Alert online users help bank foil phishing scam

By Grace Ng

VIGILANT DBS Bank customers have foiled a phishing expedition aimed at hooking cash out of their bank accounts.

It is the second time in six months that DBS has been targeted by high-tech fraudsters.

The scam involves tricking people into revealing confidential information, such as a PIN or passwords, through legitimate-looking e-mail messages linked to a DBS look-alike website.

Several DBS customers received the e-mail on Sunday night and some alerted the bank quickly.

DBS filed a complaint to an international watchdog for Internet security and had the overseas-based site shut down yesterday.

While savvy customers were quick to alert the bank, Singapore blogs also beamed out a red alert to the local Singaporean cyber community within hours of the first phish attacks.

Mr James Seng, assistant director of enabler technologies at the Infocomm Development Authority of Singapore, posted a warning at 7.47pm on Sunday. He said in his weblog that the bogus e-mail message "actually comes from hostpymes.com, registered to someone called Soria, Luis based in Peru".

"Already as early as last year, we were aware the biggest problem of spam isn't penis enlargement, Viagra or even pornography but rather the targeted phishing attacks like this," he wrote.

News reports from IT and financial publications cite at least seven phishing scams on local and foreign banks targeting Singapore customers in the past year.

Citibank was one of the most popular targets last year, with more than 400 different phishing scams hitting its outlets worldwide.

Last September, OCBC was "phished" from China. The first DBS-targeted scam followed two months later from China as well.

In the recent attack, DBS customers received e-mail messages with the subject header "DBS Verification Service", ostensibly sent out by its IT support department.

"Our suspicion is that the phishing culprits got hold of an e-mail database and targeted their e-mail at DBS because the chances of hitting a DBS customer is very high," said Ms Pearlyn Phau, DBS senior vice-president and head of i-Banking.

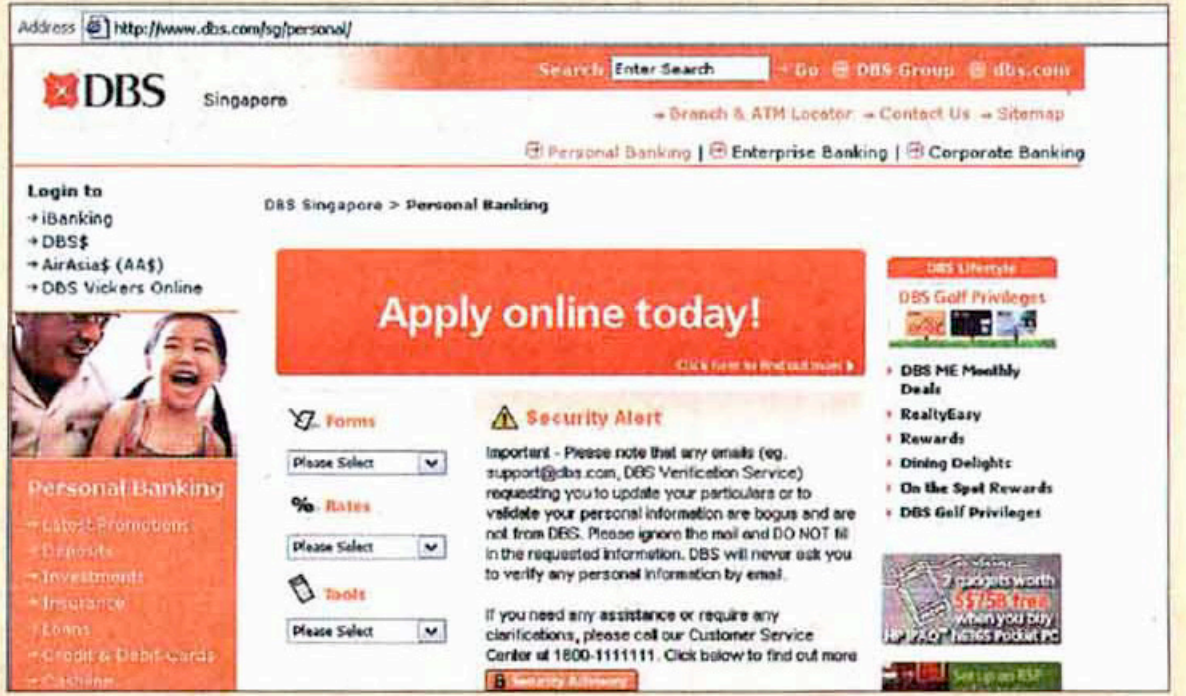
Some key points to foil phishers:

›› It is generally not a bank's policy to ask customers to verify personal details by e-mail.

Beware e-mail messages which claim that "for security purposes" the bank customer must provide personal data via e-mail. Some will claim that access to the account will be denied unless the customer provides all the data requested.

›› Enter the bank account personally and directly enter the relevant bank's website address in the browser address bar. Do not log in via any hyperlink within e-mail; and

›› Always log out after completing online transactions.



Staying vigilant

Some points to help guard against phishing:

›› Banks generally do not ask customers to verify personal details by e-mail.

›› Do not click on hyperlinks in the e-mail message but instead type in the bank's website address in the browser address bar. Also enter the bank account personally.

›› Always log out after finishing online transactions.