Bogus training offer opens hacker doors to bank accounts

February 5 2012, by Nancy Owano

(PhysOrg.com) -- Mischief-making hackers, always willing to try clever ways to bypass advanced security safeguards, have figured out a way to make off like bandits, literally. According to a BBC report, the exploit first tricks account-owning victims by presenting offers of training for an upgraded security system. The hacker criminals, with their victims unaware, proceed to move money out of these users' accounts.

What braces bank security in particular is not only the crime but the fact that hackers continue to easily skirt the latest-generation security techniques.

Bank security measures in the past like PINSentry from Barclays and SecureKey from HSBC have come up with devices that use an account holder's card or code to create a unique key at each login. The entry is valid for around thirty seconds. "While these chip and pin devices make the hackers' job more difficult, the hackers themselves have raised their game," says the BBC report.

The hacker technique at play is "man in the browser" malware, meaning that the malware is in the browser. With this kind of attack, the exploit can change what is seen and can play with details of what is being entered. Some of the attacks, for example, change payment details and amounts on screen balances. The user and the host application are unaware that a break-in is under way. "MitB" code is likely to remain a headache for banks as attackers continue to evolve their capabilities. Daniel Brett, of malware testing lab S21sec.was quoted in the report as

describing the browser attack as an advanced, banking-focused threat.

Online banking fraud losses totaled £16.9 million in the first six months of 2011, according to Financial Fraud Action UK. In the UK, banks usually refund victims of online fraud.

Actually, as worrying as new types of exploits may be, the problem is not new. The banking industry has been coping with hackers targeting them for some time. Back in December 2010, *Security Week* was reporting that attackers were starting to improve the "autonomous capabilities of MitB code." The article noted how the SilentBanker Trojan targeted more than 400 banks and had the ability to intercept banking transactions, even those guarded by two-factor authentication. Two-factor authentication refers to a security measure whereby the user is required to provide two means of identification, one of which is something the person has (a card, e.g.) and the other something memorized, something the person knows.

Banks and experts nonetheless say that online banking users can do well to simply be alert and take care. Experts suggest typing bank URLs in the browser rather than using links included in unsolicited emails.

When up on the site, they recommend users be alert to suspicious signs such as a process not looking the same as usual or a transaction taking longer than usual. If worried about a break-in, they advise users to contact the bank by phone, not e-mail, and report the time and date of the suspected incident.