03

SPECIAL ISSUE
GENERAL ELECTION
2019

Chief Information Security Officer

# ECI CYBER BULLETIN

Election Commission of India

OCTOBER 2019


## THIS ISSUE



## ASSEMBLY ELECTIONS

**For the Upcoming Assembly Elections, States have been issued detailed Cyber Security Guidelines which include special audit of all ICT Application hosted by CEO, Cyber hygiene of Electoral Staff and detailed application / Infrastructure level guidelines.**

## SECURITY AUDIT

**On 21st August 2019, ECI has issued instructions to all States / UT Chief Electoral Officer to conduct security audit of all websites / applications. Also re-audit of already hosted application was emphasied.**

**ECI has setup Cyber Security wing at Delhi who will also undertake the internal security audit of all websites/ Applications of ECI across all States / UTs.**

## CYBER SAFE GENERAL ELECTIONS 2019

On 3rd August 2018, a news item was published in Economic Times, Times of India and many leading news channel stating that "After US, Indian elections may be the next target of Russia: Oxford Professor".
ECI took very strong steps to ensure cyber safety in Lok Sabha Election of 2019. ECI brought out clear regulations for Cyber Security and educated entire electoral staff through several workshops. One of the major initiatives which ECI took was to revamp all important but old applications, reduced the number of applications and consolidated them into a few manageable ones.

Secondly, all applications were built with cyber security in design by default. The core principles followed were to reduce the attack surface area, give principle of least privileges, make the principle of defence in depth and by fixing security issues correctly.

Thirdly, all websites were security audited internally by security expert rigorously, even before they got deployed and thereafter third party security audit was performed. Every critical application were scanned frequently after deployment regularly and patched up.

Fourthly, all National Cyber Security agencies were put on high alert and appropriate defence were constructed outside the application approach areas. Finally, each State / UT designated Cyber Security...

***(Continued on Page 4)***

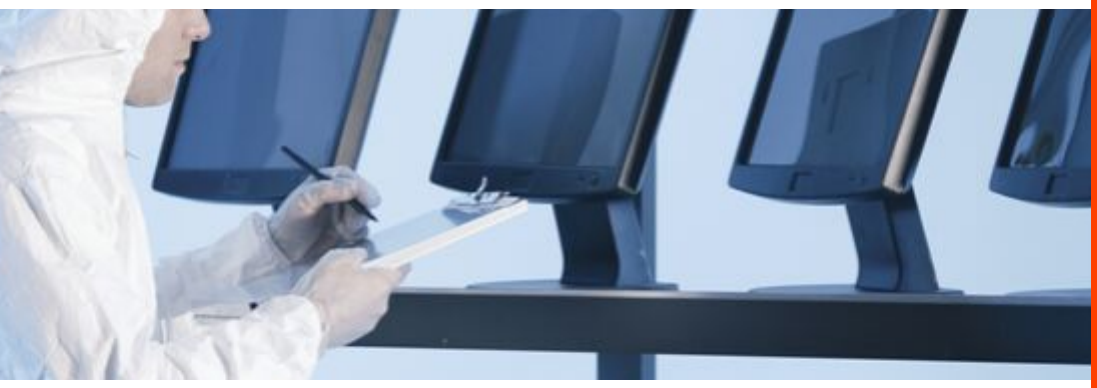
# TRENDS IN CYBER ATTACKS OF ELECTIONS

## TARGETED PHISHING ATTACKS

Phishing is the most common way of stealing information in today's cyber world as gullible users continue to fall for it. The attacks are getting sophisticated day by day with well-crafted emails. A 2018 study showed that there is a 297% increase in retail phishing websites as compared to the previous year.

## USE OF MOBILE DEVICES BY CYBERCRIMINALS

Mobiles allow quick getaways and ubiquity. Cybercriminals are developing customized applications to increase their anonymity to avoid the detection of their identity to make their tracking difficult. There is an average of 82 rouge mobile application identified each day.



## DIGITAL DICTATORSHIPS & INFORMATION WARFARE

Countries are now trying to regulate the digital space. The ICT Systems are now so designed so as to control and coerce citizen, in a gigantic social engineering that some have called as the “gamification of trust”. A society where individuals are under round-the-clock surveillance. A citizen gains or loses “social credit” according to ones behaviour, actions and even thoughts. Citizens can now be tracked with every move and decision, scoring on what one buys, what one vote for and who you see. New technologies might tempt various governments across the world to build unprecedented totalitarian regimes that will monitor and control everyone all the time. Massive surveillance, big data coupled with artificial intelligence is making it ever so easy to monitor and control billions of people and threatening democracies and fundamentals of electoral process.

## 5 CYBER SECURITY TIPS FOR ECI OFFICIALS

### 1. You Are A Target.

Realize that you are an attractive target to hackers. Don’t ever say “It won’t happen to me.”

