



## The Convenience and Dangers of Mobile Banking

By Marv Chen and Kevin Tsuei, AuditOne LLC

According to consumer data measurement firm The Nielson Company, global shipments for smartphones were up 74.4% in 2010 to 302.6 million. As of May 2011, 55% of recently acquired phones were smartphones.

There are benefits to implementing mobile banking. Mobile applications ("apps") can allow customers to locate ATMs and branches, view the bank's telephone directory, view account balances and transaction history, and transfer funds between accounts (both intra and inter-bank). Customizing the mobile app unifies the look and feel of the application across different makes of smartphones – it wouldn't suffer the display variations associated with the implementation of mobile browsers across different models of phones. Additionally, for non-smartphone users, text messaging can provide functionality such as balance inquiries and recent transaction history. Since the phone must first be enrolled with the bank in the system, text messaging does not require a login; obtaining something as simple as an account balance would only require sending a text message to the bank. The entire process would take less than 10 seconds, much less than the two minutes or more that a mobile browser would require.

However, with these benefits come risks. Mobile phones do not have the level of physical and logical access protection afforded by computers. Computers are located inside customers' homes or offices, where mobile phones are more easily lost or stolen. They can sometimes be "borrowed." Users typically don't lock their mobile phones with a password or lock pattern. Account numbers are often not masked in the browser. These risks are exacerbated for customers with online cash management capabilities, such as bill payment, ACH and wire origination, because customers' usernames and passwords on the mobile banking platform are almost always the same as those on the Internet banking platform.

An additional security consideration is that malicious software on smartphones is an emerging threat. Google recently (in June 2011) pulled malware-infected apps from its Android Market. At the 2010 Black Hat Conference, Nicolas Seriot demonstrated a proof-of-concept of how easy it was to spread malware through the AppStore and obtain data such as browser history, last GPS position, keyboard cache, email, etc. Unfortunately, smartphones typically do not have anti-virus protection. Anti-virus applications for smartphones are in their infancy, and there are few (if any) smartphone-oriented comparisons that would measure the effectiveness of anti-virus programs.

Fortunately, there are ways for us to mitigate risk. Although intended for the more traditional desktop browser-based platforms, the updated guidance released by the FFIEC on June 29, 2011 – *Supplement to Authentication in an Internet Banking Environment* – suggests some methods. For high-risk activities such as funds transfer, users can employ multi-factor authentication in combination with out-of-band transaction verification. Also, it is advisable that banks implement a customer awareness program advising customers to password or pattern-lock their phones, be vigilant when downloading mobile apps, and configure the mobile browser to not remember usernames and passwords.

Other methods may be used to force the mobile browser to redirect the customer to a

dedicated mobile banking website with a limited subset of features, e.g. masked account numbers, funds transfer and bill payment only with existing payees, disabled ability to add new payees, etc.

In closing, what we must do is maintain vigilance and regularly re-assess the risks associated with mobile banking. Because mobile banking is relatively new, the threat landscape, as well as technologies and methods used to reduce the risks, are likely to rapidly evolve in the next few years, if not months.

[<back to September 2011 Technology & Security Digest>](#)

*Marv Chen is Technology Practice Director for AuditOne ([www.audit-one.com](http://www.audit-one.com)). He can be reached at [Marv.Chen@audit-one.com](mailto:Marv.Chen@audit-one.com). Kevin Tsuei is an IT Auditor at AuditOne. He can be reached at [Kevin.Tsuei@audit-one.com](mailto:Kevin.Tsuei@audit-one.com).*