Scam alert on

Bank Trojans

How the scam works

Criminals and hackers are using malicious programs to hijack online banking sessions and steal money from corporate, as well as personal, bank accounts. Here's how it goes:

1. An IT user unknowingly picks up the Trojan horse infection, typically by opening an email attachment or website link in a phishing email, or downloading an infectious app, or from another user on a USB stick or through the network.
2. The Trojan runs quietly in the background, hiding itself from antivirus and waiting patiently until the user visits an online bank for personal or corporate banking.
3. While the user interacts with the online bank in the normal way, the Trojan intercepts and modifies the user's commands, typically diverting **thousands of dollars** to money mules. At the same time, it intercepts and modifies what gets displayed on the screen, so that to the user nothing *appears* to be wrong.
4. Even if the bank requires the user to enter a special code from a security token or TXT message to authorize or release a transaction, the Trojan intercepts and has full control of it.
5. The money mules quickly pass-on the stolen money through untraceable routes (money laundering) and the fraud is complete: the user, the user's organization and/or the bank is left out of pocket.

Avoid the scam

- Be *very* suspicious of email attachments and links.
- If possible, dedicate a specific computer solely to online banking: don't read email or browse the web from that system.
- Keep your computers and other IT devices patched, backed up and the antivirus up to date.
- Steer clear of unofficial app stores and dubious websites. It's simply not worth the risk.
- If it's too late, call your bank and Help Desk to report incidents *urgently*. In fact, call them at the earliest sign of trouble, if you merely *suspect* that something odd is going on. They would far rather investigate false alarms than have to console and refund fraud victims.

Further information

Browse the intranet *Security Zone* or contact the Help Desk to find out more about malware.