

BEYOND PHISHING – DE-MYSTIFYING THE GROWING THREAT OF INTERNET BANKING FRAUD

Internet banking is now a mass-market product that is demanded as an essential service by increasing numbers of bank customers. More and more people rely upon the convenience and ease of use of Internet banking services in their daily life. More and more, the quality of a bank's Internet banking service can affect the overall level of satisfaction and loyalty of its customers.

Ironically, the growing availability and popularity of Internet banking has created the biggest challenge to its continued viability and growth. Fraudsters are attracted by the huge potential for online theft and are posing increasingly sophisticated and effective threats to the security of customer transactions carried out over the Internet.

Gone Phishing

Much publicity has been generated lately over so-called 'phishing' attacks – attempts by fraudsters to capture and record customers' security details, then later use them to commit fraud. Phishing attacks have enjoyed a high degree of success by exploiting the banks' reliance upon simple user verification based upon identities, passwords and other 'secret' information. Phishing attacks are now mundane and commonplace – most customers are familiar with a plethora of emails of varying plausibility landing in their in-boxes purporting to be from banks asking them to go and 'confirm' their security details.

The result, as always, is that the world moves on. Banks have started to address the phishing threat by upgrading the security of their systems and adopting so-called two-factor authentication, requiring customers to use a separate card reader or hand-held authentication device to gain access to the service. However, sophisticated fraudsters always remain one step ahead, and have now moved on the threat of attack well beyond mere phishing.

Beyond Phishing - Man in the Middle (MitM)

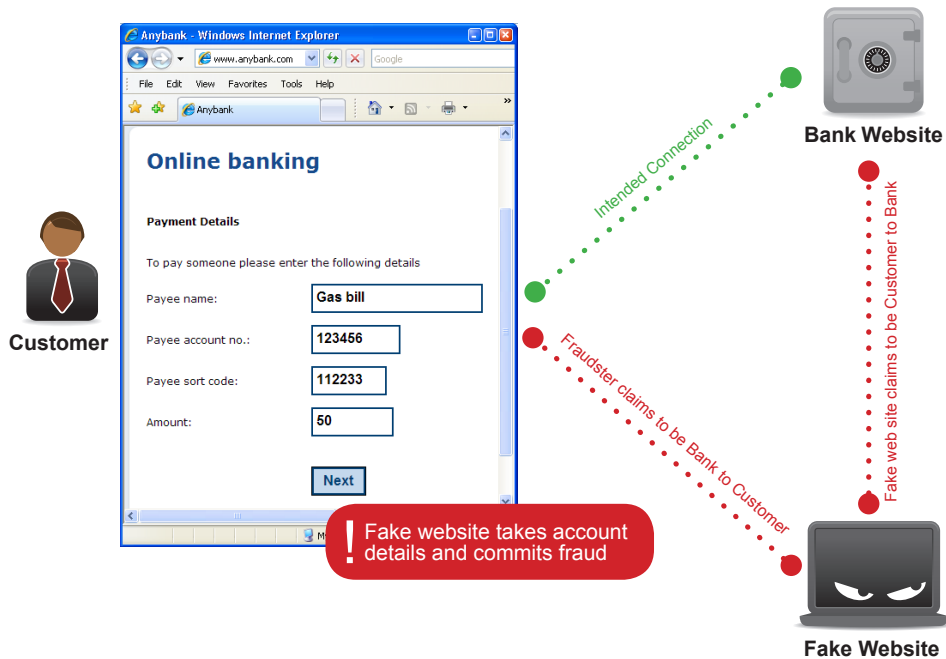
A recent and rapidly growing threat to online banking security is the so-called "Man in the Middle" (MitM) attack. This fraud technique was introduced to circumvent recently deployed security measures such as mutual authentication and tokens. While the MitM attack requires a more sophisticated approach than simply collecting details, this technique has already been used by criminals on numerous occasions and has been responsible for large amounts of fraud. There are even kits available now from the Internet, allowing comparatively unskilled fraudsters to mount apparently sophisticated attacks.

The basic MitM attack first involves the fraudster coercing the bank customer to visit a fake banking website. This is most commonly achieved by sending an email, impersonating a bank, asking the customer to click on a provided link, supposedly of the bank website. Other approaches include tampering with the customer's Internet connection so that when they try to visit the correct website, they actually are connected to the fake one.

To the user, the website will appear identical to the normal bank website. It may even be encrypted so the customer will see the expected padlock symbol in their web browser. However, details entered will go to the fake bank website, not to the real one. When these details are received, specially written software will connect to the bank's real website, impersonate the customer and make fraudulent transactions.

Between 2005 and 2007, **Nordea** was the target of a sophisticated malware attack, which caused **losses of over \$1,000,000**. The software recorded user's account details and sent them to fraudsters, believed to be based in Russia. The fraudsters made a series of small transfers, in order to circumvent the bank's fraud detection measures.

