ASA

Risk Consultants

Research Note

The Mobile Banking Phenomenon

By: Devin Luco

Keywords: Online Banking, Mobile Banking, Mobile Malware, Smartphones, Third-party Mobile Applications

Abstract – This research note discusses the rising trend in mobile banking, the risks that mobile users should be aware of and how to securely use mobile banking.

ASA

Risk Consultants

Introduction

In terms of speed, storage and bandwidth, mobile smartphones are exponentially more powerful than our earliest personal computers. This should not be surprising due to theories, such as Moore's Law, that have predicted trends of this nature to continue as our technology advances. Maybe the most astounding part of smartphones is not in its power, but in its size. The devices that we now use for everyday computing tasks, tasks that once required a personal desktop computer, are handheld and mobile. Our daily casual Internet browses, information searches, social media interactions, gaming, shopping and banking can be conveniently completed through our smartphones while on-the-go. In fact, mobile Internet usage is projected to exceed Internet usage from desktop computers by 2014.[1] Companies are beginning to understand this trend and adjust business models accordingly to cater to the needs of the changing consumer.

Mobile Banking

Financial institutions, which historically have conducted face-to-face transactions for retail banking, are becoming flexible and finding new ways to appeal to the mobile consumer. Deposits, transfers, payments and account information requests can all be fulfilled through

mobile applications available in an application store, such as Apple's App Store or Android's Marketplace. In addition, less complicated tasks such as requesting a balance or finding a local ATM can be completed through Text and SMS Banking. There are also third-party applications that may be linked to an individual's bank account for payment services. Third-party applications, such as Venmo, are used for mobile payment services to friends and families.[2] Although the concept of mobile banking is fairly recent, there are more users now than a year ago. According to a March 2013 Federal Reserve report, 48 percent of smartphone users, as of November 2012, said they have used mobile banking within the past 12 months.[3] This is an increase from the 42 percent in December 2011.[4] According to the report, 87 percent checked an account balance or transaction, 53 percent transferred funds and 21 percent deposited a check.[5] While the usage of mobile banking is increasing, it is important to note that there are a large number of users that still do not use their phones for banking. Despite the convenience, mobile banking also brings inherent risks.

Risks of Mobile Banking

It is hard to deny the benefits of mobile banking. The fact that mobile banking still has lots of room to grow, in terms of customer

base, brings the question: Why are there so many people still not using mobile banking? Could the risks outweigh the benefits? Is mobile banking truly riskier than traditional online banking? Certainly there are end-user risks that are not necessarily there with personal computers. According to a study by Morgan Stanley, 91 percent of those surveyed said that they have their cell phones within an arm's reach 24 hours a day.[6] Smartphones are carried with individuals at all times, which means the chances that the device is lost or stolen is much greater than losing a computer. Whenever a personal device falls into the wrong hands, privacy of the victim is in jeopardy. Unless the data on the phone is encrypted or password protected, the information can be retrieved fairly easily. Nevertheless, most banks usually do not store login credentials in browsers or mobile applications without the users' permission. Unless the user stored credentials on the device, the unauthorized person will most likely not be able to access any banking information. However, if a phone is lost or stolen, the unauthorized person will have access to everything on the phone, including text messages, contacts and other non-protected applications. This means that if your banking protection (login, password, etc) is weak then sophisticated hackers may be able to find a way to break into your

accounts. This can be alleviated through the use of additional authentications (locked phones, passwords to use applications) and stronger passwords.

Other threats to mobile banking include remote hackers and malware attacks. The danger of malware attacks stems from lack of awareness. Mobile devices are similar to computers in the sense that they also can be infected with viruses or malicious code. Usually this is from users not being as careful as they would be on a personal computer. Users should exercise caution when accessing their banking information through smartphones. Trusted anti-virus and spyware software should also be installed on mobile devices to protect against malware. Malware can also infect a mobile device through third-party applications. It is not uncommon for users to download applications that they may think are safe, such as games or utilities, but end up being Trojans. In 2011, Google removed several malicious applications that Symantec estimated to have been downloaded between 50,000 and 200,000 times.[7] The type of infection that can result from mobile malware includes: activity monitoring, data retrieval, system modification and unauthorized connectivity.[8] If a user is sending sensitive text messages, storing sensitive information or accessing

mobile banking through an infected smartphone, the hacker can gain all of this information for mischievous purposes. It is important to conduct extensive research of third-party applications before downloading them onto your device. Cross check reviews and look online to make sure the application is safe to download. Mobile banking applications from your financial institution are usually safe. Applications offered by financial institutions create a direct connection between the user and the bank without the need of a middle-man (third-party application or browser).[9] This gives financial institutions more control over the security and can offer a number of options that will add to the user's privacy. Financial institutions can implement further protections such as secure sockets layer (SSL) encryption, multiple authentications and remote data wiping.[10] However, when a malicious application is downloaded it can greatly affect a customer's mobile banking experience as credentials can be stolen regardless of how secure the financial institution's application may be.

Conclusion

As more users continue to use mobile devices for everyday tasks, including mobile banking, the security threats will become more advanced and prevalent on mobile devices. Traditional online banking

has been around for years, which has spawned stronger security measures to mitigate the vast amounts of Internet threats. While mobile banking is still in its infancy stages, protection against unauthorized users and malware attacks is still dependent on the users. Protection can be achieved through awareness and caution when downloading third-party applications. It is never a good idea to store sensitive information onto your mobile device or browsers. Additional precautions should be taken in the event the mobile device is lost or stolen. Furthermore, remote data wipes can control the damage if an unauthorized person gains access to the device. In any case, the risks of mobile banking can be mitigated if the user is cautious and aware.

ASA

Risk Consultants

References

[1] Richmond, Holly. "The Growth of Mobile Marketing and Tagging." *Microsoft Tag*. 21 Mar 2011. Web. 8 Jun 2013. <http://tag.microsoft.com/community/blog/t/the_growth_of_mobile_marketing_and_tagging.aspx>

[2] Wortham, Jenna. "After 2 Years of Testing, Venmo Opens Payment Service to Public." *NYTimes.com*. 20 Mar 2012. Web. 8 Jun 2013. <http://bits.blogs.nytimes.com/2012/03/20/after-2-years-in-beta-venmo-opens-payment-service-to-public/>

[3] Geffner, Marcie. "More people using mobile banking." *Bankrate.com*. 5 Apr 2013. Web. 8 Jun 2013. <http://www.bankrate.com/financing/banking/more-people-using-mobile-banking/>

[4] Geffner, n. pag.

[5] Geffner, n. pag.

[6] Daffern, Pete. "Mobile Banking Is More Secure Than Online Banking." *BusinessWeek*. Feb 2012. Web. 8 Jun 2013. <http://www.businessweek.com/debateroom/archives/2012/02/mobile_banking_is_more_secure_than_online_banking.html - share>

[7] Claburn, Thomas. "Google Removes Malicious Android Apps." *InformationWeek Security*. 2 Mar 2011. Web. 9 Nov 2012. <http://www.informationweek.com/security/vulnerabilities/google-removes-maliciousandroid-apps/229300051>

[8] Glynn, Fergal. "Mobile Security: Prevent Mobile Application Code Security Risks." *Veracode*. Web. 8 Jun 2013. <http://www.veracode.com/security/mobile-code-security>

[9] Matthews, Tim. "Don't Be Afraid of Mobile Banking Apps." *Bank Systems and Technology*. 5 Sept 2012. Web. 8 Jun 2013. <http://www.banktech.com/channels/dont-be-afraid-of-mobile-banking-apps/240006734>

[10] Matthews, n. pag.