Help Center

Select Languange / Pilih Bahasa: English

Star Media Group
Help & Information Center

This platform serves as a one-stop information centre related to the data breach incident involving the StarSearch and ESG Awards databases.

The FAQs section is to address any questions that may arise from the notification from Star Media Group (SMG) sent out on 4 November 2026 to the affected individuals.

These FAQs will be updated from time to time to reflect the latest information and developments.

*Note: Star Media Group will **never** ask for your password, banking OTP, or credit card numbers regarding this incident.*

Check if your email is affected:

Your email address | Check

Have a question? Type a keyword and click Ask Us:

Type in your enquiries here | Ask Us

Contact Us:

Email:
helpcenter@starmediagroup.my

Hotline:
1-300-88-7827

Operating Hours:
Between 9.00 AM and 5.00 PM daily from 4 November until 13 November 2026.

Subsequently, the hotline will be available from 9.00 AM to 5.00 PM, Mondays to Fridays.

Or you may go through our FAQ here:

What happened?

We detected a breach in our StarSearch (Classified section) and ESG Award database. These were the only databases that were affected, with SMG maintaining data integrity throughout the rest of the group.

StarSearch
Data exfiltrated: First Name, Last Name, Address, State, Country, Phone, Email, NRIC

ESG Awards
Data exfiltrated: First Name, Last Name, Mobile number, Email, Password

When did it happen?

We confirmed the exfiltration of personal data on 27 October 2026 and notified the Personal Data Protection Commissioner on 30 October 2026.

Who did it?

The investigation is ongoing, and those responsible have not yet been identified. As of to date, we have not received any ransom demand or other demands in connection with the incident.

How did it happen?

Our investigation indicates that the attackers exploited a vulnerability in one of our applications to gain unauthorised access.

What is being done?

We have contained the incident, engaged independent cybersecurity specialists, strengthened our security controls and enhanced our monitoring.

Have the authorities been notified?

We have filed a Data Breach Notification with the Commissioner of Personal Data Protection in accordance with Section 12B of the Personal Data Protection Act (PDPA) and also filed a police report with the Royal Malaysian Police (PDRM).

What are you doing to prevent this from happening again?

We are strengthening access controls, authentication and security monitoring, alongside an independent review of the affected systems. We are also applying security updates and reinforcing security awareness across our teams.

The findings will guide further improvements across SMG to reduce the risk of similar incidents.

Why did it happen?

The motive remains unknown, and the investigation is ongoing. The affected personal information could be misused for phishing, scams or identity fraud. We therefore encourage affected individuals to follow the precautions outlined below.

What should I do now to protect myself?

- Be Vigilant Against Phishing and Scams
  - Be cautious of unexpected phone calls, WhatsApp messages, SMS, or emails claiming to be from government agencies, banks, telecommunication providers, or delivery couriers – even if the caller quotes your exact NRIC or address.
- Do Not Disclose Verification Codes
  - Never provide OTPs, TAC codes, banking passwords, or identity documents to anyone contacting you unsolicited.
- Do Not Click On Unverified Links
  - We will never ask for your login details or passwords. If you receive a message asking for this information, do not click on any links.

Will my bank account be hacked?

The affected databases did not contain your banking details, such as bank account numbers or payment card information. These details were therefore not exposed in this incident. Exposure of your personal details does not, by itself, give someone access to your bank account.

However, scammers may use those details to make calls or messages appear genuine. Never share your banking passwords, PINs, OTPs or TAC codes, or approve transactions you did not initiate. If you notice unusual activity or receive a suspicious request, contact your bank using its official contact details.

ESG Awards Password Reset

For ESG Awards users, your ESG Awards account login credentials were among the information affected by the incident. While your password was stored in encrypted form, we are requiring all affected users to reset their passwords as a precautionary security measure. You can reset your password by following these steps:

1. Visit the official ESG Awards website by manually typing the URL into your browser.
2. Enter your registered email address and existing password on the login page.
3. Upon entering your existing password, the system will automatically send a password reset email to your registered email address.
4. Open the password reset email and click the secure link provided to create a new password. Please note that the password reset link will expire after one (1) hour.
5. Once your password has been successfully reset, you may log in using your new password.

If you have used the same password for other online accounts, we strongly recommend changing those passwords as well. We also encourage you to use strong, unique passwords for each account and enable two-factor authentication wherever available.

For assistance, you can contact our dedicated data protection support team at helpcenter@starmediagroup.my or 1300 88 7827 between 9.00 AM and 5.00 PM daily until 13 November 2026. Subsequently, the hotline will be available from 9.00 AM to 5.00 PM, Mondays to Fridays. Please manually type this address https://www.starmediagroup.my/helpcenter directly into your browser for verified information and updates.

Last updated: 5 November 2026

Star Media Group Berhad [197101000523 (10894-D)] © 2026 | All Rights Reserved