Digital banking security: The infinite loop

S. Sundararajan, Managing Director, i-exceed Technology Solutions

These days, people visit a bank's branch a lot less often than they used to. Advancements in technology have now made it possible to extend a bank's operations beyond the branch and its working hours. Furthermore, the growing numbers of mobile internet users has resulted in more people adopting digital banking due to the convenience, user friendliness, and cost effectiveness it offers. However, the increasing transactional volumes also emphasise on the need for constant evolution of security measures to prevent security breaches and fraud, feels **S. Sundararajan**.

Understanding the nature of threats

Most banks today have robust security measures in place. However, a lot of it still boils down to customers adopting the best practices to avoid misuse or fraud. The digital space is teeming with threats like viruses, Trojans, phishing attacks, worms, etc., and it's important to understand how each of them work. Every attack focuses on a specific set of information to corrupt or compromise a user's privacy.

Each threat works in a unique way – while some try to infiltrate customers' bank accounts, others may try to redirect them to a fake website to steal their login credentials (phishing). Some could initiate a fund transfer without customer's knowledge, while others could try to gain control over customer's computer to steal sensitive data. No matter what method these attacks follow, their sole objective is to steal money and information.

To avoid becoming a victim of these cyber threats, sensitive personal information must be well protected. Customers must remember that banks will never use e-mail or phone calls as a channel of communication to request for sensitive information. If one receives such e-mails allegedly from the bank, it must be reported immediately without reacting to the contents of that e-mail.

To prevent oneself from phishing attacks, one must get accustomed with bank's security measures. If there has been a change in security measures or website design, banks will usually send out notices to their customers to inform them of the change in and such changes will never be done overnight. If one finds that the website's authentication process looks different from what it used to be, they should check the website for other details by which they

can verify its authenticity. A customer should also, if possible, refrain from accessing their banking information on a public or shared computer because there are several spywares in the market designed to steal sensitive information by recording key strokes. Even while accessing the banking website on one's own computer, one must always log off and clear the cache on the browser regularly to remove any transactional records.

Current Security Measures

To protect customers' accounts, most banks today have taken measures to ensure that the identity of the account holder is properly authenticated before granting access to their bank accounts online. One of the measures includes the use of a complex password (a combination of upper case, lower case, numbers, and special characters), and a second authentication process where a one-time PIN (OTP) is sent via SMS to the registered mobile device. So the password becomes the information that an account holder knows, and the PIN is the information sent to their personal device. This ensures that only the account holder who holds both pieces of information is given access.

Banking websites also implement encryption at multiple levels to ensure that data moving through the network cannot be deciphered by a third party. Many banks also allow their customers to set financial limits to the funds that may be transferred through online funds transfer as a contingency measure to minimize losses in the unfortunate event of a compromised account. SMS' are sent to the account holder for every transaction carried out, along with an alert if a transaction for an amount beyond the set limit has been initiated.

Recent Trends

The recent advancements in emerging technologies could enable new modes of more secure authentication without impacting customer experience. These advancements leverage the inherent capabilities of smartphones to introduce a third factor of identity verification. In three-factor authentication, in addition to furnishing their regular password and an OTP that appears on their token or mobile phone, users will be asked to present something that they possess, which would irrefutably prove their identity. This third factor could be captured using either an application that is installed on the customers' smartphones or an inbuilt feature or capability of the device.

Some examples of the third factor include fingerprint reading, retinal scanning, and voice recognition. There are other possibilities of biometric authentication as well, such as capturing words spoken by customers through their phone and matching them against a previously authenticated sample of voice that exists in the bank's records, or asking them to take a photograph or retinal scan with their smartphone's camera and send it to the bank for approval and authorisation.

It is also possible for banks to perform a three-stage authentication process for customers who don't own a smartphone, by providing them a sensor

module that can be plugged to bank agent's device that is capable of capturing and transmitting the biometric information.

Conclusion

Sooner or later, every authentication present today will make way for more sophisticated ones. While multi-factor authentication looks like a fool proof solution under the current circumstances, it is also true that this will not deter an attacker completely, but simply slow them down. The implementation of security technology is not a one-time effort with a guarantee of a lifetime. It is an initiative that calls for constant continuous improvement because what looks like cutting-edge today will be standard fare tomorrow and obsolete a few years later.