

16 April 2008

By: Bogdan Popa, Security and Search Engines Editor



Visa is now the main attraction for phishers  
stuff.co.nz

## [After MasterCard, Visa Gets Scammed Too](#)

### *Sophos detects a new phishing scheme*

Following last week's report that MasterCard owners had been targeted by a phishing scheme attempting to steal their private financial details, it was only a matter of time until Visa's consumers joined the club. Security company Sophos today reports that a new phishing scam was detected, this time targeting Visa owners. Similar to other attacks in the past, the malicious email arriving in the Visa users' inboxes attempts to bring them on a dangerous webpage which asks for all sorts of details. This time, the email claims that, as Visa owners, users should register for the "Verified by Visa" technology which "protects your existing Visa card with a password you create", giving you assurance that only you can use your Visa card online. "The email came with a forged verifiedbyvisa.com 'From' address, and provides plenty of links to the real Verified by Visa page. The "Activate Now" button, however, takes you to a phishing page hosted on a compromised domain," Savio Lau of Sophos Labs wrote. As mentioned, the phishing website requires all sorts of details, starting with general information about the user and ending with financial credentials, including here the 3-digit security ID, the ATM pin and the Visa card number. However, there is a sign that clearly shows the victims of the scams that the website is fake and not a genuine one: "the help link for the security key, however, directs a user to the Yahoo! Security Key page," the Sophos official explains. "If an unsuspecting user visits the link, chances are they will get suspicious and start wondering what Yahoo! IDs have to do with Verified by Visa. So, this phish site is not very well constructed. This phish campaign also lacks the enticing 16% purchase discount offered by the previous attempt. Hopefully, even non-alert users would recognize this phishing attempt due to the inconsistencies on the site. On the other hand, alert computer users employing safe computing practices would not have clicked on the link in the first place."