



FIND SQL INJECTION, XSS & OTHER WEB VULNERABILITIES

[Articles](#)[News](#)[Reviews](#)[Releases](#)[Downloads](#)[Contact Us](#)[White Papers](#)**Sponsors:**

Is your network open to attack? Find out with the #1 sold network security scanner: GFI LANguard Network Security Scanner! [Download your FREE trial version today.](#)

Check your website security with a FREE [website security audit](#) by [Acunetix](#). Audit your web applications for [SQL injection](#), [cross site scripting](#) & more with [Acunetix Web Vulnerability Scanner](#)

Software security section is sponsored by GFI, a leading developer of network security, content security and messaging software - [Free trial!](#)

Chase Bank Scam Poses As Phishing Alert*Friday, 19 May 2006 08:03 EST*

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 quiet 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.

News

['Pay Per Click' fraud botnet discovered](#)

May 19, 2006, 09:05 EST

[Chase Bank Scam Poses As Phishing Alert](#)

May 19, 2006, 08:03 EST

[How does the UPnP flaw works](#)

May 19, 2006, 07:56 EST

[3 Key Computer Security Tools for 2006](#)

May 19, 2006, 07:54 EST

[The RFID Hacking Underground](#)

May 19, 2006, 04:49 EST

[Get Through Having Your Identity Stolen](#)

May 19, 2006, 04:47 EST

[Protect yourself from deceptive Web sites and malicious hyperlinks](#)

May 18, 2006, 15:06 EST



