



SPI DYNAMICS
secure. protect. inspect.

FREE Product Trial
Protect Your Web Applications from
ATTACK

- ABOUT US
- CONTACT
- ADVERTISE

Welcome to a new version of Help Net Security. Much has improved and more is on the way. [Subscribe to our RSS feeds and stay updated!](#)


NEWS	ARTICLES	SOFTWARE	VULNERABILITIES	EVENTS	NEWSLETTER	E-MAIL ALERTS	SEARCH	RSS
HOME	Off The Wire Security World Virus Center	Latest Articles Reviews Interviews Book Chapters	Windows Linux Mac OS X Pocket PC	Vendor Advisories Vulnerability Database	Webcasts Conferences	Subscribe Current Issue Archive		

OFF THE WIRE **SECURITY WORLD**


- [Dining out on the ID card fiasco](#) • [Automate Linux installation and recovery with SystemImager](#) • [The RFID hacking underground](#) • [CIA defends unaccountable snooping](#) • [How to get through having your identity stolen](#) • [Consumers shun backups, study says](#) • [The eternal value of privacy](#)
- [This week's new Linux security software releases](#) • [Bizarre Chase bank scam poses as phishing alert](#) • ["Pay Per Click" fraud botnet discovered](#) • [Secure Computing Announces SafeWord PremierAccess](#) • [Infosecurity Europe - the largest in the world](#)


LATEST ARTICLES **VIRUS CENTER**

- [Help Net Security Podcast: Episode 1 - Nortel's Approach To Security](#) • [How Companies Can Manage Strong Authentication Intelligently](#) • [Cross-Site Scripting Worms and Viruses: The Impending Threat and the Best Defense](#) • [Identity Theft - Should You Be Worried?](#) • [Automated Patch Management](#)
- [Virus Leaks Power Plant Secrets Twice In Four Months](#) • [Rootkit backdoor targets poker gamers](#) • ['Dialer.ay' rings In trouble for Internet users](#) • [Hoots-A Worm Preys On Network Printers](#) • [Weekly Report on Viruses and Intruders - Naload.CW Trojan and MS06-18, MS06-19 and MS06-20 Microsoft Vulnerabilities](#)

 SECURITY SOFTWARE


[++ GFI LANguard Network Security Scanner 7](#) • [++ Acunetix Web Vulnerability Scanner 3.0](#) • [WinSCP 3.8.1](#) • [JSch 0.1.28](#) • [GFI Endpoint Security 3](#) • [WinDeveloper IMF Tune 2.8](#) • [VisualRoute 2006 10.0i](#) • [Password Safe 3.0 beta 1](#) • [SSL-Explorer 0.1.16](#) • [Reason 0.5.1](#) • [Tor 0.1.0.17](#) • [Digital Invisible Ink Toolkit 1.4](#)
[Nagios 2.3](#) • [MaraDNS 1.2.07.3](#) • [The Sleuth Kit 2.04](#) • [Autopsy Forensic Browser 2.07](#) • [Sussen 0.21](#) • [KisKis 0.19](#) • [John the Ripper 1.7.1](#) • [yaSSL 1.3.0](#)
[Distributed Access Control System 1.4.12](#) • [MailScanner 4.53.6-1](#) • [Vuurmuur 0.5.71](#) • [Ethereal 0.99.0](#)
[KisMAC 0.21a](#) • [iStumbler 96](#) • [Fugu 1.2.0](#) • [Little Snitch 1.2.2](#) • [Victor 2.0](#) • [Net Tool Box 3.1](#) • [PDFKey Pro 1.0](#) • [HenWen 2.1.2](#) • [Mac GPG 1.4.1](#) • [IPSecuritas 2.1](#) • [Pastor 1.7](#) • [JellyfiSSH 4.2](#)
[WiFiFoFum 2.1.1](#) • [Crippin 2.8](#) • [AirFix 1.0b](#) • [Aircanner Mobile Encrypter 2.5](#) • [Confidential Notes 1.1](#) • [Aircanner Mobile Firewall 2.4](#) • [WiFi Graph 0.3](#)
[RC3](#) • [SignWise Pro 2.52](#) • [Sentry 2020 2.8](#) • [eWallet 4.0](#) • [Pocket Warrior 15022003-B](#) • [Touch Password Protection 2.3](#)

