ADVISORY

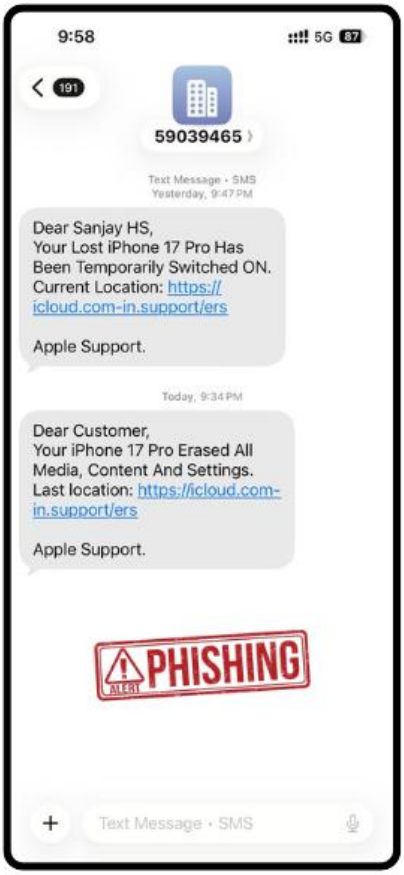
TAU/ADV/015 | Dated: 5th May 2026

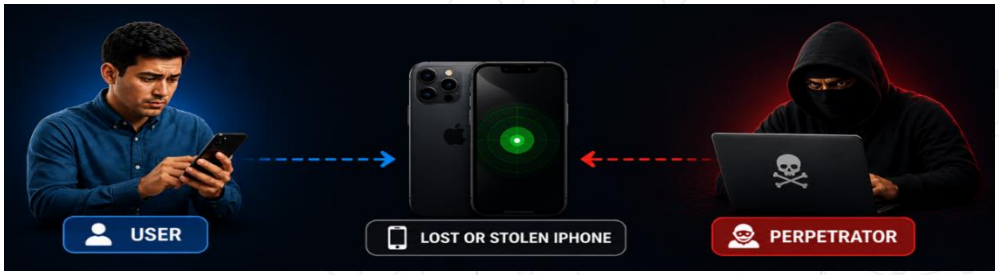
गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Indian Cyber Crime Coordination Centre
सहयोग करवाहे • Working Together With Vigour

