

Phishing Protection Business Briefing

Protect personal data by blocking fraudulent emails

"Phishing" is a technique used by online criminals to steal passwords or other account information from internet users. The term is sometimes said to stand for *password harvesting fishing*. Analyst firm Gartner estimates that phishing cost banks and credit card companies \$1.2 billion in direct losses in 2004, and that 1.4 million computer users have suffered identity theft from these activities.¹

Phishers usually work by sending out [spam e-mail](#) to large numbers of potential victims. Typically, a phishing email will appear to come from a trustworthy company and contain a subject and message intended to alarm the recipient into taking action. A common approach is to tell the recipient that their account has been de-activated due to a problem and inform them that they must take action to re-activate their account. The user is provided with a convenient link in the same email that takes the email recipient to a fake webpage appearing to be that of a trustworthy company. Once at that page, the user enters his personal information which is then captured by the fraudster².

Phishing Protection in Astaro Security Linux

Astaro's security technology, as incorporated in the *Astaro Security Linux* software and in the *Astaro Security Gateway* appliances, employs a server-side or gateway approach to blocking phishing. Placed at the point where the Internet connects to your organization's network, it is simple to manage and provides full protection of Web and Email traffic by blocking fraudulent and suspicious links and filtering spam.

Astaro provides protection from phishing attacks by a combination of different protection mechanisms:

- The virus scanner scans every email and determines some emails as phishing emails from their signature and blocks them
- All phishing emails contain a link to a fraudulent site. With surf protection enabled it is possible to block all links that are categorized as "suspicious" or are uncategorized. So even if a user is tricked by a phishing email the link will be blocked when the user tries to access it.
- The Realtime Blackhole List (RBL) contains all known IP-addresses of phishing email senders. Emails which are sent by known phishing senders are blocked.

An Improvement Over Desktop Approaches

Desktop anti-spam software and anti-virus software can detect some phishing emails when they are downloaded to the client. Also, anti-phishing toolbars for browsers are available that check the URLs typed into the browser's address bar against special databases to determine if a URL is a known phishing site. However, it is almost impossible for any administrator to check and maintain every single client. Also, these approaches only protect the user from phishing emails that have already been identified – they don't protect from new or unknown phishing messages.

Astaro's combination of gateway technologies protects personal data from both known and new phishing attacks with a minimum of administrative effort.

¹ Gartner: *Phishing Victims Likely Will Suffer Identity Theft Fraud*, May 14, 2004.

² <http://en.wikipedia.org/wiki/Phishing>