

Re: Cyber Security Attack on ECSA Website

The Engineering Council of South Africa (ECSA) between Tuesday, 09 September and Wednesday, 15 September 2026, experienced a cyber security attack on its official ECSA website.

During this period, an unauthorised individual targeted Windows computer users and added a code displaying a fraudulent "Verify You Are Human" page that impersonated Cloudflare before users could access the website.

Upon becoming aware of the incident, ECSA immediately implemented measures to secure its technical environment. The threat was successfully identified and removed on 15 September 2026, and the website was declared safe for use on the same day.

A preliminary investigation into the source, scope, and potential impact of the incident found no evidence of a data breach and no indication that ECSA's Cloudflare service was compromised.

The investigation further established that approximately 7,000 users visited the website while the malicious code may have been active. It is important to note that visiting the website does not necessarily mean a visitor was affected. For harm to occur, the following sequence of events would have had to take place:

Step	What had to happen	What we know
1.	The person visited the website	About 7,000 visitors (9–15 September).
2.	The fake "verify you are human" page was shown to them	Aimed mainly at Windows computers and hidden from some visitors. Once browsers and antivirus flagged the site as "Dangerous", many visitors were blocked before the page loaded.
3.	They followed the instructions: opened Terminal, pasted and ran the command	Requires deliberate, unusual actions, so only a minority of those shown the page would do this. It cannot be measured from the website, because it happens on the visitor's own computer.
4.	Harmful software was installed on their computer	Possible for anyone who completed step 3. The software can steal saved passwords, email and banking logins, and can give the attacker remote access.

Stakeholders who believe they may have completed **Step 3** are strongly encouraged to seek immediate assistance from their ICT support teams or qualified IT service providers to determine whether their devices or personal information may have been compromised.

ECSA is continuing its investigation into the incident. Should any new information emerge or further actions become necessary, additional communications will be issued to keep stakeholders informed.

ECSA sincerely regrets any concern or inconvenience caused by this incident and remains committed to protecting the security and integrity of its digital platforms

ISSUED BY THE ENGINEERING COUNCIL OF SOUTH AFRICA