VOL-1 Technology Division, Dak Bhavan, New Delhi 1ST AUG 2022

DIGI-DAK

IT Transformation Newsletter of Department of Posts

The beginning of Digital Transformation

The IT Modernisation Project 2.0 has been approved by the Cabinet on 19th January 2022 for the next 8 years.

India Post was successful in computerisation and networking of Post offices during the first phase of big-bang IT induction during 2012-2022. With the New age Digital transformation under IT 2.0, Department will get the agility needed to respond to changes in the Citizen / Government demands and expectations. This step also helps in staying competitive and in business.

This transformation will help Department in reducing costs, improving productivity, providing a better customer experience, ensuring governance and compliance, bringing in increased employee productivity and increase collaboration.

1

UBIQUITOUS

Post Offices to become digital IT retail hub & provide universal banking

2

COLLABORATIVE

Provide open ecosystem for mail & parcel network for effective citizen delivery

3

AGILE

Addressing any national challenges of supply chain & industry expectations.

Solution Architecture

The detailed roadmap of inter-play of various solutions has been issued.

New Email Solution

DoP moved to centralised email solution with enhanced security and expanded mailbox options.

Cyber Security Initiative

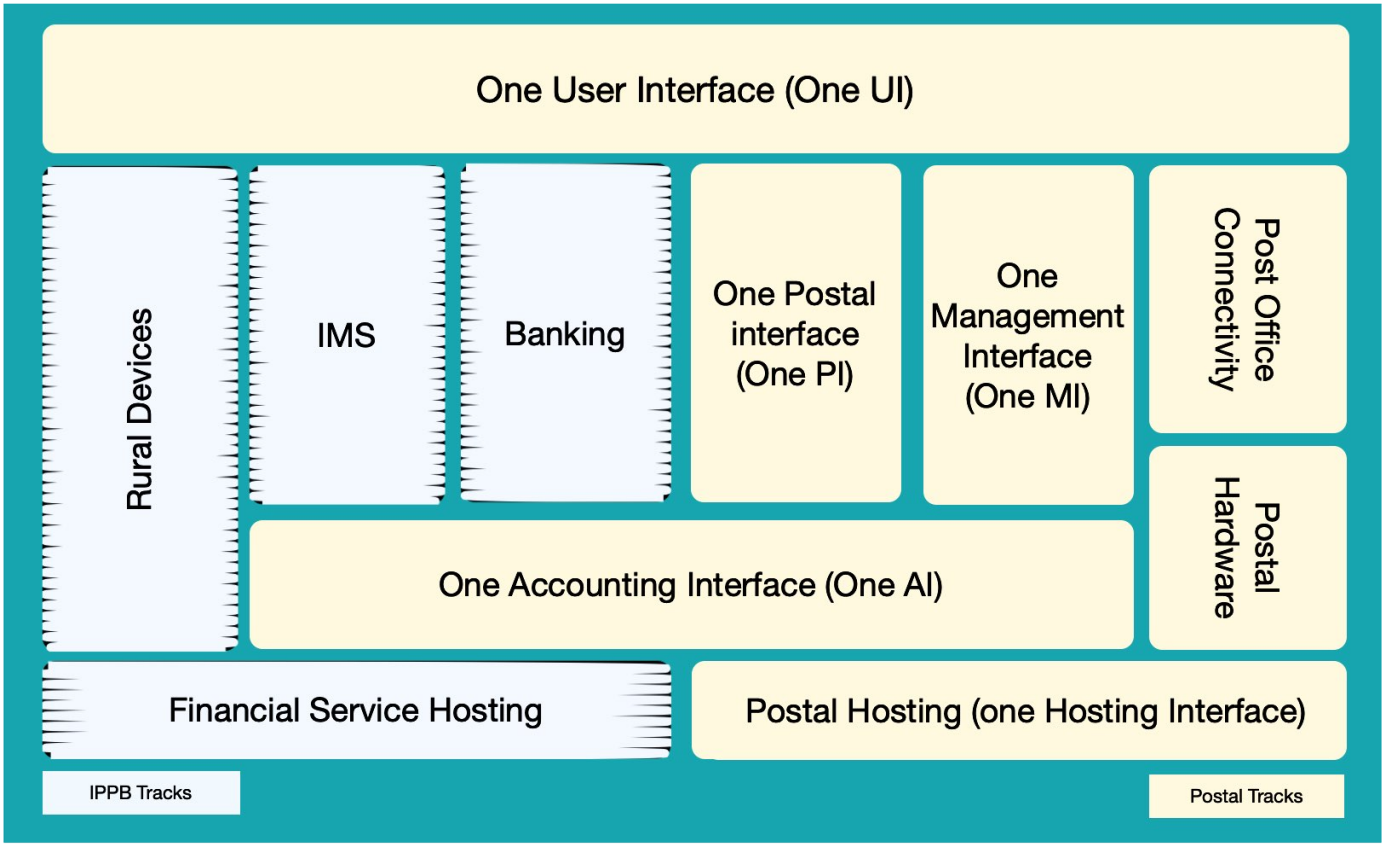
DoP initiates cyber security measures to protect its IT

SOLUTION ARCHITECTURE

To provide inclusive, integrated single-window view of postal and financial services to its stakeholders through multiple delivery channels using re-engineered processes & cutting edge Information Technologies, leading towards an era of e-Governance.

