Source : www.thehindu.com Date : 2021-08-12

A NEW PHISHING ATTACK LURKING TO SCAM BANKING CUSTOMERS: CERT-IN

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

Scammers are targeting banking customers in India using a novel phishing attack to collect sensitive information | Photo Credit: Reuters

Scammers are targeting banking customers in India using a novel phishing attack to collect sensitive information such as internet banking credentials, mobile number and OTP to carry out fraudulent transactions, the country's cyber security agency has warned in its latest advisory.

(Subscribe to our Today's Cache newsletter for a quick snapshot of top 5 tech stories. Click here to subscribe for free.)

The malicious activity is being carried out using the ngrok platform, a unique web application, it said.

"It has been observed that Indian banking customers are being targeted by a new type of phishing attack using ngrok platform." "The malicious actors have abused the ngrok platform to host phishing websites impersonating internet banking portals of Indian banks," according to the advisory issued by CERT-In on Tuesday.

The Indian Computer Emergency Response Team or CERT-In is the federal technology arm to combat cyber attacks and guarding the cyber space against phishing and hacking assaults and similar online attacks.

Phishing denotes to the fraud when an attacker, masquerading as a trusted entity, tricks a victim into clicking evil links to steal passwords, login credentials and one-time password (OTP).

Using these phishing websites, the advisory elaborated, "malicious actors" are collecting sensitive information of the customers such as internet banking credentials, mobile number and OTP to perform "fraudulent transactions." It said the phishing attacks have been seen to be triggered through SMSes containing links that end with ngrok.io/xxxbank.

The advisory explained this with a sample SMS.

"Dear customer your xxx bank account will be suspended! Please Re KYC Verification Update click here link http://446bdf227fc4.ngrok.io/xxxbank".

Once a victim clicks on this URL (universal resource locator) and log in to the phishing website using internet banking credentials, the attacker generates OTP for 2FA or two factor authentication which is delivered to the victim's phone number.

"The victim then enters this OTP in the phishing site, which the attacker captures," it said.

Finally, the attacker gains access to the victim's account using the OTP and performs fraudulent transactions, the advisory said.

Also Read | Hackers are using Morse code to launch phishing attack

The cyber security agency has suggested some "best practices" to nip these attacks in the bud, the most important being: "Look for suspicious numbers that don't look like real mobile phone numbers as scammers often mask their identity by using email-to-text services to avoid revealing their actual phone number." "Genuine SMSes received from banks usually contain sender id (consisting of bank's short name) instead of a phone number in sender information field." It further suggested internet banking users to "only click on URLs that clearly indicate the website domain." "When in doubt, users can search for the organisation's website directly using search engines to ensure that the websites they visited are legitimate," it said.

A specific check against such attacks is "exercising caution towards shortened URLs, such as those involving bit.ly and tinyurl." "Users are advised to hover their cursors over the shortened URLs (if possible) to see the full website domain which they are visiting or use a URL checker that will allow the user to enter a short URL and view the full URL," it said.

Users can also use the shortening service preview feature to see a preview of the full URL, the advisory stated.

Also Read | Cyberattacks surge in the first half of 2021, ransomware attacks dominate, report finds

It said bank customers should pay "particular attention to any mis-spelling and/or substitution of letters in the URLs of the websites they are browsing." Some other counter-measures stated in the advisory are the often-repeated principles that are advised for safe browsing and accessing the internet.

"Install and maintain updated anti-virus and anti-spyware software, filtering tools (anti-virus and content-based filtering), firewall, and filtering services." Update spam filters with latest spam mail contents, it said.

"Customers should report any unusual activity in their account immediately to the respective bank," it said.

"Phishing websites and suspicious messages should be reported to the CERT-In at incident@cert-in.org.in and respective banks with the relevant details for taking further appropriate actions," the advisory concluded.

The Ad Observatory project at NYU was started by the Cybersecurity for Democracy group with over 6,500 volunteers at the University’s school of engineering in September 2020

Telstra Corp, Optus and TPG Telecom are alleged to have made incorrect claims about the maximum speed of the internet connections they offer and also accepted payments from some customers for plans without providing the promised speeds, the Australian Competition and Consumer Commission (ACCC) said in a notice on Monday.

END