No.14(12)/2016-Coord-Misc
Government of Pakistan
Ministry of Science and Technology
******

Islamabad, the 29th May, 2025

1. The Chairman
PCSIR, ISLAMABAD
2. The Chairman
PSF, ISLAMABAD
3. The Chairman
PCST, ISLAMABAD
4. The Chairman
CWHR, KARACHI
5. The Chairman
PEC, ISLAMABAD
6. The Rector
NUST, ISLAMABAD
7. The Rector
NUTECH, ISLAMABAD
8. The Rector
COMSATS University
ISLAMABAD
9. The Director General
NIE, ISLAMABAD
10. The Director General
PNAC, ISLAMABAD
11. The Director General
PSQCA, KARACHI
12. The Director General
PCRET, ISLAMABAD
13. The Director General
NIO, KARACHI
14. The Director General
PHA, ISLAMABAD
15. The Director General
NMIP, ISLAMABAD
16. The Managing Director
STEDEC, LAHORE

Subject: **CYBERSECURITY ADVISORY ON IMMEDIATE MITIGATION MEASURE FOLLOWING MASSIVE CREDENTIAL BREACH EXPOSING 184 MILION PASSWORDS**

Enclosed please find herewith NCERT letter No.1-1/2025/DG (NCERT)/268 dated 26th May, 2025 on the subject cited above for strict compliance. The contents of the letter ~~is~~ are reproduced as under, please.

1. In view of a recently uncovered global cybersecurity incident involving a large-scale credential exposure, the attached Advisory titled "Massive Global Credential Breach Exposes Over 184 million Passwords Across Major Platforms" (Annexure) has been issued by the National Cyber Emergency Response Team (National CERT).
2. The advisory outlines the nature and impact of the breach, including the exposure of unencrypted login credentials linked to major technology platforms, government services, and critical sectors. It provides an in-depth assessment of the threat, highlights possible exploitation tactics, and recommends essential immediate and strategic cybersecurity measures to prevent further compromise.
3. It is requested that the attached Advisory may kindly be disseminated to all relevant departments and organizations under your administrative purview. Immediate attention and necessary action are advised to ensure rapid mitigation, enhance account and system security, and reinforce cyber hygiene practices.

2. This message is to all concerned in your organization for taking immediate action.

Encl: **as above.**

(RIDA NOOR)
Section Officer (Coord)
Ph# 9202520

Copy for similar action to:-

All Head of Wing, MoST

Copy for information to:

PA to Deputy Secretary (Admin), MoST

PKCERT

National Cyber Emergency Response Team

Government of Pakistan

F.No.1-1/2025/DG (nCERT)/268 **Dated, the 26th May, 2025.**

Subject: **Cybersecurity Advisory on Immediate Mitigation Measures Following Massive Credential Breach Exposing 184 million Passwords**

In view of a recently uncovered global cybersecurity incident involving a large-scale credential exposure, the attached Advisory titled "Massive Global Credential Breach Exposes Over 184 million Passwords Across Major Platforms" (Annexure) has been issued by the National Cyber Emergency Response Team (National CERT).

2. The advisory outlines the nature and impact of the breach, including the exposure of unencrypted login credentials linked to major technology platforms, government services, and critical sectors. It provides an in-depth assessment of the threat, highlights possible exploitation tactics, and recommends essential immediate and strategic cybersecurity measures to prevent further compromise.

3. It is requested that the attached Advisory may kindly be disseminated to all relevant departments and organizations under your administrative purview. Immediate attention and necessary action are advised to ensure rapid mitigation, enhance account and system security, and reinforce cyber hygiene practices.

Annexure: NCA-32 (a).052625 – National CERT Advisory – Massive Global Credential Breach Exposes Over 184 million Passwords Across Major Platforms

Dr. Haider Abbas, TI
Director General
National CERT
Ph: 051-9203422

Rida Noor
Section Officer Coordination
Monday, 02 June, 2025, 1:36:21 PM

All Secretaries of Ministries/ Divisions of the Federal Government and Chief Secretaries of the Provincial Governments

NCA-32 (a).052625 – NCERT Advisory – Massive Global Credential Breach Exposes Over 184 million Passwords Across Major Platforms

Introduction

A major global data exposure incident has been identified involving a publicly accessible, unencrypted file containing more than 184 million unique account credentials. The breach exposed usernames, passwords, emails, and associated URLs tied to services from Google, Microsoft, Apple, Facebook, Instagram, Snapchat, as well as government portals, banking institutions, and healthcare platforms worldwide.

The leaked database is believed to have been compiled using infostealer malware—malicious software that extracts sensitive information from compromised systems. This data was stored in plain text and left completely unprotected, with no encryption or password safeguarding.

