CYBER SECURITY EXPERT ASSOCIATION GHANA

+233-243 841-842
info@cyberexpertgh.org
www.cyberexpertgh.org

4th May 2025

Immediate release

All media houses

Call for Full Transparency and Accountability on the MTN Cyber Security Breach

The recent breach affecting roughly **5,700 MTN Ghana customers** is a grave event. This is not just only about numbers or reputations—it's about the personal data and trust of millions of Ghanaians. The implications are profound therefore any erosion of trust in our telecommunications sector can undermine the digital progress of our entire nation.

Let us be clear. MTN must take full accountability and pursue transparency. The Government's Communications Ministry has already launched an investigation with the Cyber Security Authority (CSA), National Communications Authority, and Data Protection Commission, and these agencies rightly expect MTN to cooperate completely. We expect MTN's leadership to cooperate fully with regulators and share their findings transparently with both the authorities and the public, within legal limits. Leadership means owning problems as well as successes. Ghanaian customers deserve a thorough explanation of what happened and why.

While investigations are still ongoing, CSEAG takes seriously circulating concerns about potential insider involvement in the breach. According to the Bank of Ghana's 2024 Fraud Report, staff-involved fraud across the banking sector including mobile money platforms such as MTN's MoMo is on the rise, which underscores the fact that internal actors can be as dangerous as external attackers. We therefore strongly urge MTN to conduct a rigorous internal review of all personnel with privileged access, to reinforce its pre-employment screening by implementing exhaustive background checks including criminal, financial, and reference verifications before bringing staff into critical roles, and to deploy continuous behavior monitoring and anomaly detection so that any suspicious insider activity is identified and contained in real time. Preventing future breaches means securing not only systems, but also the people who manage them.

We also stress that Cybersecurity is not merely a technical concern, it is a core leadership responsibility. Strong firewalls and encryption are important, but without top-down commitment, they can fail. Whiles we commend MTN's leadership for its ongoing efforts during this incident, we encourage the board and executives to continue treating cybersecurity as a top priority. This includes regularly assessing cyber risks, allocating sufficient resources, and ensuring policies evolve in response to emerging threats. With consistent, proactive engagement from the top, MTN can further strengthen its resilience and cybersecurity posture.

Equally important is having skilled professionals on the frontlines. MTN and other institutions **must invest in qualified cybersecurity experts**. We cannot rely solely on temporary consultants during crises. The fact that MTN is "working closely with leading cybersecurity experts" in the forensic investigation is a good first step. We urge MTN to build and retain an in-house team of specialists. People who understand the systems and can respond instantly at any hour. Ghana's cyber ecosystem depends on building local capacity, and MTN should lead by example.

To MTN customers and the public, please remain vigilant. We strongly advice you to update your mobile and banking apps, use strong, unique passwords, and never share your PINs or OTPs with anyone. These steps are simple but effective. If you receive any communication that seems out of the ordinary, question it. Security is a shared responsibility between companies and citizens.

We, the Cyber Security Expert Association of Ghana, stand ready to support. We will collaborate with MTN's team, the CSA, the Data Protection Commission and all relevant agencies. Whether by providing cybersecurity training, offering technical and advisory services, or helping to design awareness programs, CSEAG is committed to Ghana's digital safety. This moment calls for unity. Our industries, government, and civil societies must work together to reinforce our cyber defences and rebuild confidence.

Key calls to Action:

- **Accountability & Transparency:** MTN must provide clear, timely updates on the breach and take ownership of any lapses.
- **Investment in Talent:** MTN should build a permanent team of skilled cybersecurity professionals.
- **Leadership Engagement:** Cybersecurity must be championed at the executive and board level.
- **Public Vigilance:** Citizens must remain alert and adopt safe digital practices.
- **National Collaboration:** All stakeholders must unite to strengthen Ghana's cyber defences.

In conclusion, this incident serves as a wake-up call. Ghana's digital future depends on strong leadership, robust security practices, and the collective effort of all sectors. We remain committed to ensuring that this challenge becomes a turning point for lasting improvement in our cybersecurity landscape.

Signed,
Abubakar Issaka
President, Cyber Security Expert Association of Ghana (CSEAG)