



DEMAND PCI COMPLIANCE



Learn More ▶

- Flash Demo
- Free Trial
- Whitepaper

- ABOUT US
- CONTACT
- ADVERTISE

[Grab our main RSS feed and stay updated with fresh security news](#)

NEWS

- [Off The Wire](#)
- [Security](#)
- [World](#)
- [Virus Center](#)

ARTICLES

- [Latest Articles](#)
- [Reviews](#)
- [Interviews](#)
- [Book Chapters](#)

SOFTWARE

- [Windows Linux](#)
- [Mac OS X](#)
- [Pocket PC](#)

VULNERABILITIES

- [Vendor Advisories](#)
- [Vulnerability Database](#)

EVENTS

- [Webcasts](#)
- [Conferences](#)

NEWSLETTER

- [Subscribe Current](#)
- [Issue Archive](#)

HOME

E-MAIL ALERTS

SEARCH

RSS

OFF THE WIRE SECURITY WORLD

- [U.S. to expand domestic use of spy satellites](#)
- [New URI browser flaws worse than first thought](#)
- [Russia throws out net piracy case](#)
- [Hardening your systems with Bastille Linux](#)
- [How to set up Apache virtual hosting](#)
- [Microsoft reacts to kernel hacks, updates Vista's defenses](#)
- [Security theater](#)
- [Details on the compromised Ubuntu servers](#)
- [Details on recent Microsoft vulnerabilities](#)
- [Security features of Microsoft Exchange Server 2007 Service Pack 1](#)
- [Enterprise-class fingerprint authentication solution for SMB](#)
- [Facebook users share their info to potential ID thieves](#)

LATEST ARTICLES VIRUS CENTER

- [Malware Evolution: April - June 2007](#)
- [Working with the iStumbler Wireless Discovery Tool](#)
- [Interview with Christen Krogh, Opera Software's VP of Engineering](#)
- [Guide to Online Antivirus Solutions Part 3: Kaspersky Online Scanner](#)
- [Compliance, IT Security and a Clear Conscience](#)
- [Danger behind instant messaging applications](#)
- [Malware uses Hotmail and Gmail as spam hosts](#)
- [Spammed out "shocking photos" emails contain malicious payload](#)
- [Top 20 virus list for July 2007](#)
- [When trojans go phishing 500,000 get infected](#)

SECURITY SOFTWARE



- [++ GFI LANguard Network Security Scanner 8](#)
- [SSL-Explorer 0.2.15](#)
- [Eraser 5.84](#)
- [ShyFile 6.35](#)
- [Tor, Privoxy and Vidalia bundle 0.1.2.16](#)
- [Outpost](#)

[Firewall Pro 4.0.1025.782](#) • [Ad-Aware 2007 Free](#) • [Security System Analyzer 1.5.2](#) • [Password Policy Enforcer 5.0](#) • [WinSCP 4.0.3](#) • [Password Safe 3.09](#) • [Shorewall 4.0.2](#) • [Dropbear SSH Server 0.50](#) • [OS-SIM 0.9.9 rc5](#) • [strongSwan 4.1.5](#) • [ArpAlert 2.0.7](#) • [Prelude Manager 0.9.9](#) • [NuFw 2.2.3](#) • [MailScanner 4.62.9-2](#) • [Nagios 3.0b1](#) • [Firewall Builder 2.1.13](#) • [TCPDUMP 3.9.7](#) • [Botan 1.6.3](#) • [SafariSafe 1.1](#) • [NetShred X 4.0](#) • [TPM Setup 1.0](#) • [The DoorStop X Security Suite 2.0](#) • [LockMeBaby 1.12](#) • [1Passwd Password Manager 2.4.6](#) • [Shimo 1.0](#) • [Random Password Generator 1.6.1](#) • [Radmin Assistant 1.0.0](#) • [PDFKey Pro 3.4.1](#) • [MultiAlarm 3.4.2](#) • [Mac GPG 1.4.7](#) • [SecuBox for Pocket PC 1.22](#) • [Crippin 2.12](#) • [Aircscanner Mobile Encrypter 2.9](#) • [Sentry 2020 2.9](#) • [WiFiFoFum 2.1.1](#) • [AirFix 1.0b](#) • [Confidential Notes 1.1](#) • [Aircscanner Mobile Firewall 2.4](#) • [WiFi Graph 0.3 RC3](#) • [SignWise Pro 2.52](#) • [eWallet 4.0](#) • [Pocket Warrior 15022003-B](#)