### 2. Eight Characters Is Not Enough.

**Practice good password management. Use a strong mix of characters, and don’t use the same password for multiple sites. Don’t share your password with others, don’t write it down, and definitely don’t write it on a post-it note attached to your monitor.**

### 3. Lock It Up.

**Never leave your devices unattended. If you need to leave your computer, phone, or tablet for any length of time—no matter how short—lock it up so no one can use it while you’re gone.**

### 4.Practice Safe Clicking

**Always be careful when clicking on attachments or links in email. If it’s unexpected or suspicious for any reason, don’t click on it. Double check the URL of the website the link takes you to: bad actors will often take advantage of spelling mistakes to direct you to a harmful domain.**

### 5. Beware Of Browsing.

**Sensitive browsing, such as banking or shopping, should only be done on a device that belongs to you, on a network that you trust. Whether it’s a friend’s phone, a public computer, or a cafe’s free WiFi —your data could be copied or stolen.**

# TIPS TO PREVENT PHISHING ATTACKS WHILE USING ECI WEBSITES

**P**hishing Attacks impersonate organizations through phishing emails and fake websites. Criminals who engage in phishing attacks seek access to private and sensitive information, like login credentials, credit card details, and personal family details. ECI websites before and during elections include various forms for electoral verification and changes such as Form 1, Form 6, Form 6a, Form 7, Form 8 and Form 8a, etc. This form jacking involves inserting a small piece of malicious code, which is known as spyware or malware, onto a user's system which allows a criminal to grab the user's personal information when they are on a website, and a form appears which asks for personal information such as name, email id and phone number whenever a user submits his/her personal information which is being asked in available form on the website.

## HOW TO SAFELY BROWSE ELECTION WEBSITE

- ECI website ends with ***.eci.gov.in**. Always see that in the address bar before visiting it and for Electoral function the website is nvsp.in.
- The ECI Website has **Secured Socket Layer (SSL)** which can be identified with address starting with https.
- Look for the **Lock icon** in the address bar while visiting ECI website. Click on the Lock icon to see the SSL Certificate. It should show 'Election Commission of India' as organisation.
- All functional websites of ECI are primarily having **3rd level domain** and ends with eci.gov.in. For example https://affidavit.eci.gov.in , https://suvidha.eci.gov.in
- For submitting electoral forms use only **https://nvsp.in or voter helpline mobile app**.
- All ICT applications are available at **Google play store and Apple store**, search for developers name as “Election Commission of India”.

Commonwealth Governance and Peace Director, Katalaina Sapolu opening the expert review meeting

# INDIA PARTICIPATED IN PREPARATION OF CYBER SECURITY GUIDE FOR COMMON WEALTH COUNTRIES

The Commonwealth committee's cyber Declaration, adopted by Heads of Government at their meeting in 2018, committed member countries to building the foundations of an effective national cyber security response. The Commonwealth Secretariat have invited the Chief Election Commissioners (or their representative) of all 53 EMBs. This was scheduled at the Commonwealth HQ, Marlborough House, in London on 30th and 31st July, to bring together Chief Election Commissioners (or their representative) from across the Commonwealth. The email received from Commonwealth stated that "Given that India is a regional leader in electoral cyber security, and undoubtedly have important insights for this Guide."

## CYBER SAFE GENERAL ELECTIONS 2019..

**Continued from Page 1..**

..,.Nodal Officer in the office of Chief Electoral officer to coordinate with Chief Information Security Officer, ECI. Appropriate training and handholding was provided in cyber security enforcement by way of legal, technical and operational methods. The Election Commission of India flawlessly executed the cyber defence mechanism to ensure operational efficiency in election process at one hand and cyber safety on the other.

The coordinated defence mechanism of ECI has not only brought confidence amongst the Electoral machinery and improved the public perception of fairness and belief in use of ICT for elections.

A Commonwealth Guide on Election Cyber security is being developed to support Election Management Bodies (EMBs) to manage risks associated with the use of technologies in elections. This project was part of a wider programme of work aimed at supporting Commonwealth member countries to implement the Commonwealth Cyber Declaration adopted by Commonwealth Heads of Government in April 2018.

The Cyber Security Guide will be a stepping stone for all Election Management Bodies. It shall also make a platform to share best practices in cyber security.

Also, India briefed about the application "Voter Helpline Mobile Application", 'New Suvidha', and cVIGIL. Many Countries showed interest in cVIGIL application which prioritized the speedy and effective actions by authorities and promised users status report within 100 minutes on Model Code of Conduct Violations. Many Countries were also interested in the Real-time Counting Management System which ECI has recently developed during Parliamentary Elections of 2019.

**EDITORIAL**

Dr. Kushal Pathak

Chief Information Security Officer &
Director Information & Communications Technology,
Election Commission of India