Maharashtra Cyber Anti-Phishing Unit

Concept Note for association with partners and organisations

FEBRUARY 2019

Introduction & Background

Phishing has emerged to be one of the most extensively used means by cybercriminals to deceive online users. According to **RSA Quarterly Fraud Report, 2018**, Phishing accounts for **half of all Cyber Fraud Attacks** worldover.

India is among top 4 countries targeted for phishing attacks, while also being **the second-biggest host for such online frauds**, only after the US.

Overall, Maharashtra being one of the most digitalised states in India, is home to more than **35% of registered Cyber Crimes** across the country, with a steady rise every year.

The aim behind setting up this specialised unit called is based on these ever-growing experiences of various forms of Phishing that are dealing in identity thefts and social engineering to financially and socially exploiting users.

National Payment Council of India has joined hands in supporting **Maharashtra Cyber** in turning this vision into reality. In a letter dated January 24, 2019, NPCI has extended all-round support in institutionalising a setup dedicated to report financial phishing purposes, and has asked to operationalise the cell on “war-footing” before the end of February 2019.

Mission & Objectives

- To setup a dedicated anti-phishing unit that will help report, resolve, curb and spread awareness against Phishing.

- To establish a first-of-its kind dedicated web portal for users to report their phishing/financial identity theft incidents on.

- To make available a web portal, 24 x 7 helpline, dedicated WhatsApp account and an email ID for the same.

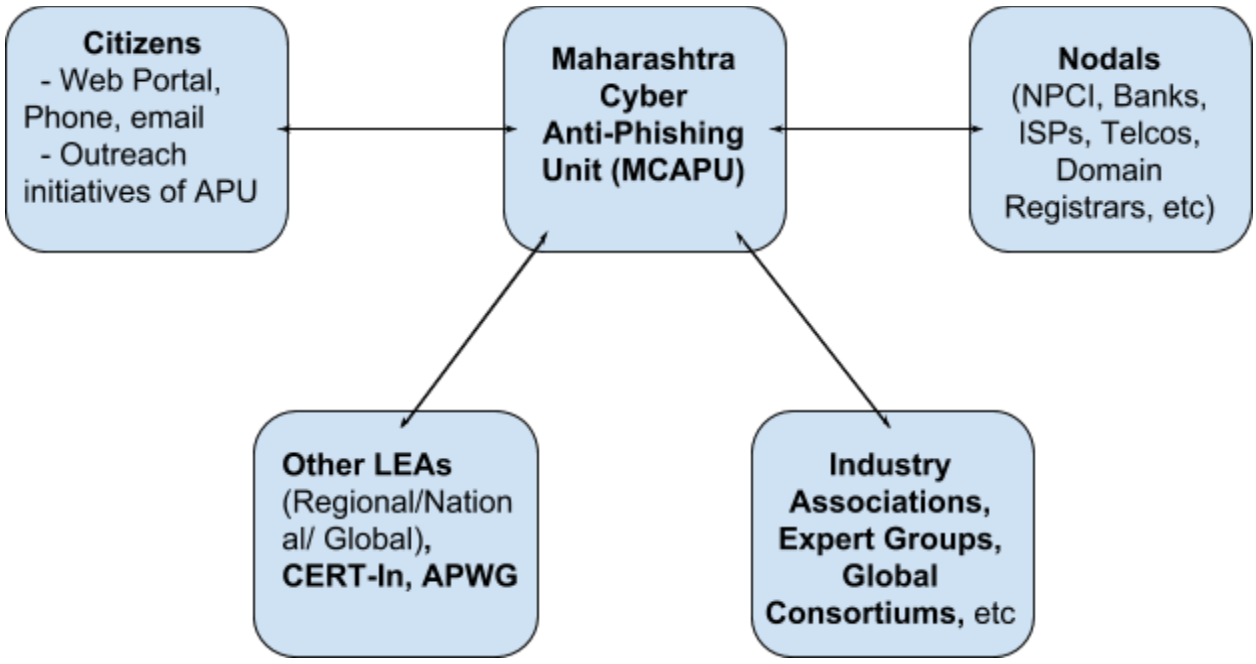
- To coordinate with nodals of various Cyber Police Units across India and abroad to help resolve/report such cases and prioritise action on them as-soon-as possible.

- To associate with nodals of various banks, social media, e-Wallets, etc so as to take action, undo damage and be prepared as much as possible.