With the directions of Cabinet to avoid the dual IT Infrastructure, the Department had approved the solution design utilising the service mesh architecture. For the first time it will enable simple, secure & single interface for both Post office and citizens using One UI. It will also allow cost effective reporting and accounting interface using One MI and One AI. This flexibility will add innumerable services providers like India Post Payment Bank, Government Departments eg. CSCs and any Commercial organisations' 'on-the-fly'. This will ensure maintaining the control over its branding in the front end and the integrity of its accounting and reporting requirements at the back end.

India Post Payment Bank will bring in IT structure for Banking, Insurance and other financial services by utilising its strict banking regulatory norms of IT safety and security. Alongside, the Department will get the opportunity to bring in new technologies in the Postal Segment utilising the scalable cloud infrastructure & cutting edge technologies like Artificial Intelligence and Machine Learning. This blend will decouple the bottlenecks of Financial and Postal IT requirements and leverage the best of both forms of IT



CISO DESK

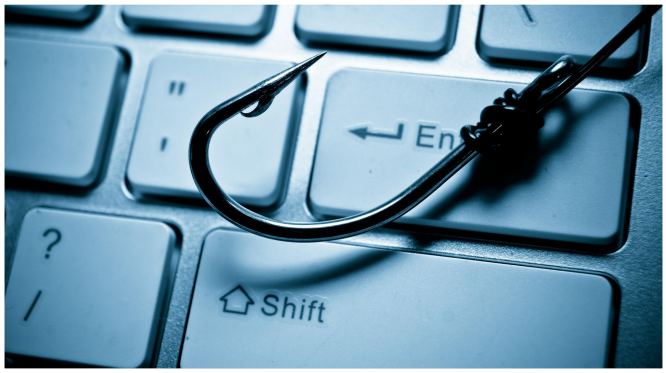
Cyber Security For Department of Posts

Saving Postal Officials from Phishing

Phishing Email: The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords

In a Phishing attack, a victim receives a message that appears to have been sent by a known contact or organization. The attack is carried out either through a malicious file attachment containing phishing software or links connecting to malicious websites. In either case, the objective is to install malware on the user's device or direct the victim to a malicious website to trick them into divulging personal and financial information, such as passwords, account IDs or credit card details.

Phishing campaigns are often built around significant events, holidays and anniversaries or take advantage of breaking news stories, both actual and fictitious. Recently a lottery system phishing was very prevalent in the DoP, and most of the websites were taken down by our security team at CEPT. The attacker tried to trick the users as if it was the genuine India Post website and tried to take the personal information like mobile numbers.