Immediate action is recommended to mitigate associated risks and to secure systems potentially impacted by this breach.

Impact

Successful exploitation of the leaked credentials may result in:

1. **Credential Stuffing Attacks** – Automated login attempts across services using reused credentials.
2. **Account Takeovers (ATO)** – Unauthorized access to user accounts and personal services.
3. **Identity Theft & Fraud** – Theft of digital identity for committing scams or impersonation.
4. **Ransomware Deployment & Espionage** – Targeted attacks on individuals and enterprises.
5. **Government & Critical Sector Compromise** – Unauthorized access to sensitive government systems.
6. **Targeted Phishing & Social Engineering** – Tailored scams using personal communication history.

Threat Details

Data Source & Nature of Exposure

- The database was publicly hosted and lacked any authentication controls.
- Appeared to be a dump from infostealer malware that had collected credentials from infected endpoints.
- Included sensitive login information for major platforms, enterprises, government agencies, and financial institutions.

Attack Complexity & Vector

- **Attack Vector**: Indirect (via malware-infected hosts; database accessed online)
- **Attack Complexity**: Low
- **Privileges Required**: None to access the file
- **User Interaction**: None (for data leak); Required for malware infection
- **Estimated Risk Score**: CVSS contextually HIGH
- **Threat Class**: Data Breach, Credential Theft, Malware Dump

Affected Systems

Potentially affected services and platforms include (but are not limited to):

- Google, Microsoft, Apple, Facebook, Instagram, Snapchat
- Government Portals (multi-national)
- Banking and Financial Accounts
- Healthcare Platforms
- Corporate and Enterprise Accounts

Exploit Conditions

Attackers may exploit this breach through:

- Credential stuffing across services with reused passwords
- Phishing attacks using associated emails and historical data
- Targeted social engineering leveraging exposed personal content
- Unauthorized access to business and government accounts
- Malware deployment using existing email/password combinations

Rida Noor
Section Officer Coordination
Monday, 02 June, 2025, 1:36:21 PM

Recommendations & Mitigation Actions

1. Immediate Remediation

- Change all passwords, especially if reused across accounts.
- Activate Multi-Factor Authentication (MFA) on all services, especially financial, email, and administrative accounts.
- Notify affected users if internal addresses or user accounts may be in the leaked dataset.

2. Credential Hygiene Best Practices

- Use unique, complex passwords for every online service.
- Avoid storing passwords in emails or unprotected files.
- Consider a password manager to securely handle account credentials.

3. Breach Detection & Monitoring

- Use any credible online service that helps you find out if your email address, phone number, or other personal data has been exposed in a data breach.
- Monitor account login activity for anomalies.
- Deploy endpoint protection software capable of detecting infostealer variants.

4. Organizational Actions

- Enforce password rotation policies at least annually.
- Apply least privilege principle across systems with sensitive access.
- Educate employees on secure credential management and phishing awareness.

5. System Security Controls

- Use email activity monitoring tools to track data exfiltration.
- Update security software and malware definitions regularly.
- Apply strict controls on cloud storage services to prevent misuse.

Monitoring & Detection

- Enable logging for unusual login attempts and credential stuffing indicators.

- Monitor for access from suspicious IP addresses or geographies.
- Use SIEM tools to track and correlate anomalies across accounts and services.

Incident Response & Readiness

- Review and update incident response plans to include credential breach scenarios.
- Validate MFA enforcement across business-critical platforms.
- Conduct tabletop exercises simulating large-scale credential reuse attacks.

Patching Summary

No software patch is applicable for this advisory as this incident pertains to credential exposure due to malware and improper data handling. Mitigation must be conducted via account protection, credential rotation, and security hygiene.

References

- https://www.zdnet.com/article/massive-data-breach-exposes-184-million-passwords-for-google-microsoft-facebook-and-more/
- https://www.techrepublic.com/article/news-database-leak-184-million-credentials/
- https://www.techradar.com/pro/security/login-and-password-details-for-apple-google-and-meta-accounts-found-in-huge-data-breach-of-184-million-accounts

Call to Action

National CERT urges all organizations and individuals to:

- Change accounts credentials immediately
- Enforce MFA across all critical services
- Educate users on strong passwords practices and password reuse risks
- Regularly monitor for suspicious account activity
- Avoid storing sensitive data in unsecured email or cloud accounts

Timely action is essential to limit the impact of this massive credential breach and prevent subsequent compromise of systems and identities.

Rida Noor
Section Officer Coordination
Monday, 02 June, 2025, 1:36:21 PM