AUSTRALIA is a world leader in phishing scams and the fourth most common launching pad for internet attacks, research shows. A recent Symantec internet security threat report, which covers trends for the six months to June 30, ranks Australia fourth behind the US, China and Canada as the "last known source" of internet attacks.

Australia accounted for 4.8 per cent of all attacks, up from 2.6 per cent in the six months to the end of December, and the US dropped from 58 per cent to 37 per cent.

Symantec counted a "huge increase" in the number of automated bot network attacks in the same period, Symantec managing director John Donovan said.

Bot networks use small applications installed on infected machines to launch other attacks.

Over the first half of the year, the number of monitored bots rose from 2000 daily to more than 30,000 daily, with occasional peaks of more than 75,000 daily, Symantec reported.

Mr Donovan said it took an average of 5.8 days to launch an "exploit" once a vulnerability had been announced.

Symantec found e-commerce was the most frequently targeted sector, accounting for 16 per cent of attacks.

Much of the growth in Australian-sourced attacks came from phishing scams, which attempt to dupe users into revealing personal information on fake websites that appear to belong to banks, finance companies and other organisations.

"Australia seems to be at the forefront of phishing schemes, particularly because we have a very well developed banking sector," Mr Donovan said.

Targeted attacks on e-commerce sites, generally aimed at theft of personal customer information or credit card details, had increased, he said.

This was part of a wider trend towards internet security attacks for financial gain.

"We can now firmly say that the style of attacks has changed and the theft of proprietary data and the theft of financial information is at the forefront of malicious code," Mr Donovan said.

Although home users were often blamed for the large number of security-compromised machines available to hackers and criminals, the study found malicious code was also emanating from 40 per cent of Fortune 500 companies.

More education, including possible government initiatives, was needed to counteract the problem of ignorant users compromising their own systems, Mr Donovan said.

"We have a monumental task ahead of us to educate people on security best practice, from individual consumers right through to enterprise," he said.
Symantec counted 4496 new viruses over the first six months of the year, and an average of 48 new system vulnerabilities a week.

Of the vulnerabilities, 70 per cent were considered easy to exploit.

This report appears on australianIT.com.au.