No. DG-II/CERT/4/124/2023/P-I
GOVERNMENT OF SINDH
SCIENCE & INFORMATION TECHNOLOGY DEPARTMENT
Karachi, dated the 14th July 2026

To,

1. The Chairman, Enquires, Anti-Corruption, Establishment Sindh, Karachi.
2. The Chairman, Planning & Development Board Sindh, Karachi
3. The Chairman/Chairperson, CMIT Sindh, Karachi
4. The Chairman Sindh HEC Karachi.
5. The Senior Member Board of Revenue (BOR) Sindh, Karachi.
6. The Additional Chief Secretary, Govt of Sindh
7. The Principal Secretary to Governor Sindh, Governor Secretariat, Karachi.
8. The Principal Secretary to Chief Minister Sindh, CM Secretariat, Karachi.
9. The Administrative Secretary, GoS (All).
10. The Provincial Ombudsman, Sindh.
11. The Inspector General of Police Sindh, Karachi
12. The Divisional Commissioner (All) in Sindh
13. The Chief Executive Officer Sindh IT Company (SITC), Karachi.

SUBJECT: **CYBERSECURITY ADVISORY - CLICKFIX SOCIAL ENGINEERING ATTACKS USING FAKE SECURITY VERIFICATION PAGES**

With reference to the letter received from National Cyber Emergency Response Team (NCERT) (**copy enclosed**), Government of Pakistan, regarding recently observed spike in targeted cyber activity following malicious campaigns exploiting human behavior, the attached Advisory titled "National CERT Advisory - ClickFix Social Engineering Attack Using Fake Security Verification Pages" (**Annexure**) has been issued by the National Cyber Emergency Response Team (National CERT).

2. In this regard, it has been requested that the **attached Advisory** may kindly be disseminated to all concerned departments, organizations, and personnel under the administrative control. All staff members may be directed to ensure timely implementation and strict compliance with the recommended security protocols particularly ensuring that no commands copied from web browsers.

(AYAZ AHMED UQAILI)
Member (IT Industry) S&ITD
0345-8219899

Annexure: NCA-36.280626 - National CERT Advisory - ClickFix Social Engineering Attack Using Fake Security Verification Pages

A copy is forwarded for information and necessary action to: -
1. Director General (nCERT). L Block, Pak Secretariat, Islamabad
2. Staff Officer to SACM for S&IT Department, Govt. of Sindh, Karachi.
3. Staff Officer to Secretary S&IT Department, Govt. of Sindh, Karachi.

Annexure

NCA-36.280626 – National CERT Advisory - Social Engineering ClickFix Attack Using Fake Security Verification Pages

Government Ministries and Organizations are advised to remain vigilant against an emerging and increasingly prevalent social engineering technique known as the ClickFix attack. Unlike conventional cyberattacks that exploit software vulnerabilities directly, ClickFix campaigns rely on deceiving users into executing malicious commands on their own systems. Attackers typically compromise legitimate websites or create convincing fake websites that display fraudulent Cloudflare verification pages, CAPTCHA challenges, browser update prompts, or other security verification messages. These pages falsely claim that additional verification steps are required and instruct users to manually open Windows Run, Command Prompt, or PowerShell and execute a command copied to their clipboard.

Once executed, the command silently downloads and launches malicious payloads from attacker-controlled infrastructure. Depending on the threat actor's objectives, the payload may install information-stealing malware, Remote Access Trojans (RATs), ransomware, cryptocurrency miners, or other malicious tools. The compromised endpoint may subsequently be used to steal credentials, establish persistence, move laterally across the network, exfiltrate sensitive information, or launch additional attacks against organizational infrastructure.

As these attacks exploit human behavior rather than software flaws, traditional security controls alone may not prevent successful compromise. Organizations should therefore complement technical security controls with strong user awareness programs, continuous monitoring, endpoint protection, and proactive security assessments of public-facing assets.

DOCUMENT SUMMARY

Sr. No.	Field	Details
1.	Advisory ID	NCA-36.280626
2.	Threat Type	Social Engineering, Malicious Command Execution, Payload Delivery
3.	Severity	High
4.	Attack Vector	Web-based deceptive prompts / Clipboard-to-CLI execution
5.	Authentication Required	None (Relies on human interaction)
6.	User Interaction	Required (High - User manually runs commands)
7.	Scope & Applicability	Government Ministries, CII, financial institutions, enterprises
8.	Affected Products	Windows Operating Systems (PowerShell, Command Prompt, Run dialog)

1. IMPACT ANALYSIS

Failure to remediate or defend against these attacks may result in:

a. Silent download and launch of malicious payloads from attacker-controlled infrastructure
b. Complete system compromise of infected endpoint/workstation analysis environments
c. Installation of info-stealers, Remote Access Trojans (RATs), ransomware, or crypto-miners
d. Credential harvesting and sensitive organizational data exposure
e. Lateral movement into enterprise networks and secondary infrastructure
f. Establishment of persistent footholds within security and directory services
g. Potential disruption of enterprise operations and business continuity

