Securing a cashless society

What is the issue?

\n\n

Push towards cashless society via demonetisation in the environment of poor precautions and security policies, leave us vulnerable to cyber-attacks.

\n\n

How good is the cyber-security in India?

\n\n

\n
- Many payment services like PayTM are certified under the Payment Card Industry Data Security Standard (PCI DSS) 2.0 certification.
\n
- It is the current industry security standard set by American Express, Visa International, MasterCard and other international dealers.
\n
- It is an essential certification for companies that store credit card information.
\n
- PayTM and other such companies also use **128-bit encryption technology** to crypt any information transfer between two systems.
\n
- It is nearly impossible to crack a password under 128-bit encryption.
\n

\n\n

What are the problems?

\n\n

\n
- These precautions do not mean that the people are not vulnerable.
\n
- The perpetrators not only try to hack the login credentials.
\n
- They also deploy methods like creating fake mobile applications and spyware that steal information, or social engineering tactics that make you reveal

your login credentials.
\n
- Forums on the Internet are abundant with step-by-step instructions on how to create fake websites that imitate digital payment platforms.
\n
- Apart from login credentials, hackers target other things like the database of the mobile company.
\n
- They use the stolen data for underground sales, identity theft, or targeted personal attacks such as extortion.
\n
- Right after demonetisation, digital payments via various platforms increased on an average of 200%.
\n
- But the speed of technological development and its integration into our economy supersedes the speed of defence mechanisms and protocols to reduce cyber-attacks.
\n
- Even companies like HDFC and ICICI recently experienced cyber-attacks.
\n
- This makes the condition of new users like street vendors, who have been forced into the digital payments due to demonetisation, pitiful.
\n

\n\n

What should be done?

\n\n

Companies, customers, and the government should collectively participate to reduce cyberattacks.

\n\n

Companies

\n\n

\n
1. Increase awareness of the customers about the risks and educate them how to be secure.
\n
2. Employ behaviour analytics and pattern analysis at their fraud prevention departments to predict suspicious behaviour.
\n
3. Be proactive in looking out for any fake apps/websites that duplicates their

service.
\n
4. Monitor discussion boards, social media platforms, and forums that discuss hacking and fraud tactics, and implement measures to prevent such tactics.
\n

\n\n

Government

\n\n

\n
1. Should check if the current policies regulating these platforms are adequate and update them regularly.
\n
2. People must be educated on the risks involved, strict policies must be enforced, and companies accountable for not meeting security standards must be held.
\n
3. Benefits that come from overlooking security precautions must be minimised, and
\n
4. Public-private partnerships on live information sharing about cyberattacks and fraud should be strengthened.
\n

\n\n

Customers

\n\n

\n
1. Should educate themselves about the risks involved and take precautions.
\n
2. Must minimise vulnerability with two-factor authentication and change their password frequently.
\n
3. Must check the authenticity of applications by looking for the number of downloads and read reviews by other users.
\n
4. Must check for other application releases from that developer.
\n
5. Must keep Web browsers updated so they can recognise illegitimate sites easily.
\n

\n\n

\n