 ADVISORIES

 VULNERABILITIES

[Mandriva Linux Security Update Advisory - kernel \(MDKSA-2006:086\)](#) • [Debian Security Advisory - awstats \(DSA 1058-1\)](#) • [Ubuntu Security Notice - quagga vulnerabilities \(USN-284-1\)](#) • [Ubuntu Security Notice - mysql-dfsg vulnerability \(USN-274-2\)](#) • [Debian Security Advisory - phpldapadmin \(DSA 1057-1\)](#) • [Debian Security Advisory - webcalendar \(DSA 1056-1\)](#)
[Azboard list.asp Multiple Variable SQL Injection](#) • [Azboard admin_ok.asp Multiple Variable SQL Injection](#) • [Confixx Pro ftplogin/ login Variable XSS](#) • [DeluxeBB misc.php name Variable SQL Injection](#) • [RadLance Gold popup.php read Variable Traversal Arbitrary File Access](#) • [Squirrelcart cart_content.php cart_isp_root Variable Remote File Inclusion](#)

GFI: [Catch hackers red-handed with LANguard Security Event Log Monitor. Download free trial!](#)

Bizarre Chase bank scam poses as phishing alert Posted on 19 May 2006.

In one of the most bizarre phishing scams to date, this fake Chase email on the prowl warns users of ongoing phishing schemes, explains many modes of online frauds that are out to con them and finally directs to click on a link to report fraudulent emails. What opens up is a form that asks to put in their account details so they can move on to report any scam!

Security experts at [MicroWorld Technologies](#) inform that this mail spoofing Chase Bank is quite an upside-down innovation in recent phishing baits. If used in targeted groups, this can potentially compromise personal financial information of a good number of account holders.

The mail starts off like this- We want you to be aware of e-mail scams that attempt to steal your personal and/or account information. Known as "phishing", these scams consist of an email that looks like it came from Chase (Complete with Chase logo) and usually takes an urgent and demanding tone. It is not our practice to send -and you should never respond or reply to- email that: Requires you enter personal information directly into email or submit some other way. Threatens to close or suspend your account if you do not take immediate action by providing personal information.....

One must say it's written quite convincingly! Now, the mail moves on to directing you to a link to report any fraudulent mail and takes it from there.

"This mail is a masterpiece design from scam artists!" says Govind Rammurthy, CEO, MicroWorld Technologies. "Over the last few years, we have been deeply

analyzing the psychological ploys in various Social Engineering schemes employed by fraudster gangs and I must say, there have been quite a number of clever ideas. But this one definitely takes the cake. It's like hijacking your senses smoothly and completely, to force you to do something really stupid before you know what happened!"

Earlier this month, MicroWorld Technologies had reported another phishing attempt on American Express card holders using an advanced Trojan, where a pop-up box appears when you manually type in the American Express web address in your browser. The Chase fraud is technically inferior, but scores high when it comes to convincing powers with the cleverly conceived con mail.

"The line between the real and fake is blurring so fast. When you go and type in the URL of your bank's website in your PC, there's no guarantee that it will take you to the authentic one anymore. In a world of keyloggers, URL Rerouting Trojans and very smart con mails like the one we have just seen, you need a three tier defense against cyber criminals. One, a powerful Spam Control. Two, total Phishing control. Three, a Proactive and Real-Time protection against all kinds of malware," asserts Govind Rammurthy.

[[Security World main page](#)]

Activeworkx
SECURITY CENTER

Click For
FREE Trial

Offers Out-of-the-Box
Compliance Reports
to Help Meet SOX and
HIPAA requirements



CrossTec
Corporation

GFiLANguard
Network Security Scanner

**DOWNLOAD FREE
VERSION TODAY!**

Secure
Your
Business.



infosecurity
CANADA

June 19-21, 2006
Metro Toronto Convention Centre
Toronto, Ontario