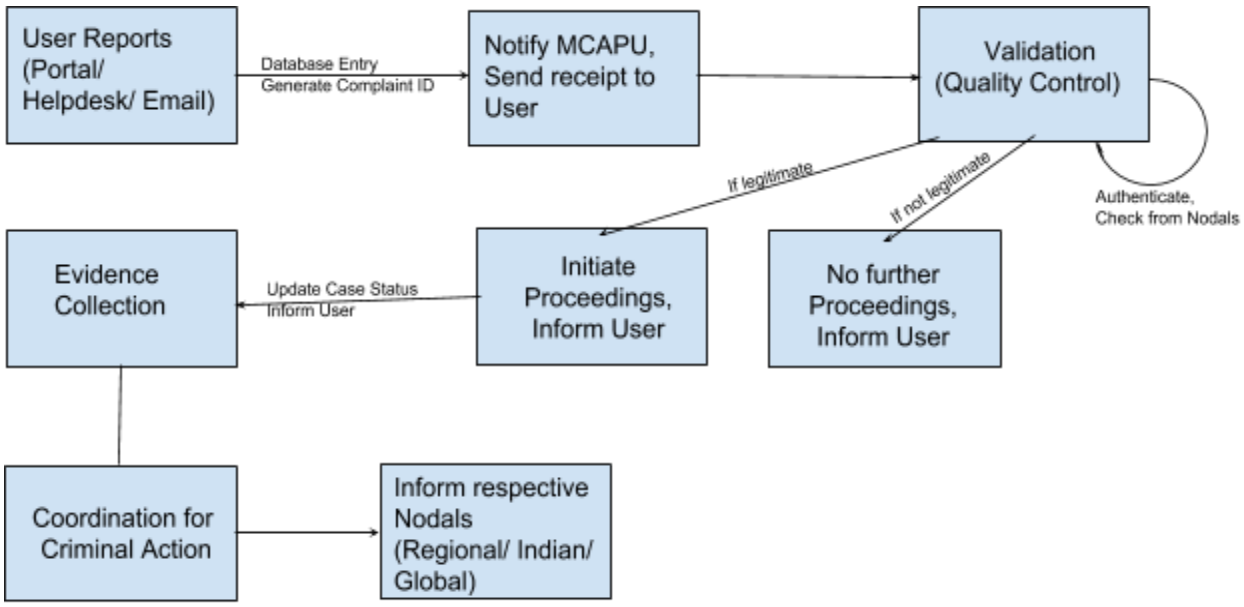
- To establish linkages with APWG, various Cyber Security Companies, Industry Bodies, Industry Experts, etc to develop more effective anti-phishing measures and help institutionalising awareness against it.

- To focus on awareness building against phishing among all sections of society with key focus on vulnerable sections like senior citizens, rural population, etc.

- To have a restricted-access dashboard for unit members to view, update and analyse all such reported complaints.



Coordination of citizens, nodals of financial organisations, cyber police units and industry and experts with the MCAPU team.



(Indicative) Process Structure of the MCAPU

Modes of Association with partners / organisations

1. Phishing URL Checker / Mobile Number Checker

A special feature as a tab on the web-portal would be a **Phishing URL / Mobile Number Checker**, that allows user to enter a URL or a mobile number and check whether it is a Phishing/unsafe website or not. This functionality would be built and managed by a technology organisation that is ready to tie-up with Anti-Phishing Unit, and the organisation would be specially mentioned with a “powered by” along with a mention as a technical partner in this initiative.

This functionality would fundamentally make use of:

- Officially whitelisted websites

- Blacklisted illegitimate/phishing websites, using our database and utilising other open data sources like PhishTank and the organisation's own Phishing database, if any
- Any other modes of phishing validation available.

The organisation would be expected to build this around a web exploration technology based on a heuristic approach that would ideally have Machine Learning.

Examples of such a feature can be seen at:

- **URL Abuse** - A tab in Luxembourg's official Incident Response website
https://www.circl.lu/urlabuse/

- **Is It Phishing**
https://isitphishing.org/

2. Association for Collaborative Phishing List

Associating Company can collaborate over Phishing Data by sharing their Phishing database with Anti-Phishing Unit. Such an association is a win-win for both organisations, as it allows our Unit to coordinate action on more phishing channels while allowing the associating company to use our database and make their software/tool blacklisting stronger or help protect their organisation's interests.

Such an exchange of information should happen as-soon-as it is validated, and would involve exchange of lists of URLs, mobile numbers, people and companies.

The respective organisation will be mentioned as 'Operational Partners' in the initiative.

3. Knowledge Partnership

Associating Company can collaborate with Anti-Phishing Unit by drafting periodic reports containing research, analysis, trends, threats, etc in phishing and financial identity theft area. This collaboration will have two-way sharing of such information.

Such partners would be labelled 'Knowledge Partners'.

4. Association for Sponsored Solutions

Anti-Phishing Solutions of security companies ready to associate in this initiative would be featured on the official portal as a 'Sponsored Solution' or would be mentioned first in the list of Solutions suggested by us.

In return, the sponsoring company could organise events/conferences for Maharashtra Cyber, promote the initiative and take care of any other such expenses concerning the unit as foreseen by Maharashtra Cyber. Also sponsoring companies can provide tools for URL Checking, Mobile Number Checking, Botnet Removal, etc.

An example of such an association is Cyber Swachhta Kendra (Botnet Cleaning & Malware Analysis Centre), where the Union Government has mentioned Quick Heal's free Bot Removal Tool on their official website https://www.cyberswachhtakendra.gov.in/security-tools.html

5. Awareness & Outreach Partners

Awareness and Outreach would be crucial for this initiative to make an impact as it is primarily user-driven, and organisations can join hands with Maharashtra Cyber in promoting this unit, spreading awareness about phishing and how it should be dealt with.

For this, the associating organisation would have to provide dedicated personnel of **at least 5 people** along with their solutions which will manage content, digital promotions, offline promotions, social media campaigns, etc to promote our unit, spread awareness about phishing and how it should be tackled. This personnel would work at Maharashtra Cyber's office.

Such an organisation would be roped in as 'Outreach Partners'.

6. Research & Prevention Partners

Associating Companies can associate with Anti-Phishing Unit over research, which will be a separate vertical in this initiative. This vertical would research emerging issues on the subject, recognise new technologies and their scope in contributing to phishing issues, study problems faced by stakeholders currently, and any other research as suggested by Maharashtra Cyber.

For this, the associating organisation would have to provide dedicated personnel of **at least 3 cyber specialists,** who would work out of Maharashtra Cyber's office, along with required tools and technologies for such research. The associating organisation would in return be mentioned as 'Research Partners' in the initiative.

7. Operational Partners

Associating organisations would provide the platform as-well-as the resources that will be required to operate specific verticals inside the Unit. This would include providing required personnel for the same.

The associating company would be labelled as 'Operational Partner' in the initiative.