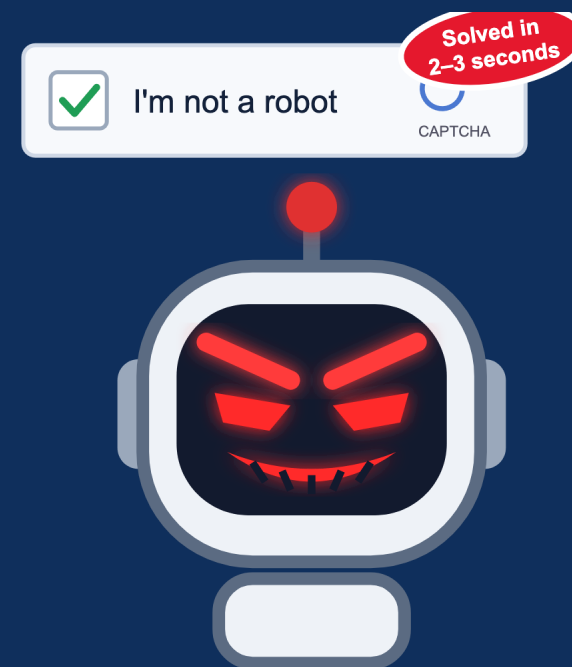




Is CAPTCHA Enough to Stop AI-Enabled Bots?

Why SMEs need more than just CAPTCHA



Need cybersecurity support? Visit www.csa.gov.sg/cybersecurityhealthplan

1

CAPTCHA Helps

Many SMEs use CAPTCHA to protect:

 Logins

 Registrations

 Bookings

 Online purchases



Type the characters



I'm not a robot



CAPTCHA



CAPTCHA is a useful check against basic bots. But hard puzzles can also turn away real customers.

2

But Bots Are Getting Smarter

Modern AI-enabled bots can:



I'm not a robot

Solved in
2–3 seconds



Solve image and audio CAPTCHAs in seconds, at very low cost



Use real web browsers and act like real users



Try leaked passwords on your login page



Create many accounts and flood you with requests



AI-enabled bots can now bypass most CAPTCHAs, cheaply and at scale.

3

What Could Happen?

AI-enabled bots can abuse your website and business processes, leading to:



Customer accounts taken over

Bots try leaked passwords until one works, then use the account.



Fake account creation

Many accounts are created to boost their chances of success.



Booking or registration abuse

Bookings or registrations are submitted automatically in bulk.



Limited stock snapped up

Bots buy scarce items first, so genuine customers miss out.



AI-enabled bots target business processes, not just websites.

4

Protect Your Business

Use a layered approach, strongest layer first:



Offer passkeys or MFA

Let customers sign in with a passkey (fingerprint, face or device PIN), or MFA if passkeys aren't available.



Step up when something looks off

New device, new country or many failed tries? Ask for a passkey or second factor, not a harder puzzle.



Limit attempts per account

Rate-limit by account, not just by IP address, and block passwords known to be leaked.



Protect bookings and purchases

Use queues and purchase limits for scarce slots and stock.



Guard password reset too

Protect reset and recovery like the login. Alert customers when a password or device changes.



Keep CAPTCHA as an extra check

Useful on sign-up, contact and booking forms. Don't rely on it alone.

5

Keep Your Accounts Tidy

Fewer unused accounts means fewer accounts for bots to take over.



Review who has access

Check staff and admin accounts every few months. Each person gets only the access their job needs.



Remove leavers promptly

Disable accounts for ex-staff, contractors and vendors on their last day.



Clean up dormant accounts

Disable staff accounts unused for a set period (e.g. 90 days). Ask returning customers to verify again.



No shared or default logins

Give every admin their own account with a passkey or MFA. Change default passwords on new systems.



Key Takeaway for SMEs

Modern bot protection needs multiple layers of defence.

Combine:



Passkeys or
MFA

+



Step-up
checks

+



Rate
limiting

+



Transaction
controls

+



Monitoring
and alerts

+



Access
reviews

+



CAPTCHA
(extra
check)

Need cybersecurity support? Visit www.csa.gov.sg/cybersecurityhealthplan

