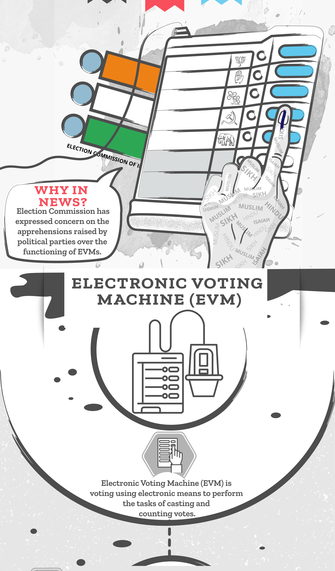
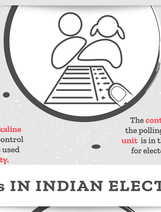
ELECTRONIC VOTING MACHINE (EVM)



WHY IN NEWS?

Election Commission has expressed concern on the apprehensions raised by political parties over the functioning of EVMs.

ELECTRONIC VOTING MACHINE (EVM)



Electronic Voting Machine (EVM) is voting using electronic means to perform the tasks of casting and counting votes.

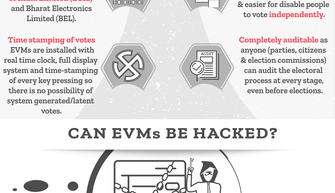
HOW IT WORKS

An EVM consists of a "control unit" and a "balloting unit" joined together by a cable.

It runs on a single alkaline battery fitted in the control unit and can even be used without electricity.

The control unit is kept with the polling officer; the balloting unit is in the voting compartment for electors to cast their votes in secret.

EVMs IN INDIAN ELECTIONS

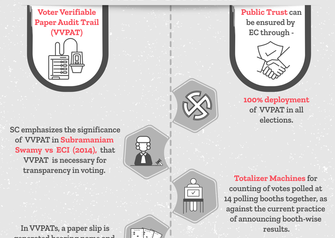


1982 - First time in Kerala Assembly by-election.

1998 - First time in State Legislative Assembly elections

2004 - First time in Lok Sabha elections.

HOW EVMs ENSURE FREE AND FAIR ELECTIONS?



Non-reprogrammable as it consists of an integrated circuit (IC) chip that is one time programmable (software burnt at the time of manufacturing).

Self Diagnostic i.e. shut down automatically in case of post manufacturing tampering.

No external communication because EVMs are not networked by any wireless system, nor do they have any frequency receiver and data decoder.

Standard Operating Procedure i.e. procedural checks and balances, trial run, random allocation, multi-stage testing, safe and secure storage post voting etc.

Secure Source Code as manufactured in-house by Electronics Corporation of India Limited (ECIL) and Bharat Electronics Limited (BEL).

Easy to use & accessible, even by illiterate voters who just need to recognize the symbols of the parties & easier for disable people to vote independently.

Time stamping of votes EVMs are installed with real time clock, full display system and time-stamping of every key pressing so there is no possibility of system generated/latent votes.

Completely auditable as anyone (parties, citizens & election commissions) can audit the electoral process at every stage, even before elections.

CAN EVMs BE HACKED?

For wired hacking - one needs a specifically designed chip that is physically plugged into its control unit or a way to artificially change the processor.

For wireless hacking - one needs a miniaturized transceiver circuit with a small-sized efficient antenna to be externally embedded into the EVM. It is technologically difficult to reduce the size of antennas.

Technically, impossible to hack EVMs as it would require high level of expertise, the blueprint of actual circuit board of the EVM and huge cost.

WAY FORWARD

Voter Verifiable Paper Audit Trail (VVPAT)

Public Trust can be ensured by EC through -

100% deployment of VVPAT in all elections.

SC emphasizes the significance of VVPAT in Subramanian Swamy vs ECI (2014), that VVPAT is necessary for transparency in voting.

Totalizer Machines for counting of votes polled at 14 polling booths together, as against the current practice of announcing booth-wise results.

In VVPATs, a paper slip is generated bearing name and symbol of the candidate along with recording of vote in CU.

In 2017, EC even held an 'EVM Challenge', where it invited political parties to demonstrate/proof any allegations of tampering

VVPATs are an "independent verification system" designed to allow voters to verify that their votes were cast correctly and provide a means to audit the stored results in case of disputes.