How to Protect from Phishing attacks

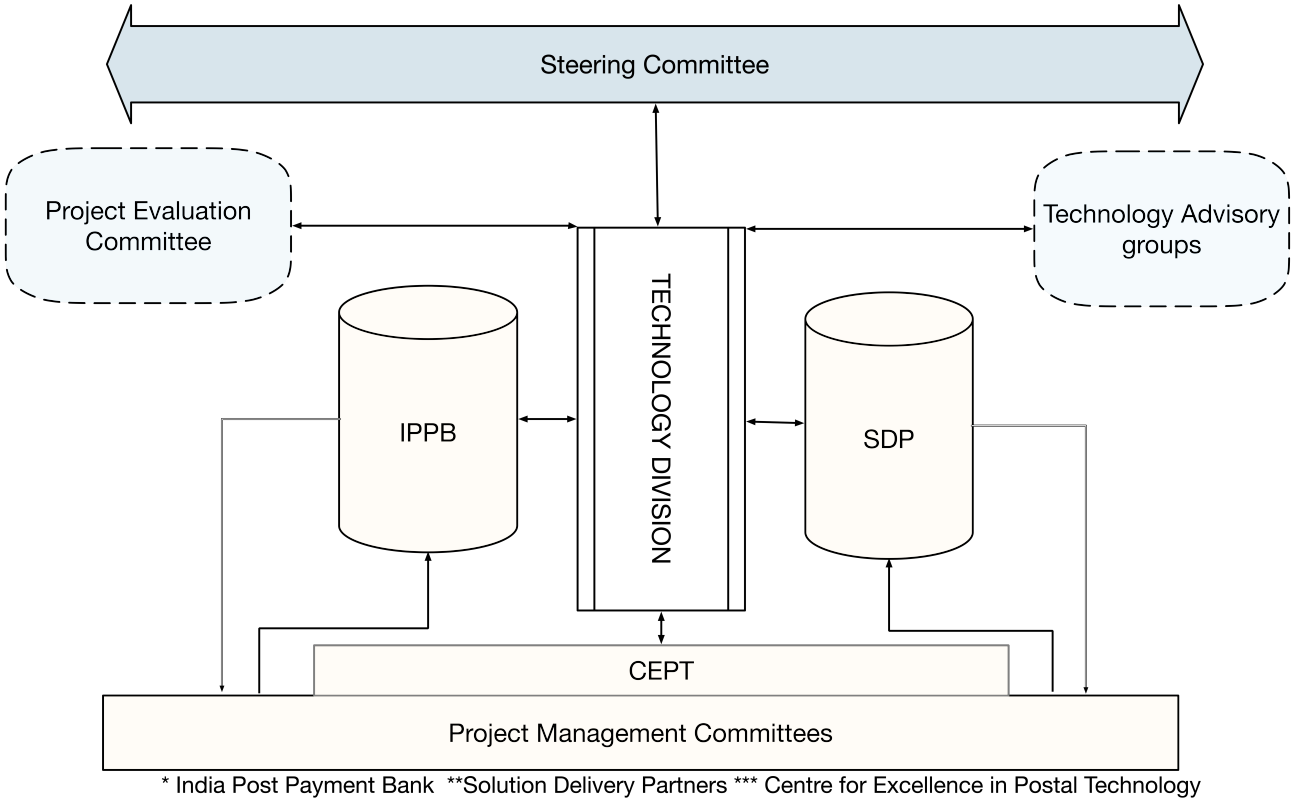
- **Think Before You Click!** – It's fine to click on links when you're on trusted sites. Clicking on links that appear in random emails and instant messages, however, isn't such a smart move. Hover over links that you are unsure of before clicking on them specially from Post Office computers, and refrain from opening such links and emails.
- **Never Give Out Personal Information** – As a general rule, you should never share personal or financially sensitive information over the Internet.
- **Keep Your Browser Up to Date** – Security patches are released for popular browsers all the time. They are released in response to the security loopholes that phishers and other hackers inevitably discover and exploit. Update them immediately.
- **Verify a Site's Security** – It's natural to be a little wary about supplying sensitive financial information online. As long as you are on a secure website, however, you shouldn't run into any trouble. Before submitting any information, make sure the site's URL begins with "https" and there should be a closed lock.

YOUR PASSWORD IS YOUR STRENGTH

Passwords are first line of protection against any unauthorized access into your personal computer. The stronger the password, the higher level of protection your computer has from malicious software and hackers. These are a set of rules covering. How to create a strong password that you can remember.

- Enforce to adopt the 8 + 4 Rule as strong password
- Use eight characters with one upper and one lower case, a special character like an asterisk and a number
- A strong password must be at least 8 characters long.
- Avoid names, places, family, pets, and dictionary words.
- It must be very unique from your previously used passwords.
- It should not contain any word spelt completely.
- Adopt pass-phrase e.g. B04t5B04t5! = Boats x Boats
- Use a keyword Pattern: #WAxcvgy7890-

IT GOVERNANCE



Steering Committee under IT 2.0 has been constituted on 22.03.2022, which is empowered to sanction all projects under the DoP IT 2.0 including total contract cost. Subsequently Steering Committee approved the detailed Governance and Solution Delivery framework for the DoP IT implementation.

On 09.06.2022, Project Evaluation Committee (PEC) has been constituted headed by Secretary Posts to monitor and release all payments. Technical Advisory Groups (TAG) having eminent persons have been formed to give technical advice on technology selection. Project Management Committees (PMC) have been formed having representation from functional divisions of Directorate, Circle, Region, Divisions, CEPT, India Post Payment Bank (IPPB) and National Informatics Centre (NIC). These committee will have the complete control over the requirements, development and delivery of the solution so deployed.

Under the aegis of above governance structure, the IT 2.0 shall have two implementation teams: 1. Software Development Agencies / Technology resources for Postal Tracks (to be brought in by Technology Division) and 2. India Post Payment Bank as Technology Service Provider for Financial Tracks.

Centre for Excellence in Postal Technology will play a vital role of providing functional support to Management Committees. CEPT shall also do the management of Software Development Agencies and technical resources under the Program.

DIGI-DAK
(**Digi**tal **D**riven **A**ccelerated **K**nowledge-base)
Issued by:
Technology Division
Postal Directorate,
Sansad Marg, New Delhi-110001
technologydivision@indiapost.gov.in
https://www.indiapost.gov.in