

ONLINE BANKING SECURITY 101: UNDERSTANDING YOUR RISKS

With millions of Europeans now banking online, there is very real concern over the security of these transactions. According to the latest Unisys Security Index which tracks consumer security concerns, 85 percent expressed worries over bank card fraud and identity theft, with 75 percent of Britons indicating they would not use a bank they cannot trust to safeguard their personal information.

Such fears over online banking security are not unfounded. Recently, in September, British police arrested a 19-person gang charged with stealing £6 million from London banks in just three months utilizing a variant of the ZeuS virus. On October 13, the Association of Dutch Banks (Nederlandse Vereniging van Banken) released figures indicating € 4.3 million in losses involving online banking fraud during the first 6 months of 2010 compared to € 1.9 million in 2009.

Yet, while the threat is real, the methods online banking thieves employ remain confusing to most people. According to the same Unisys Index, the majority of consumers limit access to personal information on user-friendly social media sites, but 39 percent admitted they rarely consider privacy protection when banking online. This article explains the methods most commonly used by online thieves.

Simple Web Use Leaves Users Vulnerable

Most hacking tools which allow criminals to gain access to bank accounts are circulated throughout the web, and are downloaded and executed on PCs while the user is simply web surfing or opening an e-mail. These hacking tools can easily capture the password, account number, and personal data which the user is inputting. They are even capable of replacing the input screen that the user is watching with a counterfeit website of the bank installed by a hacker in advance.

Attack Method #1: Bypassing Anti-Virus and Anti-Malware Programs

Anti-Virus and Anti-Malware programs are signature based meaning they work by detecting known threats. However, malicious codes which bypass these programs are rampant across the web. For example, the much publicized ZeuS virus, contains a technology that avoids Anti-Malware software, and is constantly spreading via new breeds and variants through famous web sites, fake web sites, phishing sites, and e-mail, with users completely unaware their PCs are infected.

Attack Method #2: Capturing Personal Data Input

Considered the main attack vector threatening the safety of online banking, account information stolen during input stages of the online banking process are transmitted to the hacker along with a screen image that has also been captured. When users access an online banking service, they must input a value for personal identity authentication such as an ID, PIN, and password. When the user presses the keyboard, the input signals are transmitted through the port connected to the keyboard, a number of other devices, and the keyboard driver to reach the program. Hackers capture user data during this process through key logging techniques, and as of late, polling and hooking method attacks on the port level.

Attack Method #3: Redirecting to Counterfeit Sites

Man-in-the-Browser Attacks redirect users to counterfeit sites with the intention of stealing user credentials. With a hacking tool installed on the user's PC in advance, users are shown a fake online banking site made by modifying the user's host file, or the user's online banking session is intercepted and credentials stolen by covering the user's web site through HTML Injection with a counterfeit site to be filled with account information. In the end, the user inputs account transaction information on the counterfeit web page, and the information inputted is transferred to the hacker – and then transmitted to the bank web site leaving the user unaware of the security compromise.

Attack Method #4: Exploiting Wi-Fi Environments

While nearly all banking websites use SSL (128 bit or higher) encrypted communications, SSL is unproven in Wi-Fi environments. For example, thieves could conceivably employ a Man-In-The-Middle attack exploiting the vulnerabilities of a Wi-Fi environment via ARP and DNS spoofing methods which direct users to a fake online banking site. The attacker then could bypass the 128 encryption by intercepting the SSL packet, with a packet sniffing tool such as Ethereal, which later would be decoded using a fake certificate and SSL Dump tool.

Staying Ahead of Online Banking Thieves

European and international banks have traditionally lagged behind their counterparts in the US and Asia in online banking security. However, with increased consumer concern, European banks are turning to security companies, sometimes based outside of Europe, to provide better protection from online threats.

For example, AhnLab, Inc., South Korea-based security solution provider, recently announced that the Korea operations of Citibank has joined a client roster which includes many of the world's most famous banks including Citicorp Banamex and Banco Santander, the largest bank in the Eurozone, since 2007. AhnLab offers the AhnLab Online Security (AOS), real-time internet banking protection and prevention security solution effective against an array of malicious hacking tools including Zeus.

AhnLab's AOS solution integrates a multi-facted approach to block the multi-facted attacks of hackers. The four major technologies of AOS include: AOS Anti-keylogger, which applies keyboard inputting security technology; AOS Secure Browser, a web browser dedicated to security; AOS Anti-virus/spyware', and AOS Firewall dedicated to blocking hacking tools and network security. More information on AOS and whitepaper can be found at <http://aos.ahnlab.com>.

While the threat posed by online thieves will never be entirely eliminated, the hope of European banks is that they can substantially cut down on attacks through a proactive approach.

Media Contact:

AhnLab, Inc.

Corporate Communications

Changmin Song

+82.2.2186.7955

seemefly@ahnlab.com