



PICK A CARD ... hackers can take control of tens of thousands of PCs and, unbeknown to the users, use them for malicious intent, in particular to download e-mail addresses.

Users must prevent phishing or pharming

INTERNET banking is available at all hours of the day and night, from anywhere, and is a cost-efficient service to deliver.

However, it is vulnerable to malicious practices such as identity theft, phishing and pharming, whereby a user gets redirected to a bogus website.

"Users can have all the virus protection in the world, but it is up to ISPs to ensure their servers are protected against pharming," says Simon Webster, technical consultant at Webcom.

This malicious practice involves manipulation at the point where the website address, or domain name, is translated into a numerical IP address.

Another common scam is harvesting e-mail addresses for spam and other unsolicited marketing activity.

"Harvesters can get as much as \$500 for a list of 10 000 authenticated e-mail addresses."

These e-mail addresses are obtained in various ways, including enticing users to respond to free offers or to forward chain-mail-type e-mails to all their friends and siphoning off the e-mail addresses

to the harvester's database.

Another method of harvesting is to use a program called a bot to infiltrate databases to harvest e-mail addresses, or to get the bot to feed random names into a database and come out with likely e-mail addresses.

For example, the bot might be instructed to come up with 1 000 first names, 1 000 surnames and 1 000 company names, either randomly or relating to a specific industry sector.

"They might get less than a 1% hit rate for real e-mail addresses, but they just leave the bot running," says Webster.

Then there are botnets, used by hackers to take control of tens of thousands of PCs and, unbeknown to the users, use them for malicious intent.

"These hackers are referred to as botnet herders or shepherds."

When doing internet banking it is risky for users to use a PC that is not under their control or under the control of their company, especially when travelling.

In an internet cafe there could be a network sniffer in the back office that logs the activity of users,

or a key logger device might be used to capture their keystrokes.

"Hackers can download what is being typed remotely from 10m to 100m away using Bluetooth, for example while sitting outside the internet café in a car," says Webster.

However, he says, shoulder surfing is one of the most common causes of unauthorised access to personal information.

For example, a trusted colleague watches what a user is doing, or the user is interrupted or leaves the PC unattended in the middle of what he or she is doing while getting a cup of coffee, and gains unauthorised access.

But the banks are addressing this kind of vulnerability with dual accreditation, for example sending a one-time password to a person's cellphone.

"The banks have gone beyond the bounds of banking regulations to protect their customers," says Webster.

He says the onus is therefore on customers to follow the security protocols that are provided in the same way they would when using bank cards.