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://ebay.ebayshoo.com IP Address: 182.237.3.49, 1.32.253.194, 182.237.3.48, 14.128.39.163, 134.122.140.132, 14.128.39.164, 134.122.140.144, 14.128.39.162, 134.122.140.147 Operating System:Unknown (Hosting Server Details Not Available) Make/ Model/Cloud details: Hosted by Gname.com Pte. Ltd. Affected Application details (If any): Potential phishing website at ebay.ebayshoo.com Location of affected system (including City, Region & Country): Redacted for privacy, FU JIAN SHENG, MY  Network and name of ISP: Gname.com Pte. Ltd., IP: 182.237.3.49, 1.32.253.194, 182.237.3.48, 14.128.39.163, 134.122.140.132, 14.128.39.164, 134.122.140.144, 14.128.39.162, 134.122.140.147 | | |
| Brief description of Incident: A potential phishing website was detected at ebay.ebayshoo.com. Risk Score: 76.22/10 (Confidence: Medium). The site was created on 13/07/2024 05:30 UTC.   Risk Analysis: - Login form legitimacy: There is no login form, therefore not applicable. - Brand impersonation: The page displays a FortiGuard Intrusion Prevention message indicating a phishing URL. This could be a false flag or a legitimate warning. Need to verify legitimacy of URL. - Malicious JavaScript: No Javascript identified; however this needs to be inspected dynamically. - Social engineering: The page attempts to socially engineer the user into believing a website is blocked and to click a link for re-evaluation.  The domain is registered with Gname.com Pte. Ltd.. VirusTotal scan shows 20 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): 13/07/2024 05:30 UTC Detection date & time (dd/mm/yyyy hh:mm): 17/03/2025 10:59 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) | | | | |