

PHISHING ATTACKS IN NAME OF AAROGYA SETU APP INCREASING: CERT-IN

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

Phishing attacks in the name of Aarogya Setu mobile application are witnessing a “high rise” as online scamsters are taking advantage of the increased inquisitiveness of internet users during the [coronavirus \(COVID-19\)](#) pandemic, India’s cyber security agency said on Saturday.

It said attackers are also impersonating tools linked to the World Health Organisation and popular video-conferencing platforms such as Zoom to steal sensitive data.

[Aarogya Setu app mandatory for travel on 15 special trains: Railways](#)

“Aarogya Setu app-focused phishing have seen high rise. Scamsters impersonate as HR department, CEO, or any other known person and target users by spreading messages like ‘your neighbour is affected’, ‘see who all are affected’, ‘someone who came in contact with you tested positive’, ‘recommendations to self-isolate’, ‘guidelines to use Aarogya Setu’ among others,” the CERT-In said in a latest advisory accessed by *PTI*.

The [Aarogya Setu application](#) uses bluetooth and GPS to alert users who may have encountered people who later tested positive for the coronavirus.

Phishing denotes to the cyber term of luring and cheating an internet user through a fake SMS or email and thereby breaching their privacy to steal sensitive information.

[Watch | How does the Aarogya Setu app work?](#)

“In recent trends, threat actors are taking advantage of pandemic situation to trick the users to give up their sensitive information by taking advantage of the interest associated with recent novel coronavirus activities, news, and information,” the advisory said.

The Computer Emergency Response Team of India (CERT-In) is the national technology arm to combat cyber attacks and guarding of the Indian cyber space.

It said cyber attackers (threat actors) impersonate popular video platforms such as Zoom, Google Meet, Microsoft Teams, Aarogya Setu app and WHO to send phishing messages through SMS (smishing), WhatsApp (whishing) or phishing emails to steal identities and engage in other nefarious activities during the COVID-19 pandemic.

[Health Ministry launches Aarogya Setu IVRS facility for those without smartphones](#)

The cyber attackers, it said, are using fake domains to impersonate popular apps to first lure the victims and then send them links such as “relief package”, “safety tips during corona”, “corona testing kit”, “corona vaccine”, “payment and donation during corona”.

It said the name of the WHO was also being impersonated. “Cyber criminals are sending phishing emails impersonating WHO and e-mails appear to be originating from the domain of WHO. Such e-mails may contain malicious file and URLs (universal resource locators),” it said.

The cyber agency suggested some counter-measures to check this online menace: Beware

about the domain, spelling errors in emails, websites and un-familiar email senders; check the integrity of URLs before providing login credentials or clicking a link and do not submit personal information to unknown and unfamiliar websites.

[Today's cache | Security issue in Aarogya Setu app, and more](#)

It said users should exercise caution and avoid clicking dubious URLs providing special offers such as winning prize, rewards, cashback offers and they practice safe browsing tools, filtering tools their anti-virus and use a proper firewall.

You have reached your limit for free articles this month.

Already have an account ? [Sign in](#)

Start your 14 days trial now. [Sign Up](#)

Find mobile-friendly version of articles from the day's newspaper in one easy-to-read list.

Enjoy reading as many articles as you wish without any limitations.

A select list of articles that match your interests and tastes.

Move smoothly between articles as our pages load instantly.

A one-stop-shop for seeing the latest updates, and managing your preferences.

We brief you on the latest and most important developments, three times a day.

*Our Digital Subscription plans do not currently include the e-paper ,crossword, iPhone, iPad mobile applications and print. Our plans enhance your reading experience.

Dear reader,

We have been trying to keep you up-to-date with news that matters to our lives and livelihoods, during these difficult times. To enable wide dissemination of news that is in public interest, we have increased the number of articles that can be read free, and extended free trial periods. However, we have a request for those who can afford to subscribe: please do. As we fight disinformation and misinformation, and keep pace with the happenings, we need to commit greater resources to news gathering operations. We promise to deliver quality journalism that stays away from vested interest and political propaganda.

Please enter a valid email address.

Nadella is planning to be in India between February 24 and February 26 and will likely visit New Delhi, tech hub Bengaluru and the financial capital of Mumbai, two people familiar with the plans said

The new algorithm, based on a specialised form of machine learning called deep learning, is not only turnkey, but also quick, finding performance bugs in a matter of a few hours instead of days, says a study

Subscribe to The Hindu now and get unlimited access.

Already have an account? [Sign In](#)

Start your 14 days trial now [Sign Up](#)

To continue enjoying The Hindu, You can turn off your ad blocker or [Subscribe to The Hindu](#).

[Sign up for a 30 day free trial.](#)

END

Downloaded from **crackIAS.com**

© **Zuccess App** by crackIAS.com

CrackIAS.com