

IT BackbonesTM

Security News



**INTERNET CONTENT
RATING ASSOCIATION**

An independent, non-profit organization
whose mission is to protect children
from potentially harmful material

The IT Shield - Dedicated To IT Security Issues, Featuring News, Press Releases, IT Directory & Links

- [Home](#)
- [About](#)
- [Contact](#)
- [Submit PR](#)
- [Search News](#)
- [What We Can Offer You](#)
- [IT Events](#)
- [Time & Money](#)

Ohio Bank Phishing Scam Offers New Security Mechanism!

Published 12th June 2006

Security experts at MicroWorld Technologies inform that a new Ohio Bank Phishing mail in circulation tells users that the bank is introducing a new online security mechanism for which they need the confirmation from account holders.

The mail tells users that due to recent fraudulent activities on some of the bank's accounts, Ohio bank is introducing a new security mechanism to make banking safer for its users. The bank would require to check the validity and genuineness of the account holder and it directs to click on a link to do so.

Once you click on this link, it takes you to a page that looks like an authentic Ohio Bank webpage in every sense, complete with active links and menu that connect you the original webpages of the bank. At the middle of the page, there's link that tells you to click on it, in order to verify the account information.

Now you are taken to the true face of the scam. The brazen form asks you to put in your User ID, Password, Card Number, Expiry Date and ATM PIN! Well, this scamster does not believe in stealing a few items and running away. Rather, he would go the whole hog and empty the coffer! To add to its credibility, there's a bold VeriSign logo staring at you from the middle of the webpage.

Phishing is the form of online Identity Theft using fake emails and spoof websites of reputed banks, Credit Card Companies, Online Stores, ISPs and every thing else that

has a name and credibility attached to it. The hi-tech scam has claimed countless victims around the world already. With increased awareness among computer users about Phishing, one section of phishers has already moved on to DNS redirecting Trojans or a method other wise called as Pharming. The other, more traditional group, is still relying on smarter Social Engineering schemes like the one we have just observed.

“Phishing started off with mails posing as a routine account authentication procedure from the bank,” explained Govind Rammurthy, CEO, MicroWorld Technologies. “Soon it moved on to scarier ones which told users that their accounts have witnessed suspicious activity and if they don’t verify the information, the accounts will be suspended. Then came mails that offered free tickets and coupons, which just required users to complete a small verification procedure. Now for the last few months a large number of scams like the one in question, are posing as security alerts and Phishing awareness campaigns themselves. At MicroWorld we call it Upside-down Innovation!”

“We need to see Phishing and Pharming in the broader spectrum of increasing online crimes with well-defined financial motives. You’ve got criminals hacking into large e-commerce websites, launching Denial of Service Attacks, conspiring international copyright infringements and extortion threats. All these indicate that cyber gangs are after the money of anyone who is directly or indirectly connected to the World Wide Web. The scenario positively underlines the need to secure your online interactions like never before!” said Govind Rammurthy.

Company Profiles powered by ITReseller.com

- MicroWorld - [View profile](#)

[Links](#) | [About Us](#) | [Privacy Policy](#) | [Contact Us](#) | © 2004-2006 IT Backbones Limited

Site developed and hosted by [Design Solution](#) Ltd.