint for responding to phishing incidents. It contains procedures, processes, responsibilities and points of contact in a manageable, logical sequence consistent with your culture and business model.

This plan will reflect the roles, responsibilities and process for communicating time-sensitive, phishing-related information. The plan will cover both IT and business support functions, pinpointing key personnel in IT, legal, marketing, human resources and other departments, and describing their roles and information requirements in resolving and understanding phishing security incidents.

Phishing incident response

Incident analysis and response

In order to ensure the fastest response time by experienced security personnel, Dell SecureWorks' security professionals are available 24 hours a day, 7 days a week, 365 days a year to begin incident response. Within 30 minutes of notification, Dell SecureWorks' security analysts will begin responding to the phishing incident. The team will start by gaining as much forensic information as possible about the "who, what, where and when" of the incident.

Techniques include:

- Networking analysis: traceroute, DNS lookups, ARIN searches, OS fingerprinting, scanning, system enumeration, foot-printing, etc.
- Application analysis: website code reviews, email analysis, server configuration, etc.
- Research: IRC, USENET, websites
- Propagation methodologies and magnitudes
- Severity assessment
- Log review: Web logs, server logs, firewall logs, etc.

Interim reporting

Dell SecureWorks will provide interim reports to keep key personnel and other involved parties apprised of the response.

Countermeasures and coordination

Working with your company, Dell SecureWorks will recommend, coordinate, manage and facilitate an appropriate selection of countermeasures. These countermeasures will be selected and deployed dependent on the evolving analysis of the particular incident underway.

Dell SecureWorks has a wide range of response capabilities. Our diverse staff has foreign language translation capabilities that cover a large majority of all phishing incidents. Our security expertise has led to close, ongoing relationships with key anti-phishing and security organizations including FIRST (the Forum of Incident Response and Security Teams), the United States FBI and Secret Service, CERT (Computer Emergency Readiness Team), and APWG (Anti-Phishing Working Group). We also work with local and foreign ISPs, foreign law enforcement and vendors.

Post-incident analysis and management report

After a major incident has been handled, Dell SecureWorks will review and document how effective the incident handling process was and work to identify needed improvements to existing security controls and practices. Dell SecureWorks will produce a post-incident report with a jargon-free executive summary that discusses the impact on your organization, your business, your customers and compliance requirements. The report will also be supported by detailed screen shots, code snippets and other forensic information necessary for review by your regulators and auditors. Information will be accumulated from all of these reviews and be used to identify systemic security and control weaknesses, and potential deficiencies in phishing countermeasures.

