Incident Reporting Form

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
| **I am:**  the effected entity ☑ reporting incident affecting other entity | | | | |
| **Contact Information of the Reporter** | | | | |
| Name & Role/Title |  Individual ☑ Organization | | | |
| Organization name (if any) | CatchPhish | | | |
| Contact No. | 8779959071 | | Email: | catchphish@gmail.com |
| Address: | Kj Somaiya college of engineering | | | |
| **Basic Incident Details** | | | | |
| Affected entity  (if not same as reporting entity above) | | Union bank of India | | |
| Incident Type | | | | |
| Targeted scanning/probing of critical  Data Breach Attacks or malicious/suspicious activities  networks/systems  Data Leak affecting systems/ servers/ networks/  Compromise of critical systems/information Attacks on Internet of Things (IoT) devices software/ applications related to Big Data,  Unauthorised access of IT systems/data and associated systems, networks Block chain, virtual assets, virtual asset  Defacement or intrusion into the website software, servers exchanges, custodian wallets, Robotics, 3D  Malicious code attacks Attacks or incident affecting Digital and 4D Printing, additive manufacturing,  Attack on servers such as Database, Mail and DNS Payment systems Drones  and network devices such as Routers Attacks through Malicious mobile Apps Attacks or malicious/ suspicious activities  ☑Identity Theft, spoofing and phishing attacks Fake mobile Apps affecting systems/ servers/software/   DoS/DDoS attacks  Unauthorised access to social media applications related to Artificial Intelligence  Attacks on Critical infrastructure, SCADA and accounts and Machine Learning operational technology systems and Wireless Attacks or malicious/ suspicious activities  Other (Please Specify)  networks affecting Cloud computing ----------------------------------------------------------  Attacks on Application such as E-Governance, E- systems/servers/software/applications  Commerce etc. ---------------------------------------------------------- | | | | |
| Is the affected system/network critical to the organization’s mission? (Yes / No). (Brief details.) | | Yes | | |
| Basic Information of Affected System (Provide information that is readily available.) | | Domain/URL: http://sso-cdn-coinbasepro-autthh.webflow.io IP Address: 172.64.151.8, 104.18.36.248 Operating System:Unknown (Hosting Server Details Not Available) Make/ Model/Cloud details: Hosted by Unknown Affected Application details (If any): Potential phishing website at sso-cdn-coinbasepro-autthh.webflow.io Location of affected system (including City, Region & Country): Unknown  Network and name of ISP: Unknown, IP: 172.64.151.8, 104.18.36.248 | | |
| Brief description of Incident: A potential phishing website was detected at sso-cdn-coinbasepro-autthh.webflow.io. Risk Score: 90.21/10 (Confidence: High). The site was created on 08/05/2013 07:50 UTC.   Risk Analysis: - Login form legitimacy: The provided HTML is a block page indicating a 'Phishing' category, implying a malicious intent for the blocked URL. - Brand impersonation: The page uses a logo and styling to appear as a legitimate warning or block page related to web filtering, likely from Fortinet. This impersonation can trick users into trusting the information presented. - Social engineering: The page employs social engineering by alarming the user about a 'Web Filter Violation' and 'Access Blocked' due to a violation of Internet usage policy. The redirection link labeled as a rate submission can redirect the user to a different address or conduct malicious action when clicked. - Malicious JavaScript: While no JavaScript is directly present in the provided HTML, the redirect URL, `http://sso-cdn-coinbasepro-autthh.webflow.io/`, is flagged as phishing. It can contain malicious JavaScript code for data theft or other exploits.  The domain is registered with Unknown. VirusTotal scan shows 17 engines flagged this domain as malicious out of 94 total engines. Immediate intervention is recommended to prevent potential data theft and financial fraud. | | Occurrence date & time (dd/mm/yyyy hh:mm): 08/05/2013 07:50 UTC Detection date & time (dd/mm/yyyy hh:mm): 18/03/2025 09:53 UTC | | |
| **Note:** (i) This form provides general guidance in terms of information which could be relevant to the incident.   1. It is not mandatory to fill and/or sign this form. Incidents may also be reported by providing relevant information in the communication itself or in any other readable form. 2. Reporting entity may, if desired, also provide relevant information other than mentioned in this form. | | | | |
| **Mail/Fax incident reports to: CERT-In, Electronics Niketan, CGO Complex, New Delhi 110003 Fax:+91-11-24368546 or email at:** [**incide**](mailto:incident@cert-in.org.in)[**nt@cert-in.org.in**](mailto:nt@cert-in.org.in) | | | | |