FIFA confirms hackers accessed a limited set of personal and business data



FIFA confirmed unauthorised access to a limited set of personal and business information. A group called HBHC claims it took over 12 GB and published it; FIFA says it is working with law enforcement.

- FIFA confirmed hackers gained unauthorised access to a limited set of personal and business information.
- The group Handsome Boy Hacking Club (HBHC) claims it stole more than 12 GB and failed to extort FIFA before publishing the data on a cybercriminal forum.
- The group claims it accessed FIFA's Microsoft environment; the alleged data includes identity, immigration, financial and legal documents.
- FIFA says it is working with relevant authorities, including law enforcement, and did not answer

questions on the incident's nature.

- The case follows other recent attacks on European football bodies, including LaLiga and its clubs.

FIFA, the international football governing body headquartered in Zurich, has confirmed that hackers breached its systems and gained unauthorised access to what it describes as a limited set of personal and business information. A spokesperson said the organisation is working with the relevant authorities, including law enforcement, and condemned the unlawful acquisition and publication of personal data. FIFA did not answer follow-up questions about the nature of the incident.

What is claimed

The Handsome Boy Hacking Club (HBHC), a group that emerged only last week and about which little is known, says it stole more than 12 GB of data and tried unsuccessfully to extort FIFA. It then published the data on a cybercriminal forum and claimed it had accessed FIFA's Microsoft environment. The alleged contents include identity and immigration documents, financial records, legal documents and governance information. These are the group's claims; FIFA has only confirmed a limited set of personal and business data.

Wider context

The incident follows other attacks on European football. LaLiga said hackers stole fans' personal information in an attack affecting its digital services and those of several Spanish clubs, Dutch police arrested a suspect over the hacking of Ajax in May, and the French Football Federation disclosed an attack in 2025.

For Saudi institutions, particularly those working with sports bodies, event organisers or international partners, the case is a reminder to check exposure through third parties and cloud environments, and to be ready to assess claims of leaked data quickly and calmly.

What to do now

1. Review which personal and business data shared with sports bodies, event organisers and other international partners could be exposed through their systems.
2. Check Microsoft cloud tenant security: administrative access, multi-factor authentication, sign-in logging and alerting.
3. Monitor credible sources for mentions of your organisation or staff in leaked datasets, and verify claims before reacting.
4. Confirm your incident response plan covers extortion attempts and data publication, including notification duties under PDPL.
5. Remind staff, especially those whose identity or travel documents are shared with partners, to watch for targeted phishing.