

Phishing - An Enterprise Threat

What is Phishing?

Phishing has come to be synonymous with one of the fastest growing crimes on the Internet, and by all indications, it will only get to be more treacherous. Also known as carding or spoofing, phishing is a form of identity theft that uses technical subterfuge and social engineering to deceive users into divulging sensitive personal information such as usernames, passwords, account IDs, ATM PINs, credit card details and social security numbers through electronic communication.

The term phishing arises from the use of increasingly sophisticated lures to "fish" for users' financial information and passwords.¹

Phishing Casting its net

The Anti-Phishing Working Group (APWG) provides the most comprehensive picture of the scale of email-based phishing attacks on the internet. There were 14,135 new unique phishing reports identified in July 2005. While 71 brands were targeted, six brands accounted for 80 per cent of phishing campaigns.²

Studies by the APWG have concluded that phishers are likely to succeed with as much as 5 percent of all message recipients.

In a phishing attack, the fraudster starts by sending emails to a large number of users. The email seems to come from a legitimate establishment with an urgent call for action on the user's behalf. A typical example would be that of informing the users that their account with the company would be suspended or terminated if it is not updated within the stipulated time period.

Such email messages also provide the URL links for the users to update their credentials. However, the URL is a sham and redirects the users to a phony website designed to look like the real one.

The information filled in by the naïve users on this bogus website is directly routed to the phishers. Once this data is acquired, the fraudsters may use the person's details to create fake accounts in the victim's name, ruin the victim's credit or even prevent the victim from accessing his or her own accounts. The following email message is reproduced as an example which targets the account holders of eBay.

Phishing An Enterprise Threat

Since phishing emails seek an individual's personal or financial information, most IT professionals view phishing as a consumer centric issue rather than as a threat to their organization. But phishing has rapidly moved into the enterprise threat domain with phishing mails installing spyware into the user's computer when the phishing links which come in the form of spam mails are clicked on. The originator now has access to the enterprise network, putting enterprise information confidentiality and the network itself at risk.

The damage caused by phishing is extensive, particularly in a corporate environment where the economic repercussions can be enormous such as -

- Identity theft
- Loss of confidential user data
- Loss of productivity
- Use of corporate network resources: bandwidth abuse, mail flooding, etc.
- Tarnishing the consumer's trust in the brand

Protection against phishing, particularly at the corporate level, should be a top priority for ensuring comprehensive security.

Cyberoam Phishing Protection

Cyberoam, with its unified threat management capabilities, takes a blended approach to tackling phishing threats to enterprises.

Blocks Site Access

Spyware Blocker provides comprehensive protection against spyware entry - which can be a precursor to phishing attacks - into the enterprise as well as detection of existing spyware. Cyberoam's content filtering and firewall prevent inbound and outbound traffic to sites like P2P and others that are spyware carriers. WebCat - Cyberoam site database - has a constantly updated Phishing and Fraud category with comprehensive listing of such sites, ensuring reliable access prevention. The category is updated through a series of measures that ensure comprehensive listing.

Prevents Spam Entry


Cyberoam's pre-integrated Anti-Spam marks the phishing mails as spam with policy-based action of quarantine, tag and deletion options. This stops most of the phishing mail from reaching enterprise users. In addition, Cyberoam blocks or limits access to hotmail, yahoo and other webmails, reducing the entry of phishing attacks through them.

Phishing is a particularly deceptive and destructive online threat. While consumers are the most obvious victims, the damage spreads far wider - hurting companies' finances and reputation and potentially undermining consumer confidence in the safety of e-commerce. Enterprises must thus educate their employees of phishing threats, preventing them from unconsciously creating a backdoor ingress into the network in addition to installing phishing prevention solutions.

Through its blended approach, using its existing features like Spyware Blocker, content filtering, firewall and anti-spam solutions, Cyberoam delivers dependable protection against phishing attacks with no extra cost involved for this security.

Sources

1. wikipedia.org
2. Anti-Phishing Working Group



Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply

Copyright © 1995-2005 eBay Inc. All Rights Reserved.

Figure : Phishing email targeted at eBay account holders.