

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



Finjan gives you protection that signature-based products **cannot even see**

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

- [Home](#)
- [About](#)
- [Submit News](#)
- [Search News](#)
- [IT Events](#)
- [Time & Money](#)
- [European Media](#)

When UTI Bank Becomes Axis, Phishers Smell It First

Published 14th 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, you are requested to update your account information by following the reference below.

Reference*

<https://xxxxxxxxxxxxxxxxxxxxxx>

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.

MicroWorld Technologies makes advanced AntiVirus, AntiSpam and Content Security solutions to counter all sorts of online threats. While eScan from MicroWorld tackles Phishing, Pharming and Spamming at the server and desktop level, its other product, MailScan, provides security at the Mail Server level.