Govt-Themed Phishing Attack Targets Indian Citizen

MH CERT

Advisory ID: CERTMH_CA_2025_02

Date: 09th May 2025

Summary

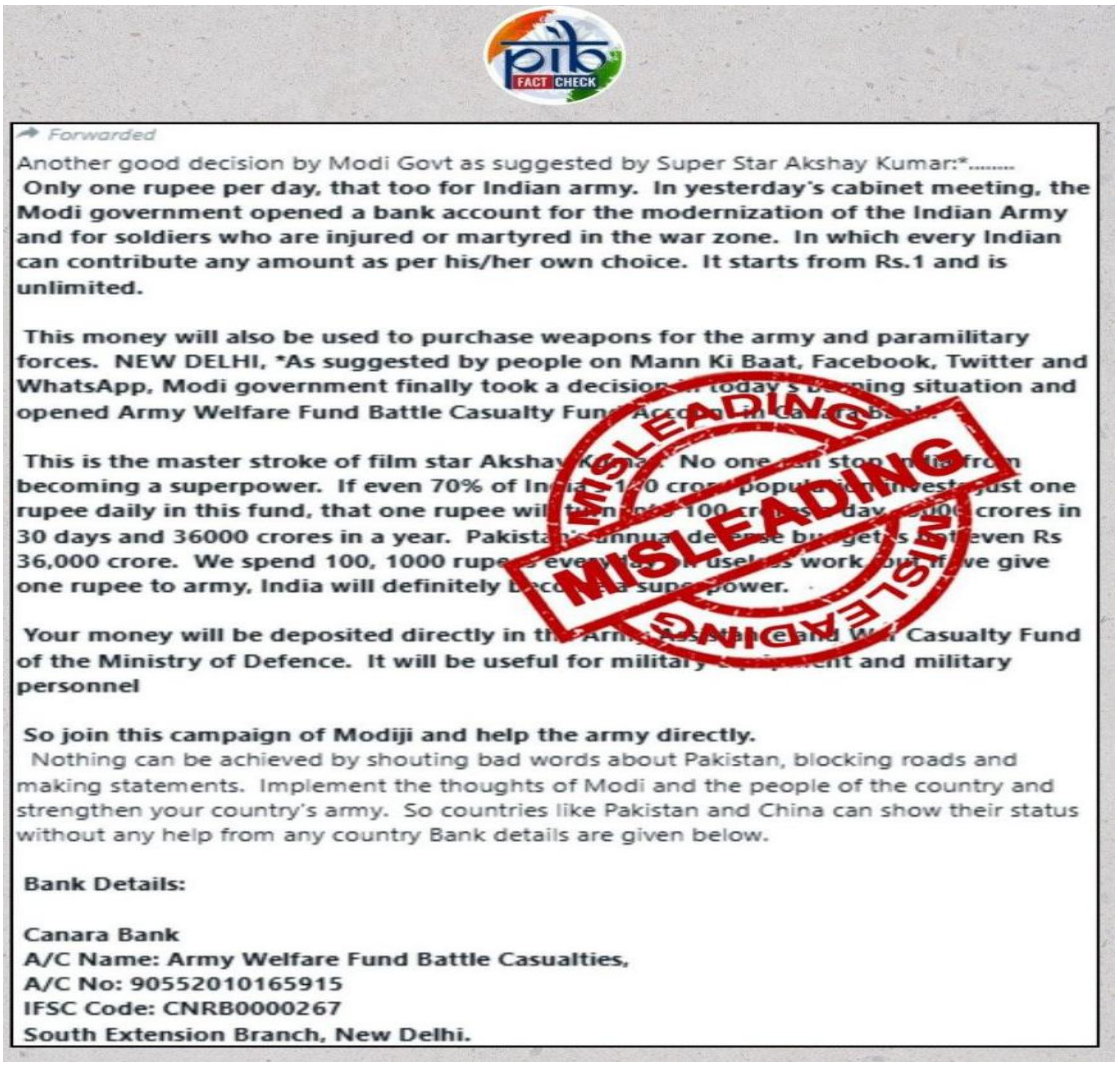
Following the Pahalgam terror attack on April 22, 2025, rising tensions between India and Pakistan have escalated into a digital conflict. Multiple hacker groups from both sides have been actively launching cyberattacks.