2. THREAT CHARACTERISTICS

Characteristic	Details
Threat Category	Social Engineering & Living-off-the-Land (LotL) Exploitation
Threat Status	Active exploitation attempts observed / Highly prevalent
Root Cause	Deceptive security verification prompts exploiting user trust
Attack Surface	Web browsers and administrative CLI tools (PowerShell/CMD)
Attack Complexity	Low (Relies entirely on human execution)
Privileges Required	User privileges (Can elevate depending on target account permissions)
Impact Scope	Full endpoint compromise and potential network breach

3. ATTACK METHODOLOGY

a. User visits a compromised legitimate website or a dedicated malicious website.

b. A fraudulent verification page appears (spoofing Cloudflare, CAPTCHA, or browser updates).
c. The user is instructed to press Windows+R, open PowerShell/CMD, paste a pre-copied command, and execute it.
d. The malicious payload is silently downloaded and launched from attacker-controlled servers.
e. The malware establishes persistence, steals credentials, enables remote access, deploys ransomware, or exfiltrates data.

4. INDICATORS OF EXPOSURE / TARGETING (IoEs)

Organizations should actively hunt for the following indicators within logs, endpoints, and telemetry:

a. Suspicious Activity Patterns

i. Web browsing sessions prompting manual commands or system key combinations (Windows + R)
ii. Users copying obscure script blocks directly from external, untrusted web environments

b. Exploitation Behavior Indicators

i. Unitalicized invocation of command-line tools like PowerShell.exe or cmd.exe spawned directly from browser processes
ii. Execution of commands containing obfuscated text, encoded blocks, or Living-off-the-Land Binaries (mshta, wscript, cscript, rundll32)

c. Network & System Indicators

i. Unexpected remote file downloads triggered directly via terminal environments
ii. Creation of unauthorized scheduled tasks or new, unexplained startup persistence items
iii. Suspicious outbound connections from endpoints to unknown or untrusted external IP addresses and domains

5. REMEDIATION & MITIGATION ACTIONS

a. Immediate Defensive Controls

Sr. No.	Action Category	Recommended Actions
i.	**User Enforcement**	Mandate that users never execute commands copied from websites. Legitimate verifications never require PowerShell or

		CMD.
ii.	**Policy Restriction**	Restrict user access to PowerShell and command-line interfaces where operationally feasible.
iii.	**Endpoint Hardening**	Enable application allow-listing and strictly monitor Living-off-the-Land Binaries (LOLBins).
iv.	**Software Updates**	Keep operating systems, enterprise applications, and web browsers strictly updated.
v.	**Endpoint Security**	Deploy and properly configure Endpoint Detection and Response (EDR) solutions across all assets.
vi.	**Network Security**	Implement robust DNS and web filtering to proactively block known malicious domains and infrastructure.
vii.	**Proactive Testing**	Perform periodic Vulnerability Assessment and Penetration Testing (VAPT) on all public-facing websites and internet-accessible applications.

b. Enhanced Monitoring & Detection Requirements

i. Monitor for any browser-spawned instances of PowerShell, Command Prompt, or scripting engines.
ii. Deploy logging rules capable of detecting and decoding encoded PowerShell execution arguments.
iii. Continuously track unauthorized remote file downloads and unexpected scheduled task creation.
iv. Flag unusual outbound connection patterns originating from standard user endpoints.

c. Incident Response Requirements

i. Isolate the affected endpoint immediately and disconnect the system from both the local network and the internet.
ii. Preserve all forensic evidence; acquire comprehensive system memory and disk images for deep analysis.
iii. Reset all user and administrative credentials associated with the endpoint.
iv. Hunt for signs of lateral movement across the broader network.
v. Review system persistence mechanisms (e.g., registry keys, scheduled tasks).
vi. Analyze firewall, proxy, DNS, VPN, EDR, and authentication logs.
vii. Notify your internal Incident Response Team and relevant cybersecurity authorities.

6. ACTION SUMMARY & RESPONSE PRIORITIES

Sr. No.	Action Type	Specific Steps
a.	User Education	Issue immediate awareness alerts regarding fake verification prompts.
b.	CLI Restriction	Tighten access control policies around PowerShell, CMD, and scripting tools.
c.	EDR Configuration	Fine-tune EDR policies to detect browser-spawned command-line utilities.
d.	VAPT Assessment	Periodically test public-facing assets to deny attackers initial compromise vectors.
e.	Log Analysis	Review proxy, SIEM, and endpoint logs for anomalous outbound commands.

7. INCIDENT REPORTING

All suspected compromise, exploitation attempts, or anomalous activity must be immediately reported to National CERT Pakistan:

a. Incident Reporting Portal: https://pkcert.gov.pk/report-incident/
b. Email: cert@pkcert.gov.pk
c. UAN: +92 519203412

8. CALL TO ACTION – KEY IMPERATIVES

- Inform all personnel that legitimate security verifications never require manual command execution.
- Deploy comprehensive EDR rules to catch and kill browser-spawned CLI processes.
- Enforce application allow-listing and restrict administrative tools for standard users.
- Conduct periodic VAPT on internet-facing infrastructure to prevent site defacement/compromise.
- Establish an immediate containment playbook for endpoints executing untrusted clipboard text.