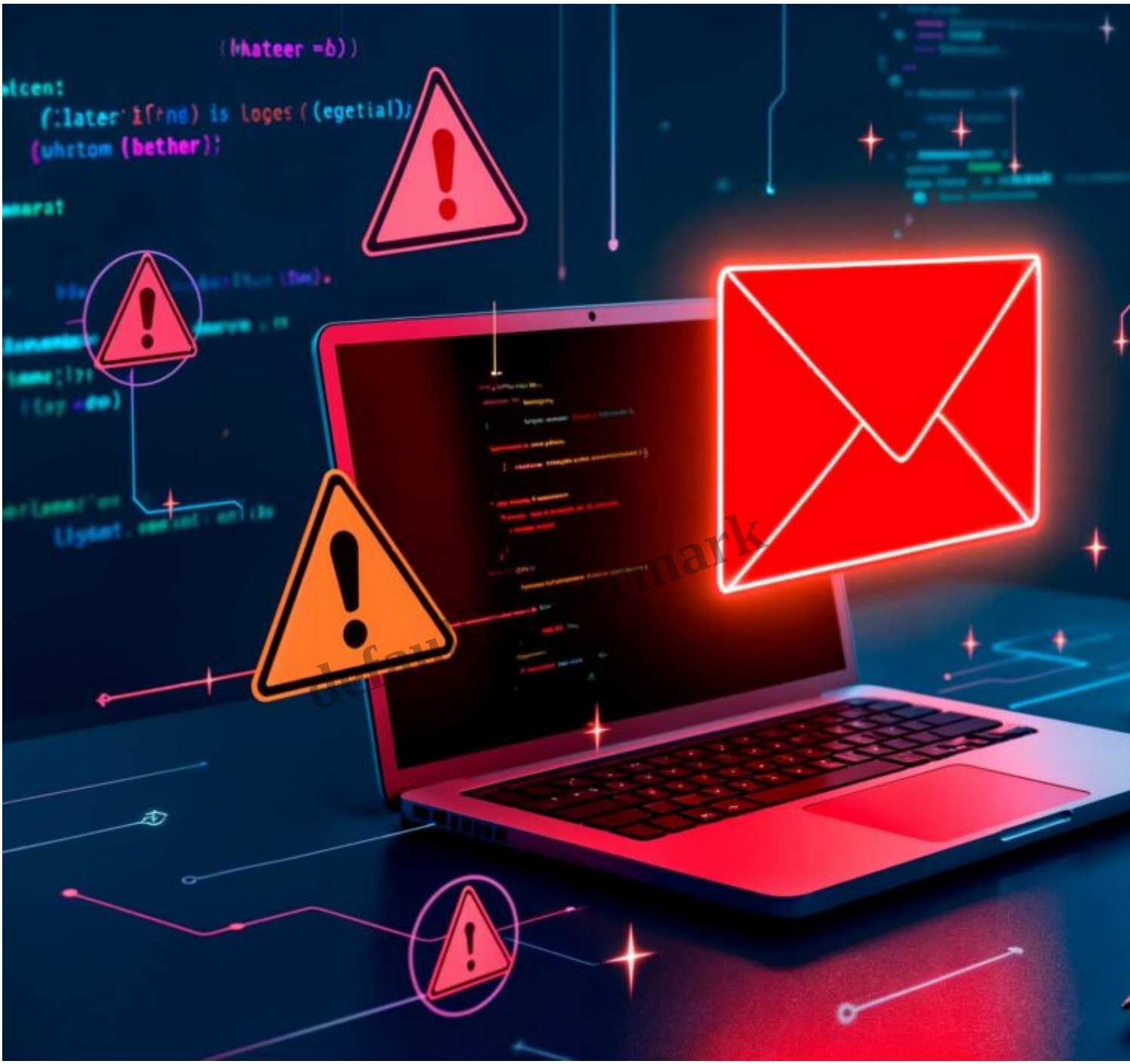
Don’t be held to ransom

Description

South Africa is the most targeted country in Africa for ransomware and attacks to steal information, which means it’s critical for each of us to play our part in protecting our business.

The State of Ransomware in South Africa Report 2025, compiled by cybersecurity firm Sophos, says the median ransom demanded increased from R2,9 million in 2024 to R17 million this year, with the firms who came under attack paying just over 60% of the demand.

A survey of 3 400 IT and cybersecurity professionals working in affected organisations found that compromised credentials were the most common cause of security breaches, accounting for 34% of all successful attacks. This is followed by exploited vulnerabilities and malicious emails.



Over the past two years, ransomware organisations have claimed credit for attacks on a range of organisations, from banks and hospitals to medical testing laboratories, universities and government.

What is ransomware?

Ransomware is a malware that blocks access to an organisation or user's data or computer systems by encrypting files until a ransom is paid. Cybercriminals typically gain access to an organisation's sensitive data through phishing emails, malicious downloads, or users clicking on unsafe links. Once

activated, the ransomware displays a message demanding payment, usually in untraceable cryptocurrency, before a decryption key is provided to unlock and recover the data or system access.

Help keep our business safe

To stay ahead of cybercriminals, here are five tips to spot and avoid ransomware:

1. **Be wary of emails:** Watch for emails with unfamiliar senders, urgent language, or unexpected attachments.
2. **Verify links before clicking:** Hover over hyperlinks in emails or messages to check their actual destination.
3. **Keep software updated:** Regularly update your system and applications to ensure they're protected against the latest known vulnerabilities.
4. **Use strong passwords:** Use unique, complex passwords and change them regularly. Avoid using the same password across different systems.
5. **Back up data:** Ensure critical data is continuously backed up to a secure, offline location, which can help to minimise damage in case of an attack.

By staying vigilant and proactive, we can build a human shield against ransomware threats. Remember, you are our first line of defence. If you notice any suspicious activity, from strange emails to sudden system changes, report it immediately.

Category

1. Our Knowledge Centre