NCA-03.021725 – National CERT Advisory: Phishing Alert Targeting Pakistani Citizens

Introduction

A new phishing and spoofing attack campaign is actively targeting Pakistani citizens through fraudulent emails impersonating law enforcement authorities. These emails falsely claim to be from the “Office of Commissioner Police Department” and accuse recipients of cybercrime offenses. The campaign aims to instill fear and manipulate victims into responding, potentially exposing their personal and financial information.

The National CERT has identified multiple red flags indicating that these emails are part of a broader social engineering attack. This advisory provides an in-depth analysis of the fraudulent emails, their impact, and recommended countermeasures to protect individuals and organizations from falling victim to this scam.

Phishing Campaign Details

The fraudulent email campaign employs fear-based tactics to pressure recipients into responding. The email falsely claims legal action will be taken within 24 hours unless the recipient complies. The primary red flags include:

1. **Non-Existent Law Enforcement Authority** – Pakistan does not have a “Commissioner Police Department.” Instead, police ranks include IGs, DIGs, SSPs, etc.
2. **False References** – The Central Bureau of Investigation (CBI) is not a Pakistani law enforcement body.
3. **Incorrect Legal Citations** – The email references the POCSO Act 2012 and Sections 67A & 67B of the IT Act, which are not applicable under the laws of Pakistan.
4. **Urgency and Threats** – The email pressures the recipient to respond within 24 hours, threatening arrest, media exposure, and blacklisting.
5. **Fake Email Domain** – The sender uses *officereportcrime.org*, which is not a legitimate Pakistani government domain. Official government emails come from (*.gov.pk)* domains.
6. **Wrong Agency Involvement** – The email claims to be from NHMP (National Highway & Motorway Police), which does not handle cybercrime cases in Pakistan.

Key Risks and Threats

1. **Identity Theft** – Victims may unknowingly provide personal details to attackers.
2. **Financial Fraud** – Scammers may use fear tactics to trick victims into making payments or providing financial information.
3. **Credential Theft** – Responding to the email may expose login credentials, enabling attackers to hijack online accounts.
4. **Social Engineering Manipulation** – Attackers use intimidation and urgency to deceive recipients into compliance.
5. **Data Breach Risk** – Individuals who share sensitive information may become targets for further attacks.

Recommendations and Action Items

1. Precautionary Measures for Individuals

a. **Do Not Respond** – If you receive such an email, do not reply, click any links, or provide any personal information.

b. **Verify Sender Authenticity** – Check whether the email originates from a legitimate government domain (. *gov.pk*).

c. **Report the Scam** – Forward phishing emails to the National CERT or relevant law enforcement agencies.

d. **Educate Yourself & Others** – Share information about this phishing attempt with colleagues and family to increase awareness.

e. **Enable Multi-Factor Authentication (MFA)** – Secure your accounts with MFA to prevent unauthorized access.

f. **Regularly Monitor Your Accounts** – Keep track of banking, email, and social media accounts for any suspicious activity.

g. **Block and Filter Phishing Emails** – Use security settings in email clients to filter out phishing attempts.

2. Best Practices for Organizations

a. **Security Awareness Training** – Conduct phishing awareness training for employees.

b. **Implement Email Security Protocols** – Use SPF, DKIM, and DMARC to prevent email spoofing.

c. **Deploy Advanced Threat Detection** – Implement security tools that detect and block phishing emails.

d. **Incident Response Planning** – Develop a plan for identifying and mitigating phishing attacks.

e. **Network Monitoring** – Monitor network traffic for anomalies associated with phishing campaigns.

3. Monitoring and Incident Response

a. **Use Email Security Tools** – Enable anti-phishing features provided by Google, Microsoft, and other email providers.

b. **Log and Analyze Suspicious Emails** – Track potential phishing attempts to improve response strategies.

c. **Coordinate with Cybersecurity Agencies** – Work with national cybersecurity teams to track and mitigate phishing threats.

4. Long-Term Strategic Considerations

a. **Regular Cybersecurity Audits** – Conduct periodic security assessments.

b. **Public Awareness Campaigns** – Raise awareness about phishing threats through media and official channels.