Man in the Middle



In 2006 the **business customers of Citibank** were targeted by a Man in the Middle attack. The email asked customers to confirm their address, stating that suspicious activity was detected. The site asked for account details, including the one-time-password from the tokens issued to customers. If they were incorrect, the customer would be asked to re-enter them.

Since the fake website has all the details the customer would normally give, the bank cannot tell the difference between the real customer and the fraudster. Because the connection to the bank occurs immediately after the customer enters their account details, any time-dependent one-time password will still be valid. If the bank has implemented mutual authentication, the fake website will receive the correct response from the bank, such as pictures or answers to secret questions, and send it back to the customer. The customer will see the expected response and so send the account details the fraudster desires. While both the bank and the customer believe they are communicating directly, in fact the fraudster is free to view and modify any of the transmitted information.

Diligent bank customers may be able to identify fake sites, since their address may be incorrect. While some are encrypted, carefully inspecting the website certification may show that the site does not really belong to who it claims to. Also, while fraudsters may try to connect to the bank website from a computer in the same country as the customer, bank fraud detection systems might notice suspicious characteristics.

Things get worse - Man in the Browser (MitB)

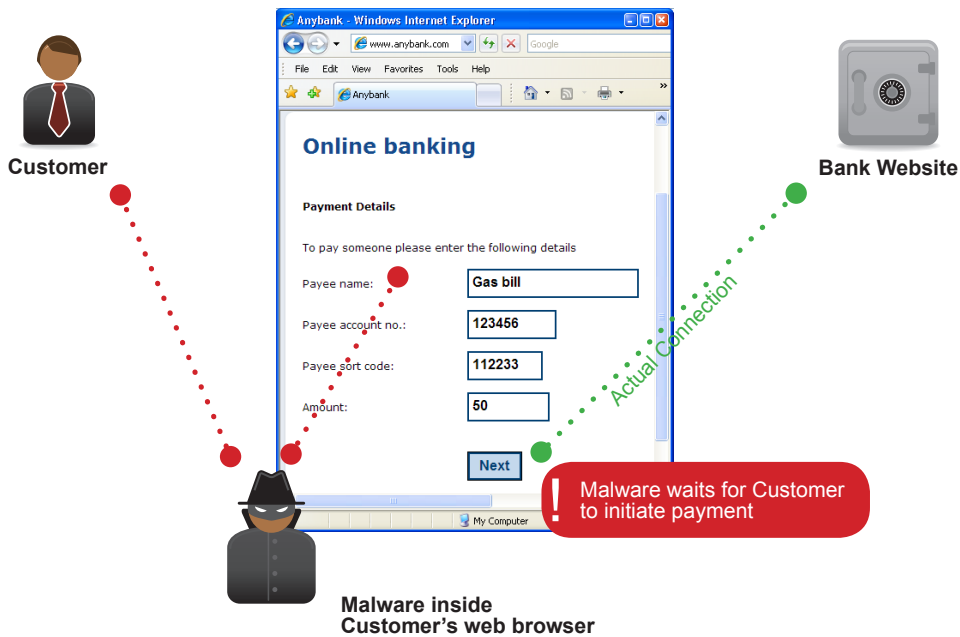
For these reasons, fraudsters have now developed a more sophisticated variant of MitM – the Man in the Browser (MitB) attack. Here, rather than intercepting communication between the customer's computer and the bank website, the MitB intercepts between the customer and their web browser.

A MitB attack is mounted by installing malicious software (malware) on the customer's computer. This can occur by a customer opening an email attachment or downloading a file from a website. Just visiting a website, or viewing an email, may be sufficient for a fraudster to install malware without the customer giving permission. In some cases criminals have tampered with existing legitimate websites, so that they will infect their visitors.

The customer is unlikely to notice that anything is different. As much as 80% of new malware is undetected by anti-virus software. Normal web browsing will be unaffected, but the malware will recognize when the customer visits their online bank website. Then, the malware can freely alter the web page as it is displayed to the customer, and modify the requests sent back to the bank.

In 2007 **ABN AMRO** was the victim of a malware-based attack on their online banking service. Customers were sent an email, claiming to be from the bank itself, which contained an attachment. When the customer visits their banking site, they will be sent to a fake one which collects the account details. **Even though ABN AMRO deployed two-factor card reader based authentication**, the fraudsters were able to place transactions while the one-time-password is still valid.