MH-CERT is monitoring several Pakistan-origin cyberattacks in recent days. With the ongoing cyberattacks, we are advising Citizens with respect to sudden rise in malicious activities targeting personal devices, emails, and networks across India.

These attacks include the distribution of malicious PDF files linked to phishing domains, aiming to steal data and compromise systems. These attempts are believed to be a direct fallout of the geopolitical escalation and are part of a broader campaign of cross-border cyber aggression.

Citizens are urged to remain vigilant, avoid suspicious emails or downloads, and report any cyber incidents to MH-CYBER PORTAL.

Misleading Viral News



The above image shows a post from PIB (Press Information Bureau) Fact Check, which has labelled a message about an "Army Welfare Fund Battle Casualty Fund" as "MISLEADING."

- The message falsely claims:
  - The Modi government has opened a bank account where Indians can donate as little as ₹1 per day to support army modernization and help injured soldiers.
  - The initiative was supposedly suggested by actor Akshay Kumar.
  - It includes bank account details for Canara Bank.
  - It states that if 70% of Indians contribute ₹1 daily, it would generate ₹36,000 crores annually.

Phishing Attack Targeting Government Entities and Citizen

Malicious documents are being circulated under the guise of official government reports and updates. These documents may appear legitimate, but they contain embedded links that redirect individuals to fake login pages designed to steal personal and sensitive information.

Observed Malicious Attachment Names:

- ***"Report & Update Regarding Pahalgam Terror Attack.pdf"***
- ***"Report Update Regarding Pahalgam Terror Attack.pdf"***
- ***"Action Points & Response by Govt Regarding Pahalgam Terror Attack .pdf"***
- ***"J&K Police Letter Dated 17 April 2025.pdf"***
- ***"ROD on Review Meeting held on 10 April 2025 by Secy DRDO.pdf"***
- ***"RECORD OF DISCUSSION TECHNICAL REVIEW MEETING NOTICE, 07 April 2025 (1).pdf"***
- ***"MEETING NOTICE – 13th JWG meeting between India and Nepal.pdf"***
- ***"Agenda Points for Joint Venture Meeting at IHQ MoD on 04 March 2025.pdf"***
- ***"DO Letter Integrated HQ of MoD dated 3 March.pdf"***
- ***"Collegiate Meeting Notice & Action Points MoD 24 March.pdf"***
- ***"Letter to the Raksha Mantri Office Dated 26 Feb 2025.pdf"***
- ***"Alleged Case of Sexual Harassment by Senior Army Officer.pdf"***
- ***"Agenda Points of Meeting of Dept of Defence held at 11 March 25.html"***
- ***"Action Points of Meeting of Dept of Defence held at 10 March 25.html"***
- ***"Agenda Points of Meeting of External Affairs Dept 10 March 25.pdf.html"***

What to Look Out For:

- **Suspicious Links:** Be cautious of the documents contains links, especially those that direct to websites with unusual or suspicious domain names.
- **Sensitive Topics:** Attackers exploit current geopolitical events, such as the Pahalgam terror attack, to increase engagement with phishing content.
- **Fake Login Pages:** Clicking on malicious links will redirect individuals to a fake login page that asks for sensitive credentials, including government or Defence-related emails (such as those ending in @gov.in or @nic.in). These credentials are then sent directly to the attackers.
- **Unsolicited Emails/Attachments:** Be cautious of unexpected emails related to national security or government matters. Do not open attachments or click links unless you're sure of the source.

How to Protect Yourself

- **Verify the Source:** If you receive an email or document claiming to be from a government agency, always verify the sender's email address. Official communication will come from recognized government domains.
- **Check Links Carefully:** Hover your cursor over any links (without clicking) to check if the URL matches the official website. Do not click on suspicious or unfamiliar links.
- **Do Not Enter Personal Information:** Never enter your login credentials, especially government or organizational email details, on websites you are not familiar with.
- **Use Antivirus and Security Software:** Ensure that your antivirus and security software are up to date to protect against malicious attachments and links.

SAVE THESE 24x7 HELPLINE NUMBERS & REPORT

- **1945 & 1930**
- **https://mhcyber.gov.in/ (MAHARASHTRA CYBER CRIME PORTAL)**