SECRET

ROUTINE

General Headquarters
IGT&E Branch HRD Dte
Rawalpindi
Tel: 30191
2939/01/HRD-NUST-EBP9G6A
16 Dec 2025

To: NUST Affairs
National University of Technology (NUTECH) IJP Road Sector I/12 Islamabad
National University Of Modern Languages Islamabad
Info: IGT&E-Coord
HRD-Coord
ID: HRD-HEIs
Office Copy
Subj: **Advisory Phishing Campaign - MOFA**

HQ 101 Cyber Division ltr no. 11/1506/Cyb/Ops-Gen Corres dated 5 Dec 2025 (pasted below) is fwd herewith for info/nec action, pl.

MOST IMMEDIATE

Headquarters 101 Cyber Division
Rawalpindi
Telephone (Civil): 051-5510630
11/1506/Cyb/Ops-Gen Corres
05 Dec 2025

To: National Cyber Emergency Response Team (NCERT)
All Internet Facing Organizations

Info: Chief of General Staff Secretariat, General Headquarters
Communication & Information Technology Branch
Military Operations Directorate, General Headquarters
Inter-Services Intelligence Agency, Islamabad
Pakistan Air Force - Air Headquarter
Pakistan Naval Headquarter

Internal: Headquarters 101 Cyber Division

Docu ID: EBP9G6A APPROVED By GSO-1 (HEIs) Lt Col Abdul Muqeet Khan Niazi on 16 Dec 2025
Note: Computer Generated Documents Do Not Require Signature.

SECRET

Subj: **Advisory Phishing Campaign - NTC & MoFA**

TIME SENSITIVE

1. Indian origin Advance Persistence Threat (APT) **SideWinder** launched **a phishing campaign to target individuals employed at public sector organizations including NTC/ MoFA** through **impersonated / fake MoFA domain.** Following fake domains has been registered by Threat Actor (TA) for luring employees, necessitating **immediate blocking/ flagging by PTA on Email servers, Firewalls, End Point and Security & Info Event Management (SIEM) solutions:-**

Ser	Malicious Domains	Impersonated Organizations	Malicious Files/ IPs
a.	https://mail-ntc-net-pk[.]zeabur[.]app/	NTC	
b.	https://webmail-mofa-gov-pk[.]zeabur[.]app/	MoFA sub domain	

2. In this connection, **Cybersecurity Advisory** is fwd herewith as per **Annexure A** to **alert NTC and MoFA** regarding the phishing campaign.

3. Fwd for information / necessary action please.

Annexure A

APT SIDEWINDER - PHISHING ATTACK

1. **Context**. The **Sidewinder group** (also known as Rattlesnake, Hardcore Nationalist (HN2) and **T-APT-04)** is operating since 2012. The group is engaged in **Cyber Espionage**[1] against members of **South Asian states' institutions.**

2. **Targets**. The APT Sidewinder primarily targets **Government & Military setups** of countries including **Pakistan** to **steal confd/ sensitive info.**

3. **Modus Operandi - Phishing Attacks**

   a. In this particular campaign TA attempts to **steals victim's credentials** email for launching of **further phishing attks.**

   b. Cyber Threat Actor (TA) **sends deceptive emails or links/ files/ media** that **appear to originate from trusted sources** (Govt offices, banks, online services etc).

   c. Emails/ links **contain official messages/ orders or some appealing content** such as security alert instrs, acct suspension warnings or password reset requests, **urging the receiver for an immediate action.**

4. **Potential Consequences**. Following are the **possible consequences** if the attack remains successful:-

   a. Credentials Compromise.

   b. System compromise for expanding malicious ingress.

   c. Installation of malware.

5. **Suggested Measures - Users & Administrators**

   a. **Communication Vigilance**

      (1) All users and administrators are advised to remain **vigilant regarding phishing emails**. Moreover, MoFA administrators advised to **change all user passwords for mail servers.**

      (2) **Verify identities** through **independent channels** if any email or message claims affiliation with MoFA.

   b. **Device Security**. Update Email, other social media applications and device operating

[1] Act of using digital methods to steal confd or sensitive info from indls, mil or govt orgs.

systems regularly to **patch vulnerabilities**.

c. **Digital Hygiene**

(1) **Do not** click on **unknown links & URLs** received through emails, social & communication media.

(2) **Strong password policy**[2] & **multifacter authentication** be **implemented** for all users.

(3) **Email spam filter** on **mail server** settings be set to **max security level**.

(4) **AV & URL/ Link scanners** be integrated with email server for scanning of email attachments before receipt by users.

(5) **Personal mobile phones must not** be **connected** to **official PCs/ Laptops**.

d. **Use Reputable Security Software**. Keep your **Antivirus** and **Anti-malware** software up-to-date and actively scan your system for threats.

6. **Way Fwd**

a. This advisory may be **disseminated** to **all ranks of NTC and MoFA** through appropriate channel (official corres, notice boards, command briefings).

b. Incident reporting channels for internal **CS teams ex NTC / MoFA** and **NCERT** (cert@pkcert.gov.pk) be advertised at all work places to encourage employees to promptly report any infection / incident.

c. **All military persons be sensitized to report** any abnormal cyber activity to 101 Cyber Div on PAMCOM **6001-38662** and email **cyberhawk001@proton.me**

[2] Alpha-numeric-spec characters comb, min 12 characters length, password expiry after 7 days, user should not be able to keep last 5 passwords.

Annex B

DISTR LIST - INTERNET FACING ORGANIZATIONS

			Copy No
1.	**CLS Sectt., DGP (A).**	-	1
2.	ISPR.	-	2
3.	**AG Br**		3
a.	PA Dte.	-	via AG Br
b.	ISSB.	-	via AG Br
c.	Housing Dte.	-	via AG Br
d.	Fauji Foundation & FFC		via AG Br
e.	AWT.	-	via AG Br
f.	MH Hosps & AFIs.	-	via AG Br
g.	NUMS & Affiliated Med Colleges	-	via AG Br
4.	**QMG Br**	-	4
a.	CSD.	-	via QMG Br
b.	NLC.	-	via QMG Br
5.	**IGT&E**		5
a.	C&SC.	-	via IGT&E Br
b.	AIMH & Regional Museums.	-	via IGT&E Br
c.	NUML, NUTECH & NUST incl affiliated Colleges	-	via IGT&E Br
d.	APS Sectt.	-	via IGT&E Br
6.	**E-in-C Br**	-	6
a.	FWO.		via E-in-C Br
b.	MES.	-	via E-in-C Br
7.	**CAFs**	-	6

a. Pakistan Rangers (Punjab) - 7

b. Pakistan Rangers (Sind) - 8

c. FC KP (N) - 9

d. FC KP (S) - 10

e. FC Bln (N) - 11

f. FC Bln (S) - 12

g. PCG - 13

8. **MoD**. ML&C - via SD-1A

9. **MoDP** - via SD-1A

a. NRTC. - via MoDP

b. POF. - via MoDP

c. HR. - via MoDP

d. DGMP. - via MoDP

e. DGDP. - via MoDP

f. DEPO. - via MoDP

10. **MoIT&T**. SCO. - 16

11. **NDU** - 17

12. Pak Mil Accts Dept (PMAD). - via SD-1A

(Contents requested to be further shared with UC/ affiliated Dtes/ setups by concerned Sects/ Brs/ Ministries)