 **ADVISORIES**  **VULNERABILITIES**

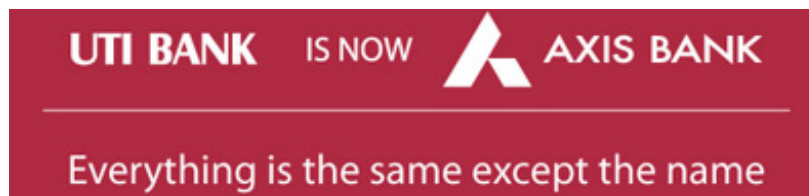
• [Cisco Security Advisory - Local Privilege Escalation Vulnerabilities in Cisco VPN Client \(cisco-sa-20070815-vpnclient\)](#) • [Gentoo Linux Security Advisory - Mozilla products: Multiple vulnerabilities \(GLSA 200708-09\)](#) • [US-CERT Technical Cyber Security Alert - Microsoft Updates for Multiple Vulnerabilities \(TA07-226A\)](#) • [Microsoft Security Bulletin - Summary for August 2007](#) • [Ubuntu Security Notice - xfce4-terminal vulnerability \(USN-497-1\)](#) • [Debian Security Advisory - kdegraphics \(DSA 1355-1\)](#) • [Windows Metafile AttemptWrite Heap Overflow](#) • [Microsoft Internet Explorer VGX.DLL Compressed Content Heap Overflow/Vulnerability](#) • [Microsoft Windows Media Player Malformed Skin Header Code Execution Vulnerability](#) • [Microsoft Internet Explorer substringData\(\) Heap Overflow Vulnerability](#) • [Multiple vulnerabilities in Live for Speed 0.5X10](#) • [Crash in Zoidcom 0.6.7](#)

Qualys: [Scan your server for thousands of vulnerabilities with FreeScan. You will also receive detailed information on each risk.](#)

Bank changes its name, phishers smell the potential Posted on 09 August 2007.

UTI bank, one of the leading banks in India has changed its name to 'Axis'. And who better than phishers know to fish in the muddy waters of confusion. Security experts at MicroWorld Technologies warn that a spammed email is trying to loot the bank's customers in the backdrop of the name change.

Like most Phishing mails targeted at Indian banks, this one too talks about a security upgrade. What you see at the top bar of the mail is an image which says, "UTI bank is now Axis Bank, Everything is the same except the name'. And it's a straight lift from the actual redirect page that appears when you key in 'utibank.com' in the address bar of the browser.



The content of the mail is as follows;

Dear Customer,

Axis Bank Internet Banking, is here by announcing the New Security Upgrade. We've upgraded our new SSL servers to serve our customers for a better and secure banking service, against any fraudulent activities. Due to this recent upgrade,

Bank changes its name, phishers smell the potential

you are requested to update your account information by following the reference below.

*Reference**

https://xxxxxxxxxxxxxxxxxxxxxxxx

If your account information is not updated within 48 hours then your ability to access your account will become restricted.

Thank you.

Axis Bank Account Review Department

“The Phishing website linked to the mail is already taken down by the hosting firm. However you can’t wish away the probability of the same mail bouncing back with a new website hosted somewhere else,” observes Sunil Kripalani, Vice President, Global Sales and Marketing, MicroWorld Technologies.

“What’s interesting here is the perfect criminal timing of the mail. When you have a big bank changing its name, naturally there’s bound to be some confusion among its customers. A naive customer might think that the security update is a part of the bank’s name changing process,” he adds.

The success of a Phishing scam depends largely on the Social Engineering tactic used in it. The idea is to get as many people as possible to click on the link in the mail and follow the instructions without thinking much. And phishers experiment with shock, lure or scare to achieve this end.

“Phishing has advanced much in technology as well. A computer infected with a Phishing Trojan can redirect a user to a fraudulent website even if he keys in the actual URL of the bank in the browser! This method is called pharming and it can only be countered by protecting computers with a proactive security solution,” points out Sunil Kripalani.

[[Security World main page](#)]

