

Cyber Incident Helpline on 6890 9555 offers free first-response help to Singapore businesses on weekdays

Description

default watermark

Organisations in Singapore that are hit by a cyber incident can now call a dedicated Cyber Incident Helpline on 6890 9555 for first-response advice on weekdays from 8am to 6pm, at no cost to businesses. The Cyber Security Agency of Singapore (CSA) said the helpline was launched on 14 October by Senior Minister of State for Digital Development and Information Tan Kiat How, alongside the Singapore Cybersecurity Health Report 2025, which found that almost nine in 10 organisations surveyed had at least one incident last year.

The Cyber Resilience Centre (CRC), set up by the Singapore Business Federation in 2025 with the Singapore Chinese Chamber of Commerce and Industry and SGTech and with CSAâ??s support, runs the service. RSM Stone Forest IT manages the helpline.



The Cyber Incident Helpline on the Cyber Resilience Centreâ??s website: 6890 9555, Monday to Friday, 8am to 6pm except public holidays. Crop of the CRC page: Cyber Resilience Centre

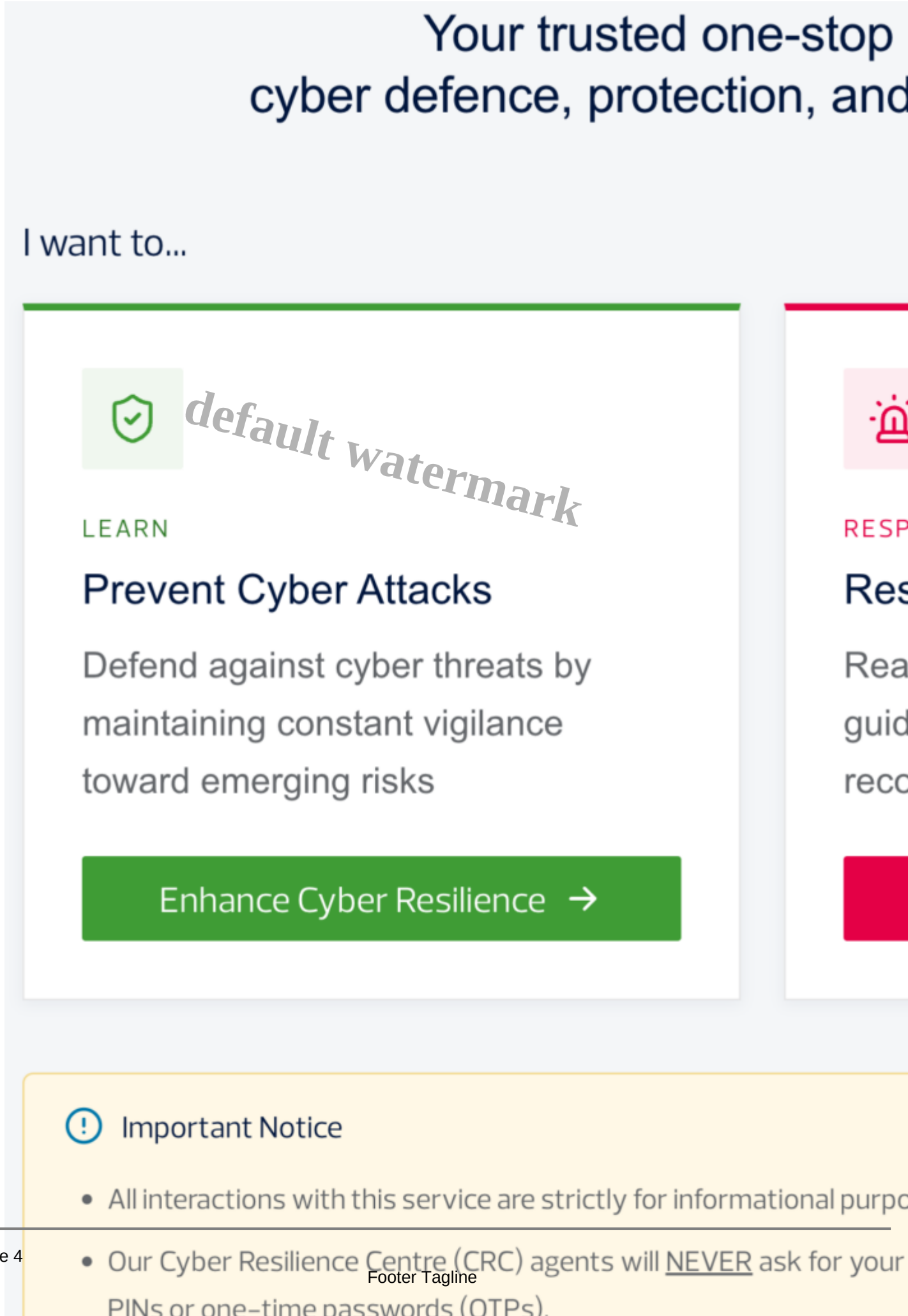
What the helpline does

The helpline gives initial incident triage, advice on containing an attack, and referrals to service providers and resources for recovery. Any organisation can use it, whether it is preparing for an incident or already in one. Callers can also submit a request online.

A request made during operating hours is meant to get a callback within two hours from the same 6890 9555 number. A request made outside Monday to Friday, 8am to 6pm, or on a public holiday, is attended to on the next working day.

The limits are set out as plainly as the services. The CRC does not do remote technical troubleshooting, digital forensics evidence collection, data restoration, audit log reviews or system configuration changes, and it does not act as the incident responder or report incidents to the authorities. Where deeper help is needed, it refers the organisation to a provider. Its agents will never ask for bank details, passwords, PINs or one-time passwords.

default watermark


Your trusted one-stop
cyber defence, protection, and
I want to...
default watermark
LEARN
Prevent Cyber Attacks
Defend against cyber threats by maintaining constant vigilance toward emerging risks
Enhance Cyber Resilience →
RESP
Res
Rea
guid
reco
Important Notice
All interactions with this service are strictly for informational purpo
Our Cyber Resilience Centre (CRC) agents will NEVER ask for your
PINs or one-time passwords (OTPs).

The CRC portal splits its help into prevention and response, and carries a notice that its agents never ask for passwords or one-time passwords. Crop of the CRC page: Cyber Resilience Centre

What the 2025 survey found

CSA surveyed 2,005 businesses and non-profit organisations of varying sizes between October and November 2025. Ransomware was the most commonly reported incident for both groups, followed by compromised credentials and social engineering such as phishing and impersonation scams.

Reported impacts were lower than in the 2023 survey. Among businesses, the share reporting incident response costs fell by 3.8 percentage points, business disruption by 3.1 points and financial losses by 2.7 points. Non-profits recorded larger falls: 18.4 points for data loss, 8.2 for business disruption and 7.4 for financial losses.

Adoption of the five categories of measures in CSAâ??s Cyber Essentials mark ranged from 71 per cent to 80 per cent. Software and system updates were highest at 80 per cent, while asset management and asset protection were lowest at 71 per cent each. Among businesses, 56 per cent cited a lack of knowledge and experience as a challenge, 46 per cent saw themselves as unlikely targets and 37 per cent cited insufficient manpower and resources.

default watermark

Other support for smaller firms

CSAâ??s CISO-as-a-Service programme lets organisations engage consultants to draw up a tailored cybersecurity plan, with up to 70 per cent co-funding for eligible SMEs. The CRCâ??s clinics and workshops have reached close to 500 organisations, and another 300 are expected to take part in a phishing simulation exercise.

Date Created
10/11/2026
Author
vanessakoh