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://dskjkfegbpne.xyz IP Address: 124.156.198.80 Operating System:Unknown (Hosting Server Details Not Available) Make/ Model/Cloud details: Hosted by Dominet (HK) Limited Affected Application details (If any): Potential phishing website at dskjkfegbpne.xyz Location of affected system (including City, Region & Country): Guangdong Province, CN  Network and name of ISP: Dominet (HK) Limited, IP: 124.156.198.80 | | |
| Brief description of Incident: A potential phishing website was detected at dskjkfegbpne.xyz. Risk Score: 82.51/10 (Confidence: High). The site was created on 14/03/2025 20:46 UTC.   Risk Analysis: - Login form legitimacy: No login form present in the HTML, so no associated risks. - Brand impersonation: The HTML uses FortiGuard branding. While the HTML itself is not necessarily malicious, it \*could\* be part of a phishing attack if presented outside of the legitimate Fortinet context. The URL `http://dskjkfegbpne.xyz/aupayindex` is highly suspicious and indicates a phishing attempt. - Malicious JavaScript: No JavaScript is present in the HTML, so there is no risk of malicious script execution directly from this content. However, the redirect URL could lead to a page with malicious Javascript. - Social engineering: The page informs the user that access to a web page has been blocked, which can be legitimate. However, the provided link `https://globalurl.fortinet.net/rate/submit.php?id=4B4E2C09265B1F2D2F646829296B2827&amp;cat=3D&amp;loc=http://dskjkfegbpne%2exyz%2faupayindex&amp;ver=9` is a potential risk. The URL `http://dskjkfegbpne.xyz/aupayindex` appears to be the target of the 'phishing' categorisation, making the click-through more tempting. The domain and long ID make it questionable. - The base64 encoded image is very large, increasing the page load time, potentially making the user more anxious. It should be verified  The domain is registered with Dominet (HK) Limited. VirusTotal scan shows 11 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): 14/03/2025 20:46 UTC Detection date & time (dd/mm/yyyy hh:mm): 17/03/2025 21:10 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) | | | | |