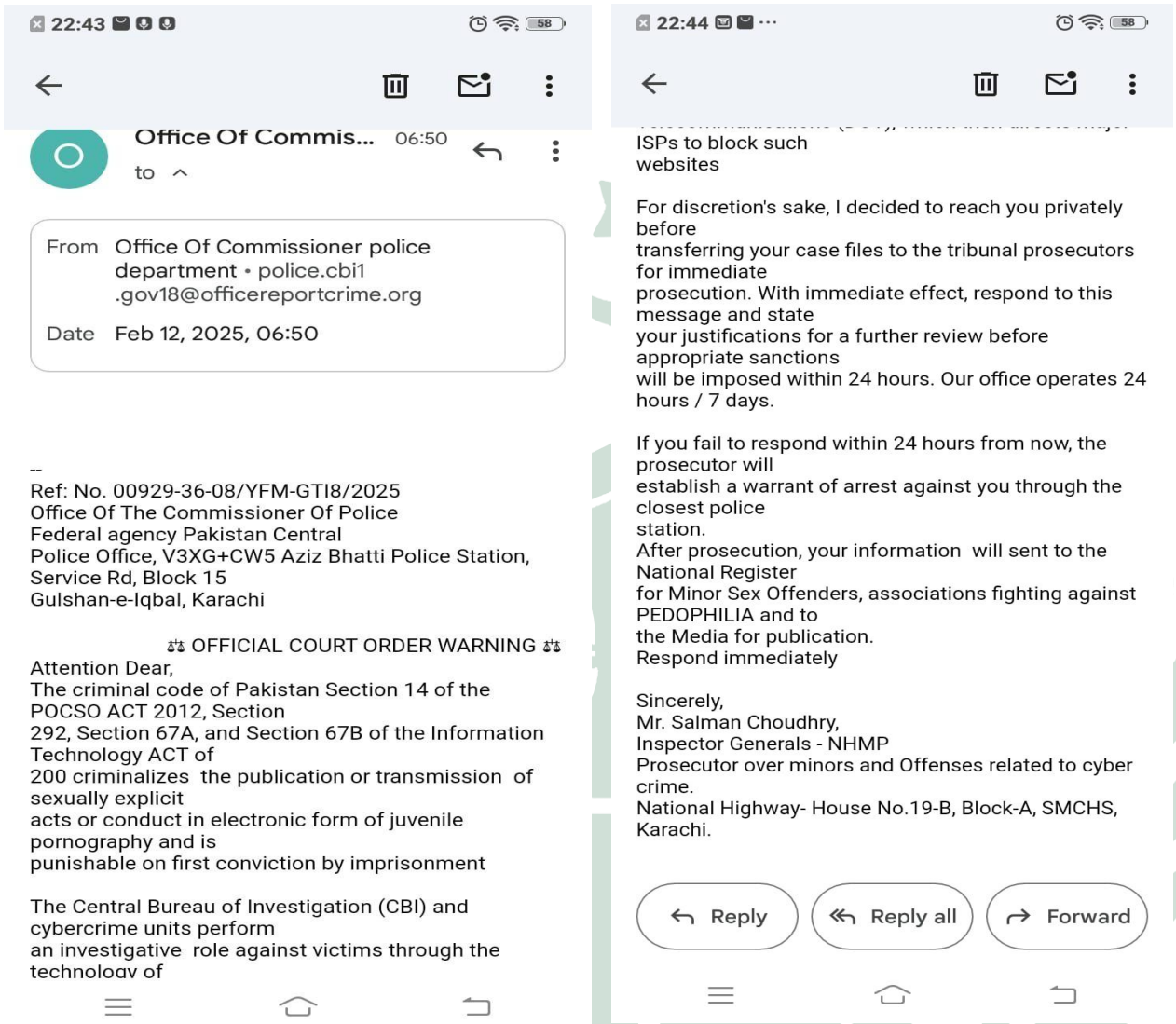
c. **Zero-Trust Security Approach** – Implement strict authentication and access control measures.

d. **Government Policy Updates** – Strengthen legal frameworks to combat cybercrime and phishing scams.

Conclusion

This advisory highlights the importance of vigilance against phishing attacks impersonating law enforcement authorities. The National CERT urges individuals and organizations to follow the recommended precautions and report any suspicious emails. By staying informed and adopting proactive security measures, we can collectively mitigate the risks associated with cybercrime and phishing scams.

Annex A



22:43

Office Of Commis... 06:50
to

From Office Of Commissioner police department • police.cbi1.gov18@officereportcrime.org

Date Feb 12, 2025, 06:50

--
Ref: No. 00929-36-08/YFM-GTI8/2025
Office Of The Commissioner Of Police
Federal agency Pakistan Central
Police Office, V3XG+CW5 Aziz Bhatti Police Station, Service Rd, Block 15
Gulshan-e-Iqbal, Karachi

⚖ OFFICIAL COURT ORDER WARNING ⚖
Attention Dear,
The criminal code of Pakistan Section 14 of the POCSO ACT 2012, Section
292, Section 67A, and Section 67B of the Information Technology ACT of
200 criminalizes the publication or transmission of sexually explicit
acts or conduct in electronic form of juvenile pornography and is
punishable on first conviction by imprisonment

The Central Bureau of Investigation (CBI) and cybercrime units perform
an investigative role against victims through the technology of

22:44

ISPs to block such
websites

For discretion's sake, I decided to reach you privately before
transferring your case files to the tribunal prosecutors for immediate
prosecution. With immediate effect, respond to this message and state
your justifications for a further review before appropriate sanctions
will be imposed within 24 hours. Our office operates 24 hours / 7 days.

If you fail to respond within 24 hours from now, the prosecutor will
establish a warrant of arrest against you through the closest police
station.
After prosecution, your information will sent to the National Register
for Minor Sex Offenders, associations fighting against PEDOPHILIA and to
the Media for publication.
Respond immediately

Sincerely,
Mr. Salman Choudhry,
Inspector Generals - NHMP
Prosecutor over minors and Offenses related to cyber crime.
National Highway- House No.19-B, Block-A, SMCHS, Karachi.

Reply Reply all Forward

Screenshots of the Phishing Email