FIFA Confirms Cyberattack Exposing Personal and Business Information



FIFA says attackers accessed a limited set of personal and business information and that it is working with law enforcement. It has not said when the attack happened or what exactly was taken.

- FIFA says hackers accessed a limited set of personal and business information.
- The organization is working with relevant authorities, including law enforcement.
- FIFA did not state when the attack occurred or the precise nature of the data.
- A group calling itself Handsome Boy Hacking Club posted a screenshot of purported FIFA files on X and later appeared to claim the hack.
- A post claimed more than 12 gigabytes of internal documents were leaked; this is a claim, not confirmed by FIFA.

FIFA, the world governing body for soccer, has said it was the victim of a cyberattack in which hackers gained access to what it calls a limited set of personal and business information. The statement was sent to The Associated Press and reported by SecurityWeek.

What is known

FIFA says it is working closely with the relevant authorities, including law enforcement. It did not say when the attack took place or give the precise nature of the information involved. It condemned the unlawful acquisition and publication of data, particularly personal data, describing it as a serious violation of privacy that can have significant consequences for the people affected.

Last week a group calling itself the Handsome Boy Hacking Club posted a screenshot on X of what it claimed were FIFA files. Three days later it appeared to take credit for the hack, replying to a post that said more than 12 gigabytes of internal documents had been leaked. The size and content of the leak come from those claims and have not been confirmed by FIFA.

Why it matters for regulated institutions

The case is a reminder that organizations with many partners, vendors and stakeholders hold personal and business data that can be published quickly once taken. Many details remain open, so institutions with relationships with large international bodies should avoid assuming impact either way and instead check their own exposure calmly.

What to do now

1. Check whether your organization shares personal or business data with FIFA or its affiliates, and ask the relevant contacts for any notification they intend to issue.
2. Review which third parties hold your staff, customer or partner personal data and confirm their incident notification obligations in contracts.
3. If your data may be involved, assess it under PDPL requirements and the SDAIA notification timelines, and document the decision.
4. Brief staff who may be targeted with phishing that references leaked documents, and remind them to report suspicious messages.
5. Make sure your incident response plan covers publication of stolen data by threat actors on social media, including communications and legal steps.