Principles: Safety and security, Fairness and non-discrimination, Privacy, Transparency and explainability, Responsibility and accountability, Awareness and literacy, Multi-stakeholder and adaptive governance and collaboration
Values: Human Rights , Living in harmony and peace
Stakeholders: Civil society, Public sector, Media, Private sector, Academia, Technical community, International and regional organizations

Personal information at risk when there is a lack data protection norm on new technologies

A Chinese group created the mobile company called Tecno Mobile. It produces and sells low-cost smartphones targeting almost exclusively African markets.

Because of its low price, their products become very attractive to low budget families and can be found all over the continent such as in Ethiopia, Cameroun, Ghana and many more.

Secure-D, an anti-fraud platform finds that malware had been preinstalled in the smartphones. From 2018 up to 2020 it consisted in eating up the mobile data – often very expensive - and registering the people to unwanted subscriptions.

As a response, the Chinese group declared that if users encountered any difficulties with their product, they should simply download the fix through their phones or contact after sales support. They added that this malware was due to an “unidentified vendor in the supply chain process” and that the privacy of their users was essential for the group.

As much as these responses fix to the problem, they are insufficient to properly deal with this kind of abuse. Today, people rely more and more on their digital devices and proper sanctions have to be implemented when such practices occur. Furthermore, this malware targeted poorer families thus taking advantage of their situation which only deepens inequalities.

How could this situation have been avoided in the first place?

Here are our recommendations per stakeholder:

- Developers are encouraged to reinforce security parameters of their applications so that no third party cannot have access to the data.

- Companies should be transparent as to the production process and if third parties intervene in the production process.

- International and regional organization have to take it under their jurisdiction to sanction the foreign influence. It is established that Africa must establish a solid legal and ethical framework to ensure that the digital journey of AI leads to positive outcomes.

- Governments are asked to increase technology related regulations as to sanction abuses and refrain more of them. Awareness campaign on the risk that these technologies present should also be implemented.

- The technical community is encouraged to enhance checks on companies as to find this kind of malware faster.

- Users should be more careful when selecting a product and if a glitch or abnormal thing happen, declare it.

Privacy & Human Rights & Responsibility and accountability & Safety and Security & Fairness and non-discrimination & Transparency and Explainability & Awareness and Literacy & Multi-stakeholder and adaptative governance and collaboration

Know more about this case:

- “Tecno phones in these African countries have malware, but there’s a fix”, Techpoint, https://techpoint.africa/2020/08/26/tecno-malware-risk/

- “Chinese phones with built-in malware sold in Africa”, BBC, https://www.bbc.com/news/technology-53903436

- “China's Tecno sold thousands of smartphones with malware in Africa”, CNN, https://edition.cnn.com/2020/08/26/tech/tecno-malware-africa/index.html