Phishing Email Downloaded Malware that Hijacked a Link to the Bank's Website

This attack involves receiving a phishing email which contains an infected attachment. For example, these emails would often include words such as "invoice" in the subject field and an attachment also titled "invoice". Opening the attachment installs malware onto the computer. This malware provides the criminals with access to the system. With this access the criminals can then employ many methods of gaining access to confidential information.

In one case the criminals "hijacked" a link on the system to the online banking website. When the solicitor tried to access his online banking facility by clicking on this link they were directed to what appeared to be the bank's genuine site. However, this was not the case, as the criminals had redirected them to their fraudulent site.

Each time the solicitor entered their login details they were returned to the same page, rather than gaining access to the accounts. The solicitor contacted their bank and was advised to delete their browsing history, log off and wait a period before logging back on. The solicitor followed these instructions and what appeared to be an authentic bank message appeared stating that as a routine security measure that they should enter the code provided by their cardreader, the device required to authorise payments, and press continue. The solicitor did this, assuming that they had been locked out of the accounts due to the number of failed attempts, but still did not gain access to the accounts.

It transpired that while the solicitor was attempting to log in to the accounts the fraudsters had used the login details to access the genuine accounts and set up transfers to their own accounts. By entering the code from the cardreader the solicitor was authorising substantial payments from the client account.

Precautions Specific to this Type of Attack

Ensure your anti-virus software is fully up-to-date and set to automatically update.

Be skeptical of any attachments received in an email, particularly from an unknown source. If in doubt, do not open the attachment.

Be wary of "failed" attempts to log in to your bank account. Contact your bank and express your concerns to them.

Always check the website address in the address bar to ensure you are on the bank's genuine site. The site will include a "lock" symbol to show that it is genuine.