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 8,** June 2019

CyberSuraksha Dishanirdesh

Vishing Calls

Vishing (a combination of the words Voice and Phishing) is a phone scam in which fraudsters try to trick us into divulging our personal, financial or security information or into transferring money to them.

What can you do?

- Beware of unsolicited telephone calls
- Take the caller's number and advice them that you will call them back
- Don't validate the caller using the phone number they have given you (this could be fake or spoofed number)
- Fraudsters can find your basic information online (e.g. social media).
- Don't assume a caller is genuine because they have such details.
- Don't divulge any type of data/information on request over phone

For reporting any suspicious activity write to NHA Security Team

SMiShing SMSs

SMiShing (a combination of the words SMS and Phishing) is the attempt by fraudsters to acquire personal, financial or security information by text message.
The fake text message is providing you with a fake website link, where the information you provide will be used to commit identity theft, fraud and other crimes

What can you do?

Don't click on links, attachments or images that you receive in unsolicited text messages without first verifying the sender.

Don't be rushed. Take your time and make the appropriate checks before responding

Never respond to a text message that requests your PIN or your online banking password or any other security credentials

If you think you might have responded to SMiShing text and provided NHA's data, contact NHA security team immediately