



# SpamStopsHere Identifies New Spear Phishing Spam Email Attacks Targeting eBay Sellers

SpamStopsHere, January 03, 2006

URL: <http://www.pr9.net/comp/internet/3357january.html>

*Greenview Data, Inc., the industry leading provider of SpamStopsHere email security solutions, announced today that a new wave of spear phishing attacks are targeting eBay sellers.*

PR9.NET January 03, 2006 - Ann Arbor, MI, Greenview Data, Inc., the industry leading provider of SpamStopsHere email security solutions, announced today that a new wave of spear phishing attacks are targeting eBay sellers.

Cyber criminals are targeting eBay members selling items on the World's Largest Marketplace by sending forged auction inquiries from what appears to be eBay's "Question from eBay Member" message portal. Account holders are prompted to respond to the inquiry by clicking the "Respond Now" link button in the email, and are then directed to a fraudulent eBay login screen. After the seller has entered their login information, cyber-criminals then "hijack" the seller's account and steal their identity.

Spear phishing is the latest spam technique used by cyber-criminals to gain access to personal and corporate accounts and steal sensitive data. Unlike traditional phishing attacks in which millions of emails are sent indiscriminately, spear phishing attacks are extremely targeted and focus on one end user or organization at a time. Spear phishing emails are designed to appear as if they are sent from a trusted individual, and typically ask for login IDs and passwords.

"Just about anyone with an email account has undoubtedly seen an eBay phishing scam email at one time or another," said Ted Green, CEO of SpamStopsHere. "We are seeing an evolution in phishing and spear phishing attacks. The sophistication of attacks is constantly increasing. Cyber criminals are relentless in developing new and ingenious methods of monetary and identity theft. End user education is the best defense against spear phishing attacks."

www.SpamStopsHere.com recommends the following guidelines when confronted with any suspected phishing attack:

1. If an email asks you to log into your bank, PayPal, eBay or other personal account, assume it is a phishing scam.

**DO NOT UNDER ANY CIRCUMSTANCE CLICK ON THE LINK IN THE EMAIL**

2. Never enter banking information, social security numbers or other sensitive information by clicking a link in an email.

3. Never enter your computer user name or password into an email that requests it, not even if it claims to be from your IT manager or other co-worker. It is easy for a spammer to forge the sender's name.

4. If you are unsure as to the legitimacy of a particular email, open an Internet browser and manually type in the URL of the institution in question, e.g. "www.chase.com". Do not use the URL in the email as a reference, as it may be a forgery.

5. Treat any email that asks for sensitive data as a phishing scam.

###

## About SpamStopsHere

About Greenview Data:

Greenview Data, Inc. has been providing its critically acclaimed SpamStopsHere network security solutions to clients across the globe since 2002. Greenview Data also created and developed the powerful VEDIT™ text editor, which has been licensed to over 150,000 users since 1980. EBCDIC to ASCII conversion makes up the third division of Greenview Data, providing conversion solutions through turn-key contracting and consulting. Through the growth of its SpamStopsHere hosted service, and exciting R&D projects, Greenview Data, Inc. is looking to the future and another successful 25 years. Greenview Data is headquartered in Ann Arbor, Michigan.

**Website:** <http://www.spamstopshere.com>