Phishing thieves try a spot of pharming
Kelly Mills
MARCH 29, 2005

ONLINE identity fraud attacks on customers of financial institutions continue to rise as phishers try new tactics to obtain personal financial information.

Last month, 13,141 new phishing email messages were reported to the US-based Anti-Phishing Working Group.

This was an increase of 2 per cent, compared with January.

In the past, most phishing attacks have used spoofed emails and fraudulent websites to fool customers of financial institutions into divulging personal financial information.

According to the APWG, phishers have turned to using alternative methods to obtain information.

Use of instant messaging to spoof and phish for information is becoming more frequent.

"Phishing without a lure is becoming more prevalent among attack styles," the February 2005 Phishing Activity Trends report says.

The most common new method is malicious code, which either modifies the host's file to go to the fraudulent site, also known as "pharming", and malicious code that logs keystrokes.

"Domain name server cache poisoning is an alternative means to get information to non-legitimate pharming websites," the report says.

The US is the country where most phishing sites are hosted.

Last month it had more than 37 per cent of sites, up almost 6 per cent on the previous month.

Other countries high on the list include China, Korea, Brazil and Germany.

The financial services sector continues to be the most targeted, averaging 78 per cent of the most commonly virtually hijacked companies.

In February, the number of companies targeted by email phishing attacks remained at 64, the same number reported in January.

The APWG was formed last June and has more than 1200 members globally, including eight of the top 10 US banks and four of the top five US internet service providers.

This report appears on australianIT.com.au.