International Journal of Multidisciplinary Research and Development

IJMRD 2015; 2(2): 448-451
www.allsubjectjournal.com
Impact factor: 3.672
Received: 03-02-2015
Accepted: 18-02-2015
E-ISSN: 2349-4182
P-ISSN: 2349-5979

Sheel Ghule
Persistent Systems Limited, Nagpur

Correspondence:
Sheel Ghule
Persistent Systems Limited, Nagpur

Mobile Banking: Security Measures

Sheel Ghule

Abstract
The banking industry has never seen such a fundamental change as mobile banking. Globally, millions of consumers are already using a wide array of mobile devices to conduct banking - and millions more are expected to go mobile in the coming months. But with that growth come a whole new set of threats: mobile malware, third-party apps, unsecured Wi-Fi networks, risky consumer behavior. And it does not matter whether an institution uses a proprietary or third-party mobile banking application - the bank owns the risks. New security measures are available to mitigate the risks associated with advanced mobile banking and payment capabilities. The key to protecting the mobile channel is to realize that it is deeply connected to the online channel. Effective protection must consider risk indicators that span both channels and extend to both to protect against the full range of attack vectors. So, how do banking/security leaders mitigate their risks and protect their customers from evolving mobile threats?

Keywords: Risk Identification, risk mitigation, Malware, SMS, SSL/TLS, Wi-Fi.

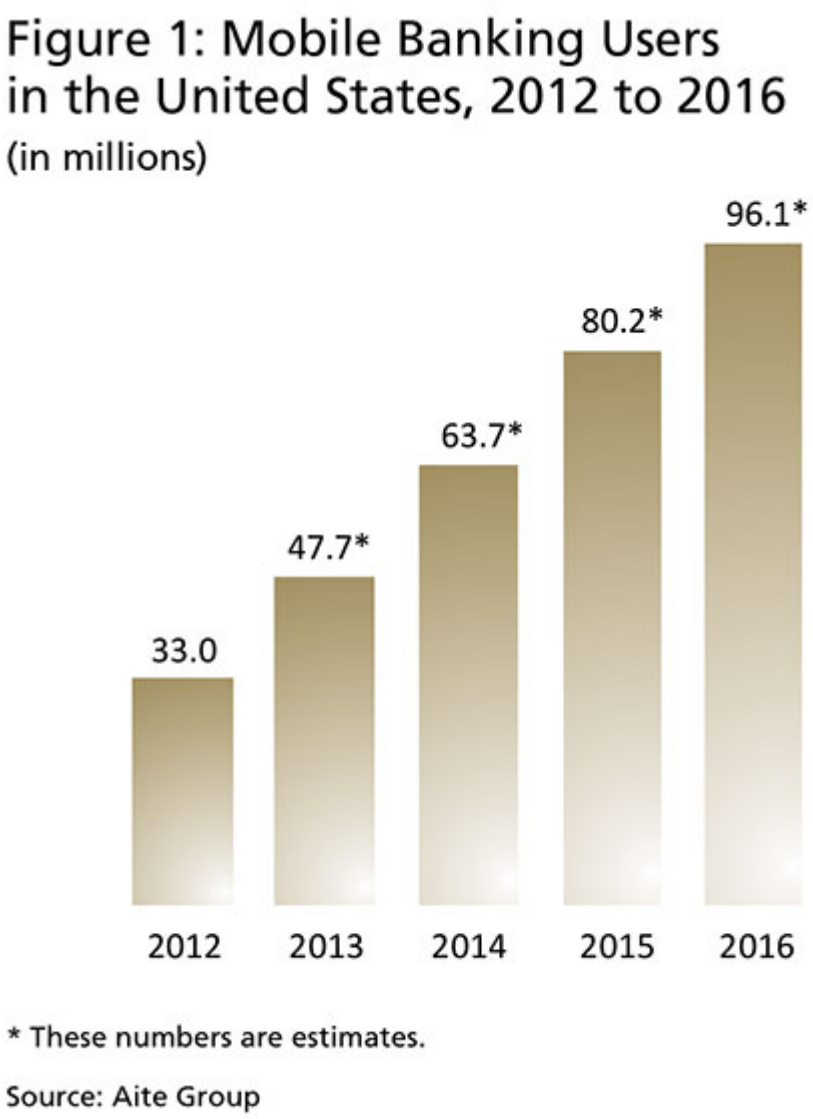
1.0 Introduction
Mobile banking continues to gain momentum, growing faster than any other delivery channel to date. Many financial institutions want to expand capabilities in the mobile channel, but are concerned about security. Given the evolving threats, mobile innovation has outpaced the industry's appetite for deploying new capabilities. Mobile devices — smartphones and tablets — are easy to use and can be taken almost anywhere. They provide users with easy access to personal and financial data via applications that allow the movement and storage of data locally on the devices and/or allow data to be sent to and stored with a third party. But they can also be lost or stolen, infected with malware, and used as a vehicle for fraud. Even so, smartphones and tablets are here to stay. The way consumers use them may change over time, but it is clear that mobile banking via smartphones and tablets is on trend to grow rapidly in the coming years. The mobile threat landscape is ever-evolving, and institutions and consumers alike are wary of the risks. Among today's growing concerns:

- Mobile Malware - Trojans, viruses and rootkits migrating from traditional online banking and designed specifically for the mobile marketplace. Researchers see an increase in mobile malware development - in pace with market growth.
- Third-Party Apps - Consumers love their smart phone and tablet applications, but often these apps come from third parties with questionable security practices. Or worse, the apps are created by fraudsters and loaded with malware.
- Unsecured Wi-Fi - The unsecured wireless network is a toll-free highway for fraudsters to gain access to mobile devices, either to seize control of or gain access to account information.
- User Behavior - Consumers are prone to download third-party apps, use unsecured wireless networks, open and click links in SMS text messages and e-mails, and lose their mobile devices. Mobile-use behavior is creating a suite of vulnerabilities, and fraudsters are eager to take advantage.

While mobile banking and payments are still relatively young in the U.S, adoption is more mature in international markets such as Asia.

Mobile Banking Users:
Mobile device software provider Malauzai Software, Inc, released data on August 14, 2013, that confirmed the growing use of mobile banking applications. The report indicated that "For banks and credit unions that have been live a minimum of 12 months, the average month-over-month growth rate is 4.19 percent. The best in class number is 11.56 percent,

with several banks and credit unions topping 10 percent. Organic growth is strong and can be attributed to the general growth of mobile smart phone handsets as well as these financial institutions making mobile part of all of their marketing campaigns."1 In another report based on a 2012 survey of 1,115 U.S. consumers, the Aite Group forecasted that the number of mobile banking users would continue to grow significantly, as shown in Figure 1.



Many community banks recognize the value of mobile banking — it provides them with avenues and opportunities to reach geographically remote or rural markets, to focus on new markets, to innovate, to overcome infrastructure limitations and improve efficiency, to access payment systems, or even simply to retain market share. However, the rapid growth of mobile banking introduces security risk and privacy issues that must be managed. It is critical that banks anticipate and recognize risk in order to protect customers and their own reputation. This article reviews mobile banking risks and risk mitigation solutions, discusses regulatory guidance, and suggests ways to implement mobile banking risk assessment and ongoing risk management strategies at community banks.

Mobile Banking Risk Identification

Providing consumers with the ability to transact banking business using a mobile device — with security settings of the customer's choosing — places an increasing amount of control over sensitive financial data into consumers' hands. The net loss of control over this information makes it more difficult for the bank to assess risks and implement effective risk mitigation strategies.

To understand mobile banking risk, it is important to understand the three most common delivery channels (many institutions offer all three channels to reach the greatest number of customers):

- Text messaging/short message service (SMS)
- Mobile-enabled Internet browser
- Mobile applications

Text Messaging/SMS

SMS, commonly referred to as "texting," is limited in the number of characters used. It is most often used as an alert and inquiry delivery channel. SMS is used to make mobile banking available to users of older cell phones that do not have web browsers or applications. SMS messages are sent in cleartext over widely used telecommunications networks,

with no encryption capabilities. Also, the customer's account identifier is stored in an SMS message, which means that there is the possibility of misuse if the phone is lost or stolen. SMS mobile banking users can also be susceptible to receiving misleading or socially engineered messages that could prompt them to reveal account information. Because of the limited utility of older cell phones and the growth of smartphones, the use of SMS for mobile banking is fading.

Mobile-Enabled Internet Browser

Mobile Internet banking via a mobile-enabled Internet browser is an extension of the online banking channel. Customers can navigate to a website on a smartphone or tablet via the embedded browser in much the same way that they can access a site from a personal computer. Although banking from a mobile device using a mobile-enabled Internet browser is open to the same vulnerabilities as banking from a personal computer, it is usually harder to see and use security features on a mobile device.

Mobile Applications

Mobile application banking uses a custom-designed software application installed on a smartphone or tablet that provides for a more user-friendly interface than is possible with either SMS or mobile browser-based banking. As such, this is the fastest growing delivery channel for mobile banking. However, this channel introduces risks that may arise if third parties write the code for these applications, as well as the possibility that the applications can be compromised if customers install rogue, corrupted, or malicious software.

The storage of customer data on a phone or tablet presents the opportunity for misuse if the device is lost or stolen. In addition, likely attacks against mobile banking include fraudulent requests (e.g, phishing e-mails or SMS messages) that appear to require the installation of a new application or security feature from a bank, or malware that can steal credentials by prompting users to type an account number and password.

