

topstory



June 18, 2008 03:19pm AEST

New protection for online banking users

Karen Dearne | June 18, 2008

The IT industry is beginning to provide tools that give consumers control over their own security during online transactions.

This week, TrustDefender unveiled a software tool that allows online users to check if they are genuinely connected to their own bank's website, and prevents man-in-the-browser attacks that can hijack legitimate banking sessions.

Man-in-the-browser attacks are particularly dangerous, because the malware (malicious software) activates after a user has logged on and authenticated a session, rendering two-factor or SMS code authentications useless.

TrustDefender has developed a database of URLs, network security information including SSL certificates, and software policies for every major bank in Australia. Users can download the software, and it then automatically checks bank website credentials each time an online session begins. Users will be alerted if unauthorised internet requests intervene in the session.

The tool is bundled with TrustDefender v2 Gold Edition, a home user protection package which costs about \$24 a year.

"The product is designed as an additional layer of protection, and does not replace existing bank or consumer security arrangements," Andreas Baumhof, TrustDefender chief technical officer, said.

The application is part of a broader online security push dubbed the Financial Trust Network (FTN) which is managed by TrustDefender.

The FTN operates independently of local financial institutions, but is supported by most, Mr Baumhof said. The initiative is an attempt to look at internet security problems from a consumer's perspective.

"Online fraud cannot be solved by the banks or merchants on their own," he said. "It's a disaster for consumer confidence. Would you put your card in an ATM with its sides ripped open, even if the bank assures you that it's safe, and in any case they'll reimburse any money you lose? No, you wouldn't, but that's the online scenario today.

"In order to solve this, we really need to increase the first-line of defence, on the desktop," Mr Baumhof said.

He claimed that for the first time, web users could take action themselves, rather than relying on the security of individual banks.

"Unfortunately, too many banks regard security as a competitive advantage, resulting in a mixture of security approaches which confuses people," he said. "Knowing exactly which SSL certificates or internet requests belong to a particular web service is a fundamental step towards consumer protection."

TrustDefender also plans to launch independent Financial Trust Networks in the US, Britain and Germany. It has just appointed security expert Martin Schottenloher as chairman and head of operations in Europe.

Anti-virus software vendor McAfee last week released an anti-theft product that allows people to secure private data stored on mobile phones and other devices.

Last month, German federal police officer Andre Dornbusch told the AusCERT conference man-in-the

browser attacks relied on sophisticated social engineering to trick users into authenticating to malware, effectively opening a second session which remained open after the initial transaction ended.

"Often there is a request, seemingly from the user's bank, asking the person to re-enter the transaction authentication, and that allows the attacker to take over the session," Mr Dornbusch said.

"The attacker then keeps the session open, and can transfer money out of the account. Worryingly, users won't see these transactions on their records, and won't be aware that their online banking session was breached."

Copyright 2008 News Limited. All times AEST (GMT +10).