national health authority
सत्यमेव जयते

arogya Samvad

Pradhan Mantri Jan Arogya Yojana
Ayushman Bharat
PM-JAY

"AROGYA SAMVAD" *Newsletter for AYUSHMAN BHARAT - Pradhan Mantri Jan Arogya Yojana* **ISSUE 6,** Apil 2019

Social Media Monitoring

Ayushman Bharat - Pradhan Mantri Jan Arogya Yojana (AB PM-JAY) since its inception has garnered large media/public attention and curiosity, especially regarding the enrolment/availing benefits under the scheme as beneficiaries. Many unscrupulous individuals, agencies, websites, digital media channels, mobile apps, job portal websites and organizations are trying to harness the curiosity of the citizens for their selfish gain. These parties are misusing National Health Authority's (NHA) brand name and falsely posing themselves as authorized representatives of NHA for the purpose of duping public at large.

Fraudulent techniques for duping include unauthorized means of data collection such as unofficial beneficiary enrolment or employee recruitment drives either by themselves or through a contracted third party via fake application or other social media means etc.

In the wake of such fraudulent activities, NHA constitutionalized the social media monitoring activity for the sole purpose to identify, track and report the fake/fraudulent websites and mobile applications disseminating false information/services via internet. The process adopted for social media activity to ensure a vigilant approach against the fraudulent website and applications is as follows:

Identification

- Team adopts a vigilant approach to identify fraudulent activities across internet.
- We monitor Google play store for fake mobile application
- Our team surf the internet daily to identify fake websites impersonating PM-JAY website

Reporting

- Fortnightly report sent to MeitY, NIXI, NIC, Cert-IN
- Mothly letter to CEO, NIXI for the closure of fake website on .IN domain
- Monthly complaint letter to DCP office for lodging FIR
- Mothly report to google for the closure of fake mobile application.

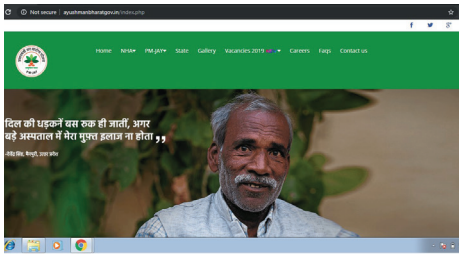
Tracking

- The team collects evidences against all the fraudulent entity as a proof for future reference.
- We update status of all the websites/application found to track the closure.
- Websites are classified as per their severity level in accordance to a predefined defination.

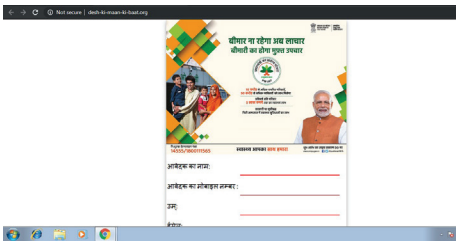
Through the consistent and tenacious effort of the team, NHA has identified 110 Fake Websites out of which 67 were pulled down as a result of several actions taken by NHA, and 126 Fake mobile applications were identified out of which 120 were de-listed from Google Play store. The closing of such applications took place after NHA issued individual legal notices against the developers publishing the fake mobile applications.

Some screenshots of fake websites identified till date:

1. Some fake websites have mirrored the PM-JAY website to trick innocent citizens.



2. Some fake websites are collecting personal information from citizens by claiming to be an authorized website.



3. Websites after collecting information from residents ask the victim to share the website on whatsapp, in order to receive their registration number. Thus, spreading at an exponential rate on social media.

national health authority
सत्यमेव जयते

arogya Samvad

Pradhan Mantri Jan Arogya Yojana
Ayushman Bharat
PM-JAY

"AROGYA SAMVAD" *Newsletter for AYUSHMAN BHARAT - Pradhan Mantri Jan Arogya Yojana* **ISSUE 6,** April 2019

They are Phishing for you...do not get Hooked !!!

Detecting a Phishing Email

Being vigilant in detecting phishing emails and educating stakeholders of NHA to be proactive is a crucial step in protection.

Here is a quick top 10 list of how to spot and handle phishing email:

1 Don't trust the display name of who the email is from

Just because it says the email is from a person you know or trust doesn't mean it truly is. Be sure to look at the email address to confirm.

2 Look, but don't click

Hover the mouse over parts of the email without clicking on anything. If the alt text looks strange or doesn't match what the link description says, don't click on it - report it.

3 Check for spelling errors

Attackers are less concerned about spellings or being grammatically correct than a normal sender would be.

4 Consider the Salutation

Is the address general or vague? Is the salutation to "valued customer" or "Dear employee". Beware of these general salutations.

5 Is the email asking for personal information

Legitimate companies are unlikely to ask for personal information in an email. Never provide your personal information or sensitive information to an unverified user.

national health authority
सत्यमेव जयते

arogya Samvad

Pradhan Mantri Jan Arogya Yojana
Ayushman Bharat
PM-JAY

"AROGYA SAMVAD" *Newsletter for AYUSHMAN BHARAT - Pradhan Mantri Jan Arogya Yojana* **ISSUE 6,** April 2019

6 Beware of urgency

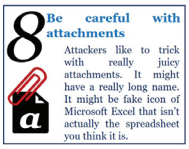
These emails might try to make it sound as if there is some emergency, do not fall into the trap. [eg. NHA CEO/PMO requests the beneficiary health information of Kerala state as soon as possible].

7 Check the email signature

Most legitimate senders will include a full signature block [eg. Name, designation, company name, contact details, office address] at the bottom of their emails.

8 Be careful with attachments

Attackers like to trick with really juicy attachments. It might have a really long name. It might be fake icon of Microsoft Excel that isn't actually the spreadsheet you think it is.



9 Don't believe everything you see

If something seems slightly out of the norm, its better to be safe than sorry. If you see something off, then its best to report it to NHA Information Security (IS) team.

10 When in doubt, contact IS team

No matter the concern, the NHA Information Security (IS) team would rather have you send something that is legit than to out NHA's sensitive and beneficiary personal data at risk.