Subject: **Cybercriminals using fake Social Media Verification Badge to steal credentials.**

Threat Summary

Various social media platforms such as Facebook, Instagram, Twitter, etc. offer verification badges as a credibility indicator to help show authenticity and integrity to visitors. To obtain a badge, profiles must meet various requirements and undergo a verification process.

These coveted verification badges are being used as a phishing lure for social engineering campaigns targeting some of the most popular social networks across the internet. The lure of social media verification badges entices unsuspecting victims.

Fig. 01 – Fraudsters perpetrating frauds using fake social media verification Badge lure

Users in popular social media platforms are attractive targets for cybercriminals, due to the trusted brand and enormous customer base of such platforms.

Modus Operandi

- Fraudsters send phishing emails to their target victims, on the email id registered in their social media accounts.
- Unsuspecting victims are lured into submitting their information to obtain a verified badge. The victims are provided with option to apply for the badge.
- After clicking 'Apply Now', the webpage reveals a series of phishing forms on the domain that fraudsters create beforehand.
- The form targets the victim's social media login information and then asks for their email address and password credentials, which are used to reset and verify ownership of the phished social media accounts.
- Fraudsters gain unauthorized access to the victims' social media accounts and other sensitive personal and financial information, which is leveraged for further cyber financial frauds.

Suggestions

- ❒ Exercise caution when clicking on links provided on emails, and verify that they're safe before you take any action.
- ❒ Verify policies for attaining verification badges of twitter, Facebook, Instagram, etc. on their official websites.
- ❒ Scrutinize, if a request seems too urgent, as fraudsters typically show urgency in their requests.
- ❒ Scrutinize the domain name of the webpages where information is required to be filled.
- ❒ Don't open attachments or download files from untrusted sources.
- ❒ Report any such incidents on the cybercrime.gov.in portal and follow @CyberDost on Twitter, YouTube, Facebook, Instagram, Public, Koo and LinkedIn to know more about safety tips.

Regards

Indian Cyber Crime Coordination Centre
CIS Division, MHA
011-23438207