|  |  |
| --- | --- |
| **Telecommunication Development Advisory Group (TDAG)**  **31st Meeting, Geneva, Switzerland, 20-23 May 2024** | A close up of a sign  Description automatically generated |
|  |  |
|  | **Document** **TDAG-2****4/46-E** |
|  | **8 May 2024** |
|  | **English only** |
| RealTyme SA | |
| Social media messenger apps privacy concerns | |
|  | |
| **Summary:**  Exploitation of Data: Various entities, from advertisers to governments to cybercriminals, may exploit user data for targeted campaigns or cyber threats. Phishing and Malware: Users are at risk of phishing attacks and malware distribution via messaging apps, endangering personal data and device security.  **Action required:**  Action.  **References:**  Analysts reports, and public references | |

|  |
| --- |
| **Lessons learned and suggested best-practices (if appropriate):**  Lessons learned: Prioritize compliance, transparency builds trust, collaborate for solutions, adapt continuously, educate users for safety. |

Regulatory bodies can take several actions against messaging app providers or users to enforce compliance with laws and regulations and address security concerns:

* **Enforcement Actions**: Regulatory bodies may issue fines, penalties, or sanctions against messaging app providers for violating privacy or data protection laws. These enforcement actions serve as deterrents and encourage compliance with regulatory requirements.
* **Investigations**: Regulatory bodies have the authority to conduct investigations into alleged violations of laws or regulations by messaging app providers. These investigations may involve gathering evidence, interviewing witnesses, and examining company records to determine the extent of non-compliance.
* **Compliance Audits**: Regulatory bodies may conduct compliance audits of messaging app providers to assess their adherence to regulatory requirements. These audits help identify areas of non-compliance and provide recommendations for corrective action.
* **Regulatory Guidance**: Regulatory bodies can provide guidance and recommendations to messaging app providers on how to comply with relevant laws and regulations. This guidance may include best practices for data protection, security measures, and transparency in user communications.
* **Licensing and Certification**: Regulatory bodies may require messaging app providers to obtain licenses or certifications to operate legally in certain jurisdictions. These requirements ensure that providers meet minimum standards for privacy, security, and user protection.
* **Consumer Education**: Regulatory bodies may engage in consumer education efforts to raise awareness about potential risks associated with messaging apps and provide guidance on how to use them safely. This may include issuing advisories, publishing educational materials, or conducting outreach campaigns.

Overall, regulatory bodies play a crucial role in promoting compliance and protecting the interests of consumers in the messaging app ecosystem.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_