2 February 2012 Last updated at 11:12 ET

Hackers outwit online banking identity security systems

By Spencer Kelly Click presenter

Criminal hackers have found a way round the latest generation of online banking security devices given out by banks, the BBC has learned.

After logging in to the bank's real site, account holders are being tricked by the offer of training in a new "upgraded security system".

Money is then moved out of the account but this is hidden from the user.

Experts say customers should follow banks' official advice, use up-to-date anti-virus software and be vigilant.

Devices like PINSentry from Barclays and SecureKey from HSBC - which look a lot like calculators - ask users to insert a card or a code to create a unique key at each login, valid for around 30 seconds, that cannot be used again.

This brought a new level of online banking security against password theft. The additional line of defence provided security even if a user's computer along with any password information was hacked.

While these chip and pin devices make the hackers' job more difficult, the hackers themselves have raised their game.

'Man in the Browser' attack

A test witnessed as part of a BBC Click investigation suggests even those with up-to-date anti-virus software could be at risk.

There is no specific risk to any one individual bank.

In the test the majority of web security software on standard settings did not spot that a previously unseen piece of malware created in the software testing lab was behaving suspiciously.

The threat does not strike until the user visits particular websites.

Called a Man in the Browser (MitB) attack, the malware lives in the web browser and can get between the user and the website, altering what is seen and changing details of what is being entered.

Some versions of the MitB will change payment details and amounts and also change on-screen balances to hide its activities.

With the additional security devices, the risk of fraud is only present for one transaction, and only if the customer falls for the "training exercise".

"The man in the browser attack is a very focused, very specific, advanced threat, specifically focused against banking," said Daniel Brett, of malware testing lab S21sec.

"[Although] many products won't pick this up, they've got a much bigger scope, they're having to defend against all the viruses since the beginning of time."

Every time a new update to the malware is released, it takes the security companies a number of weeks to learn how to spot it - to learn its common features.

But one security company did privately concede that, if this threat had come from a source not known to be bad and started communicating with a web address also not on the black-list of "bad" sites - until they had discovered and analysed it - it probably would have beaten their protection.

Fraud detection software

Makers of many of the security products featured in tests argued that it was not valid as it only tested one part of their protection.

They point out that they continually search for and blacklist websites, emails, and other sources of malware.

Mark Bowerman, of Financial Fraud Action UK, said: "Banks also employ what's called back-end security and that's what's happening behind the scenes to protect you from online banking fraud.

"We've got intelligent fraud detection software, and it's used to seeing how you operate your online bank account.

"Any deviations from the norm and the software is going to pick it up - that may be the type of transaction you've made or the amount."

Most PC security products will block this kind of threat if their security settings are turned up to maximum but will also block many legitimate programs too.

Online banking fraud losses totalled £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 as a matter of course.

Banks and experts say customers must continue using online security anti-virus products.

Hackers can even manipulate online statements so customers will not automatically see changes