iPhone users targeted in *hybrid* cybercrime – theft & unauthorized access

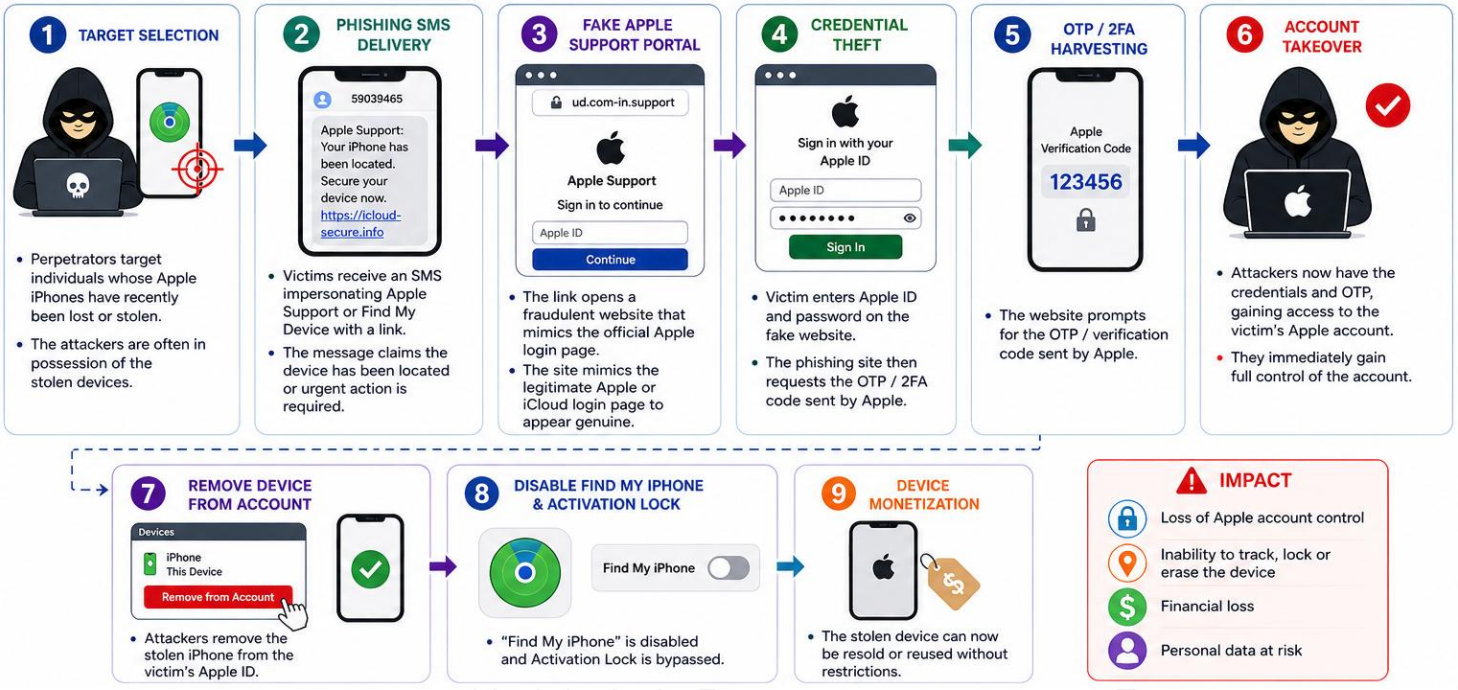
The **National Cybercrime Threat Analytics Unit (NCTAU)** of **I4C** has identified a sophisticated phishing campaign targeting Apple iPhone users whose devices have been lost or stolen and are in the possession of perpetrators. The perpetrators impersonate Apple Support and exploit victims' urgency to locate or secure their missing devices through fraudulent SMS messages containing phishing links. These messages closely resemble legitimate "**Find My iPhone**" or Apple Support notifications and redirect users to counterfeit Apple login pages designed to steal Apple ID credentials and One-Time Passwords (OTP). Once compromised, attackers gain unauthorized access to victims' accounts and remove the linked Apple ID from the stolen device.





Modus Operandi

- **Selection of Targets:** Perpetrators specifically target individuals whose Apple iPhones have recently been lost or stolen and also having physical possession of the lost or stolen devices.
- **Phishing SMS Delivery:** Victims receive fraudulent SMS message impersonating Apple Support or the "Find My Device" service from *majorly numeric SMS header*. These messages contain phishing links and typically claim that the lost device has been temporarily switched off or that urgent action is required to erase contacts, media, and other data.
- **Fake Apple Support Portal:** When victims click the phishing link, they are redirected to a fraudulent website designed to closely resemble the official Apple Support or iCloud login page. The phishing domains often use deceptive naming conventions to appear legitimate.
- **Credential and OTP Harvesting:** Users are prompted to enter their Apple ID credentials, followed by the One-Time Password (OTP) or two-factor authentication code sent by Apple.
- **Account & Device Takeover:** Once the credentials and OTP are obtained, perpetrators gain unauthorized access to the victim's iCloud account, remove the Apple ID linked from the stolen device, disable "Find My iPhone," bypass security features, and resell or reuse the device without restrictions.



Recommended Precautions

- Avoid clicking links received via SMS (especially from international SMS Headers) or unsolicited messages & carefully check the URL before entering credentials.
- Request for blocking lost/stolen mobile at CEIR Portal - **Link**
- Do not enter OTPs on unverified websites neither disclose OTPs to anyone.
- Use apple official "Find Devices" service page - **https://www.icloud.com/find**
- Do not remove devices from your Apple ID without verification & ensure "Find My iPhone" remains active.
- Always activate Two-Factor Authentication (2FA), use strong passwords & keep devices updated with latest security patches.
- Report phishing attempts immediately to **https://cybercrime.gov.in/** or call **1930.**

"Your awareness & caution are the strongest defense against phishing attacks."