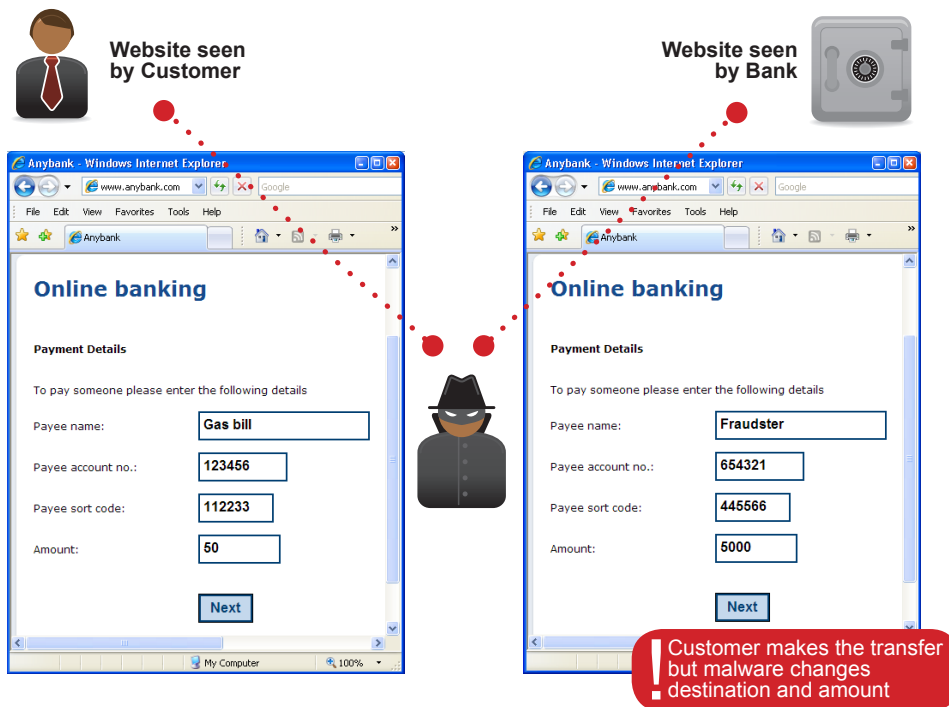
Man in the Browser



In January 2008, the **SilentBanker trojan** targeted **over 400 banks** worldwide including the USA, France, Spain, Ireland, the UK, Finland, Turkey. The malware is capable of executing a **Man in the Browser attack** and includes an automatic updates mechanism for extending the list of targets.

For example, if the customer makes a transfer to one account, the malware could change the destination account number to that of the fraudster, and increase the amount. Similarly, once the bank confirms that the transfer has occurred, the malware will change what is displayed to the customer, making them think that their desired transaction has been executed.

Man in the Browser



Generic malware packages are available which allow fraudsters to easily configure the software to attack particular banks. The configuration file is downloaded from a website, so can be rapidly updated to add new banks or adapt to changes in website structure. One such package, known as the SilentBanker, is able to mount attacks on over 400 different bank websites worldwide, and has features specifically designed to circumvent two-factor authentication. Not only is it capable of classic MitM attacks, but it is also capable of MitB.

The MitB attack is even harder to defend against than MitM. Since the network connection is not being interfered with, the website address and certificate will be correct. Fraud detection systems are also hampered by the fact that, from the bank's perspective, the customer is visiting from their normal computer and using their usual Internet connection. As with MitM, because MitB attacks happen in real time, tokens and mutual authentication can be circumvented. Since the fraudster has full control over the customer's computer, biometric-based security mechanisms are also ineffective.

So where do Banks go from here?

In summary, Man in the Middle and Man in the Browser attacks are a serious and growing threat to online banking. They work by tricking customers into believing they are communicating directly with their bank, when in fact a fraudster is reading and modifying information sent and received. Because the attacks work in real time, standard security techniques, such as tokens, one-time-passwords, mutual authentication and biometrics can all be bypassed. What can the banks do to counter these latest threats?

The answer lies in transaction authentication, where not only the customer's identity but also the details of the transaction to be carried out must be authenticated by the customer. This, in conjunction with two-factor authentication (using a separate device or card held by the user) provides a much more robust defence. The customer has to verify that all the details of every transaction are correct, including for example the payee name, account number and, amount of a payment, before it can be executed.

A number of banks have recently issued chip card readers to their customer to implement two-factor authentication and protect against phishing attacks. These devices can also be used to provide transaction authentication. However, the transaction details must be manually re-entered by the customer (with only numeric keys available), greatly restraining what is authenticated, and so opening up vulnerability to attack. Also, requiring customers to re-enter all significant transaction details is error prone and harms usability.

A more usable and versatile method of delivering strong transaction authentication can be found in solutions such as Cronto's 'Visual Cryptogram', where visual signing using the camera in the customer's mobile phone or a dedicated optical token removes the need for awkward authenticators and time consuming re-keying of challenge codes or transaction details. The larger capacity allows more transaction details to be authenticated, and these can be changed rapidly, in response to adaptation in criminal behaviour.

"A new form of man-in-the-middle attack, called **"man-in-the-browser"** has surfaced. These attacks can bypass current browser security mechanisms to read, insert, and modify transaction data... So, what should enterprises do to protect themselves against this new threat? ... A longer-term solution lies in **transaction verification**. Organizations that do business online should re-evaluate their solution road maps and incorporate transaction verification as a core component of their overall security strategy."
Forrester Research, 2007