COMPUTERWORLD
The voice of the ICT community

NEWS ▾

THURSDAY, 05 AUGUST 2010

FOLLOW US ON TWITTER | | BECOME A FAN ON FACEBOOK | | RSS

Invalid banking cert spooks only one user in 300

Users remain the weakest link

BY STEPHEN BELL | WELLINGTON | MONDAY, 16 MAY, 2005

✉ EMAIL   🖶 PRINT

Up to 300 BankDirect customers were presented with a security alert when they visited the bank's website earlier this month — and all but one dismissed the warning and carried on with their banking.

The bank's logs show about 300 customers used the single affected server during the 11-hour period when the certificate was out of date and only one backed out of the page, says Clayton Wakefield, head of technology for BankDirect owner ASB.

Peter Benson, chief executive of Auckland-based Security-Assessment.com, says he is "not at all surprised" at the statistics. "In my experience, the single weakest point in the chain of [computer] security is the space between the keyboard and the floor."

A lot more education of users in responding appropriately to security alerts is needed, he says.

That said, an expired security certificate probably does not represent a great risk in itself, Benson says. It's most likely someone in the organisation just forgot to do the regular update, as was the case at BankDirect.

In a worst-case scenario, he says, such a warning may be connected with a sophisticated phishing or pharming attack aided by DNS "cache poisoning". Here malicious hackers use a DNS server they control to feed erroneous information to other DNS servers. A user relying on a poisoned DNS server to manage their web surfing requests might find that entering the URL of a well-known website directs them to an unexpected or malicious web page.

The main risk such a fault indicates is social and educational, not technical, Benson says. The kind of person who thoughtlessly clicks away an expired-certificate warning is likely to indulge in more risky behaviour, such as visiting a fraudulent website whose URL is included in an email and disclosing confidential information such as an account number.

Peter Muggleston, group manager of ASB Online, is also not surprised by the figures, but doesn't see it as a reason to worry about users' lack of caution. The certificate was only one day past expiry, he notes, and all its other details were valid. "We don't know how many customers just clicked the warning away because they didn't know what it was, and how many looked at it and made a considered judgement that the mistake didn't reflect anything serious. And we wouldn't know that without calling every one of the 300 and interviewing them.

"It's not a good look for us," he concedes, "and we'd always like our customers to be cautious", but users made the right decision in this case and most probably thought before acting.

It's also possible that some users did not even see the warning, because some browsers configured with a low security setting will not warn of expired certificates.

SHARE THIS STORY WITH:

✉ EMAIL
🖶 PRINT

READ | COMMENTED | EMAILED | SHARED

- "UFB is a piece of …"
- Internet account ban no worse than driving penalty
- Datacom chief dies suddenly
- iFiasco
- At the 2degrees 3G launch
- Chorus2 can deliver on urban and rural fibre

POPULAR EVENTS

The Sustainable 60 Awards
Entries open now.
Click here for more details

Unlimited Investment Challenge 2010
Entries open now.
Click here for more details

The Sustainable 60 Workshops
Dates confirmed
Click here for more details

SPONSORED LINKS

COMPUTERWORLD
Local and International news
Enterprise ICT must know info
Subscribe today

PC WORLD $599!
NZ's most trusted tech advice
Free NZ Delivery
Subscribe today