



## **Barracuda Networks Anti-Spoofing Solution**

---

With the advent of phishing schemes and other unsavory techniques for obtaining information and account access from unsuspecting victims, the importance of solutions that prevent local email addresses from being impersonated has grown significantly.

There are now many examples of emails that have been sent to large and small organizations under the guise of impersonating someone inside the organization. These often successful attempts to “phish” or obtain confidential or security-related information have grown drastically over the last year. These attempts include schemes to convince unsuspecting users to volunteer their account information and passwords.

With most phishing schemes, the “From” portion of the email envelope is “spoofed” or forged. For example, someone from outside an organization sends an email to a user inside the organization that appears to be from another internal user. This technique has been used to prey upon new employees who receive emails that appear to be from the organization’s IT department and often request that the new employee visit a Web site and re-enter their account name and password. If the recipient of the email replies or follows the directions in the email message text, the password and account information is passed to the phisher. The network then becomes vulnerable to attack by the impersonator outside the organization. This technique has even been used to compromise the security of systems using RSA-based dynamic ID systems. Many companies have been specifically preyed upon by targeted efforts to obtain specific access or confidential information. The problem is very serious.

Recent highly publicized phishing scams, including one perpetrated against AOL users in April, have demonstrated just how sophisticated phishing schemes can be. As reported by the Anti-Phishing Working Group (<http://www.antiphishing.org/>), in the AOL incident, victims received emails from a spoofed AOL email address (service@aol.com), which led them to believe that the email was coming from a legitimate internal AOL source, when in fact the email was coming from an impersonator. The email indicated that the user’s credit card information for their account had expired and requested that the user go to a specific URL included in the email to restore their account access. The fake URL and corresponding Web site was designed to look very similar to a real AOL Web page, displaying the same color scheme and logos. Those users that fell for the scheme were asked to provide confidential information including credit card, bank account and social security information. All of this information was collected by the perpetrators and used for criminal purposes.

In less publicized, but still common schemes, organizations fall prey to phishers sending spoofed emails that appear to come from the victim’s colleague with a message appearing to regard official business matters (i.e., “Hello! Per our discussion, attached is the outline of tomorrow’s meeting agenda”). While the message seems harmless, the attachment often carries Trojans or viruses that could harm the network if opened.

The Barracuda Networks Spam Firewall Family of solutions incorporates anti-spoofing features that, when enabled, will not allow an external email to appear as if it came from someone inside the organization. Any email that would have this appearance would be

blocked. With the Barracuda Spam Firewall, this anti-spoofing feature can be enabled and disabled on a domain-by-domain basis. The Barracuda Spam Firewall includes features that allow larger organizations to specify a list of IP addresses that are allowed to have a "From" address that appears from inside the organization to support multiple sites and multiple email servers.

There is one problem with effectively implementing an anti-spoofing solution: road warrior access. Users that work outside of the network from home or on the road must connect via methods other than standard SMTP such as VPN, SSL-VPN, or Web mail if they want to send email to their colleagues in the organization and have that email appear as if it came from their internal email account. This can be a drawback; however, the consequences of a phishing scheme for an organization are so severe that many large and small organizations are choosing the safer route and implementing comprehensive anti-spoofing solutions. This results in a minor inconvenience when someone who is a member of the company and is traveling wants to send email internally.

The Barracuda Spam Firewall incorporates a comprehensive anti-spoofing solution that is suitable for both large and small organizations. All organizations should enable this feature to avoid impersonators' attempts to access their network and obtain critical and confidential information.

###