security quotient.

Suspicious documents in your inbox?

Think twice before opening them!

Beware of document based phishing!

Attackers send documents as email attachments to deliver malware or fake website links, prompting victims to share sensitive data or download harmful software. Here are 4 tips to stay safe!

Verify the source

If an email seems suspicious but appears to be from someone you know, contact them directly using a trusted method to confirm whether they really sent it.

Check for unusual file names

Don't open file attachments with strange names or unusual file extensions (like ".bin" or ".scr").

Avoid scanning QR codes

Don’t scan QR codes or click on links/buttons in documents unless you’re sure they come from a trusted and verified source.

Look for signs of corruption

If you open a document and it shows "unreadable content" or asks you to "recover" it, treat it as suspicious and proceed with caution.

“

Make your workforce cyber resilient

security®
quotient.

Singapore | India | Malaysia