Mobile Malware Can Make Online Banking Risky Business

This is how it’s happening: Banks using two-factor authentication require customers to log into their online accounts using their user name, password and a mobile transaction number sent to their device via a text message. This two-step verification process is supposed to add an extra layer of online security for customers. But cyber crooks have figured out a way to defeat it. McAfee Labs identified four new types of mobile malware used to capture banking logins and passwords. Once that happens, the malware intercepts SMS messages containing account login credentials in real time. That allows hackers to access consumers’ accounts and transfer their funds. Back in 2005, computer security specialist and writer Bruce Schneier predicted that attackers would find a way around multi-factor authentication. In his essay, The Failure of Two-Factor Authentication, he said the way they would do it is with tools that attack transactions in real time – namely “man-in-middle attacks and Trojan attacks against the client endpoint.” The only thing that would change over time, said Schneier, is how cybercriminals would do it: “Two-factor authentication will force criminals to modify their tactics, that's all.”

Suggested risk mitigation solutions

- **Identify and protect sensitive data on the mobile device.** Store sensitive financial and consumer data on another computer instead of on the mobile device. If data are stored on the device, use strong encryption technology provided by a trusted source.
- **Ensure that sensitive data are protected while in transit.** Assume nothing is secure. Mobile banking applications should enforce the use of an end-to-end secure channel such as secure sockets layer/transport layer security (SSL/TLS) and use strong encryption.
- **Implement user authentication, authorization, and session management correctly.** Require appropriate-strength user authentication, for example, multifactor versus strong authentication. Physical tokens or voice, fingerprint, or behavioral authentication factors may be appropriate.
- **Secure data integration with third-party services and applications.** Ensure that mobile banking applications and code are tested, come from a reliable source, have supported maintenance, and have no back-end malware (for example, Trojans).

General guidelines for the highest level of mobile banking safety

- Avoid making your personal information readily accessible. Don't share your PIN, password or security question with anyone or save it on your phone.
- Password-protect your phone so others cannot access your information if it is lost or stolen.
- Call your bank immediately if your phone is lost or stolen and change all account passwords from a computer as soon as possible.
- Monitor your records and accounts on a regular basis.
- Make sure your device’s operating systems and applications are up to date and its security settings and software are enabled.
- Disable features that allow your phone to automatically connect to new WiFi networks or Bluetooth devices.

Mobile banking security tips when using SMS

SMS, or short message service, can send out convenient text message alerts when your balance is getting low or you're approaching your credit limit. To increase your mobile banking security while using SMS, remember not to ever share personal information over a text message. It should raise a red flag if anyone asks for it via text message as banks will never ask for this information.

Mobile banking safety when using a mobile web browser

With Smartphones becoming more popular, many people are using mobile web browsers to handle their banking. These web browsers do have some built in features, like standard site encryption, to protect your mobile banking security. For added mobile banking security follow the tips below:

- Log out and close your browser when you are not using the internet on your phone
- Set up daily alerts to track account activity. This is a great way to detect fraudulent activity on your account.
- Use secure, encrypted websites for transactions on your mobile phone
- Don't click through to websites from emails, even if they look like they are from your bank. Always visit your bank's website by typing in the domain, or bookmark it.
- Never give your password or account number on a site you are unsure about
- Avoid public Wi-Fi, if possible

Enjoy mobile banking security with a mobile banking app

- Using a mobile banking app may be the safest way to access your checking account from a mobile phone. These applications link directly to your banks computers, often making them faster, and the interface is easier to use. And since the bank designed the mobile banking app, they will have taken extra precautions to ensure proper security measures are implemented.
- Most mobile banking apps are resilient to phishing (a way for a third party to obtain your sensitive information by posing as your bank) since there is no browser, but there are additional mobile banking safety measures you can take to further protect yourself.
- Log out of the application when you're not using it
- Add mobile security software to your device, if possible
- Don't accept any connection requests if you are unsure about the device wanting to contact you.
- Be careful when opening MMS. MMS can also be used to distribute malicious code. Always delete any MMS from unknown senders immediately.
- Switch off «automatic call acceptance», as this can be exploited to establish a connection without your knowledge.

Conclusion

Whether it is because of demand from customers or a desire to enter new markets, many community banks are beginning to offer mobile financial services to their customers. As with all new products, bankers need to understand the mobile banking environment being used and the associated risks. Effective risk identification and implementation of mitigation controls and processes based on the data type, state, and location are key to achieving this objective. With the proper strategy and risk management elements in place, both the bank and its customers should experience a safer mobile banking environment

References

1. http://www.bankinfosecurity.in/webinars/mobile-banking-emerging-threats-vulnerabilities-counter-measures-w-285
2. http://www.citizensbank.com/checking/mobile-banking-security-tips.aspx
3. http://www.computerworld.com/article/2487497/mobile-security/security-analysis-of-mobile-banking-apps-reveals-significant-weaknesses.html
4. http://research.microsoft.com/apps/pubs/default.aspx?id=132349
5. Malauzai Software, Inc, "Monkey Insights: Mobile Banking Smart Device Usage," August 2013, available at malauzai.com/docs/monkeyinsights_0813.pdf.
6. “Indian Banking Sector”, Banking Sector report by JM Financial dated Aug 2008
7. http://www.privatewifi.com/report-finds-malware-attacks-are-defeating-online-banking-security-measures/