Risks of digitisation of cash transactions

One of the undisputed benefits of the recent demonetisation exercise has been the concerted push towards digitisation of cash transactions. There has been rapid growth in the use of smart devices, primarily mobile phones.

\n\n

While many welcome the idea of trackable, transparent and frictionless monetary transactions, there are significant risks associated with moving to these systems. In a population that is largely illiterate or technologically naïve, this creates a challenge for policy-makers and system providers alike.

\n\n

Mobile-based systems:

\n\n

There are a number of mobile banking applications that have been developed by major banks for their respective customers to perform transactions that they would normally have conducted over the bank's web-portal.

\n\n

\n

- The Bharat Interface for Money (BHIM) application has been developed by the National Payments Corporation of India (NPCI) to allow any customer of a Universal Payment Interface(UPI)-live bank (like SBI, HDFC, ICICI, etc.) to conduct certain basic transactions such as sending or receiving money.
\n
- While these applications do not (claim to) store any bank-related information on the phone itself, they connect directly to the consumer's bank accounts, which may be a cause for concern.
\n

\n\n

Mobile Wallets:

\n\n

\n

- Mobile wallets on the other hand are applications that act like our physical

wallets but in the digital world.
\n

- We can add money to our wallets from our bank accounts, debit or credit cards and then use these funds for various transactions – be it paying vendors or friends.
\n
- SBI Buddy, Chillr, Paytm, Oxigen, MobiKwik, etc. are examples of mobile wallets.
\n
- The limitation with such wallets is that the vendor and the customer should also be using the same wallet.
\n
- Their advantage over the banking application is that the liability of the consumer is limited to the amount kept in the wallet (just like physical wallets).
\n

\n\n

What are the risks involved?

\n\n

\n

1. **Compromised applications:**
\n

\n\n

\n

- The most plausible vulnerability with payment applications is the presence of other applications on a consumer's mobile phone.
\n
- If a user has an alternative keyboard application, it could be a risk in terms of logging passwords and pins while performing bank transactions.
\n
- It is also possible that a user inadvertently downloads an application while browsing the web that could compromise his/her phone data and transactions.
\n
- With some payment wallets, anyone having casual access to a user's mobile phone could be a vulnerability as application PINs are not set up.
\n

\n\n

\n

2. **Denial of service:**

\n

\n\n

\n

- A vulnerability associated with all forms of payment systems is a denial of service attack on the network as whole.
\n
- This could be at the level of the telephony network via jamming devices or at the server where billions of illegitimate requests could be sent in a short period of time, making it difficult for legitimate transactions to be completed.
\n

\n\n

\n

3. **Man-in-middle vulnerability:**
\n

\n\n

\n

- In this scenario, a hacker gets access to either the servers on the telecom network, the payment wallet or the bank's networks.
\n
- Listening to the communication (despite being encrypted) could still be considered a risk.
\n
- This type of vulnerability could be considered to be more esoteric.
\n
- Hacking of a bank's or NPCI's servers could end up exposing personal details of users, while hacking of a mobile (GSM) network (A5/1 encryption has known vulnerabilities) could expose all communication, especially the USSD-based transactions.
\n

\n\n

What are the steps that can minimise the risks?

\n\n

There are trade-offs between convenience and security. While it is impossible to eliminate all vulnerabilities and risks, there are some simple steps that users, payment system providers, banks and governments could take to minimise their risks while using payment systems.

\n\n

\n

- Users need to carefully protect their mobile devices from unauthorised access.
  \n
- In the least, one should have a PIN to lock the phone.
  \n
- A biometrics-based locking/unlocking system would most secure as of now.
  \n
- PIN access for applications — especially for banking applications or digital wallets would be another layer of protection.
  \n
- Payment systems should ensure that their systems are continually audited for security vulnerabilities and patched frequently.
  \n
- Systems should be hosted with active measures to mitigate denial of service attacks, while also maintaining flexibility to handle seasonal upsurges in traffic.
  \n
- While the government has put its weight behind the concept of a cashless economy, it needs to invest sufficiently in securing the network as well as educating the population on how to avoid becoming a victim of fraud.
  \n
- There should be a robust training programme, especially focusing on the old and illiterate who will be affected the most by this transition.
  \n
- Lastly, it must revisit laws and establish a special mechanism to ensure that entities stealing data or preventing legitimate digital transactions are dealt with severely and swiftly in a manner apparent to the public.
  \n

\n\n

\n\n

Category: Mains | GS - III | Economics

\n\n

Source: The Hindu

\n