Computer Emergency Response Team of Mauritius

A Department of the Ministry of Information Technology, Communication and Innovation

CERT-MU Security Alert

Date of Issue: 20 June 2025

Data Breach: 16 billion login credentials exposed for Apple, Google, Telegram and Facebook

Description

A massive data leak, potentially the largest in history, has exposed 16 billion records across numerous platforms, including Apple, Google, Telegram and Facebook. Researchers discovered 30 datasets containing billions of login credentials, URLs, and passwords, labeling it a "blueprint for mass exploitation." As per security researchers, this is not a new data breach. Instead, it is a compilation of previously leaked credentials obtained since early 2025:

- Infostealer malware
- Past data breaches
- Credential-stuffing attacks

The data collected through infostealers (a malware that infects computers and harvests credentials, browser-stored passwords, crypto wallets, and sensitive data) could be used for phishing campaigns, taking over accounts, ransomware attacks and attacks that compromise business emails. Since these are compiled data sets, it is difficult to determine if the data of a particular user or organisation was included or what sites may have been compromised.

In this context, CERT-MU advises users take general security precautions to protect their online accounts and enhance their security by switching to passkeys to mitigate risks from phishing and account takeovers.

How to know/check if you are impacted?

1. **Check if Your Credentials Were Leaked:**
   - Use trusted tools like Have I Been Pwned to see if your email or password appears in known data breaches.
2. **Look for Unusual Logins or Alerts:**
   - Review your recent login activity on key services like Google, Microsoft, Facebook, and banking apps.
   - Check for any "unrecognized device" or "suspicious activity" alerts.
3. **Run a Full Malware/Virus Scan:**
   - Use a reputable antivirus or anti-malware solution to scan your device.
   - If malware is detected (especially an infostealer), remove it before taking further actions.
4. **Change Your Passwords (After Scanning):**
   - Only change your passwords after ensuring your system is clean to avoid re-compromise.
   - Focus on high-value accounts first (email, banking, cloud storage, etc.).
5. **Enable Two-Factor Authentication (2FA):**
   - Turn on 2FA on all accounts that support it.
   - Prefer app-based 2FA (e.g., Google Authenticator, Authy) over SMS-based codes.
6. **Stay Informed:**
   - Follow cybersecurity updates from trusted sources.
   - Be cautious of phishing emails claiming to help you with this breach.
7. **Report Concerns to Your IT or Security Team:**
   - If you are part of an organisation, report any suspicious findings or issues immediately for further investigation.

Report Cyber Incidents

Report cyber security incident on the **Mauritian Cybercrime Online Reporting System (MAUCORS - http://maucors.govmu.org/)**

Contact Information

Computer Emergency Response Team of Mauritius (CERT-MU)
Hotline No: (+230) 800 2378
Fax No: (+230) 208 0119
Gen. Info. : contact@cert.ncb.mu
Incident: incident@cert.ncb.mu
Website: http://cert-mu.org.mu
MAUCORS: http://maucors.govmu.org