Helping you tackle cyber risks

Most cyber attacks exploit people and processes through manipulation rather than technical or system weaknesses.

Access training to protect your business

Medium to large businesses can follow the National Cyber Security Centre framework

A 10-step framework covering the key areas companies should address to manage cyber risk and strengthen security.

10 steps to cyber security

Train all staff to recognise cyber threats

Practical guidance to help non-technical employees recognise and avoid the most common cyber threats.

Training for all staff

Prepare board members, directors and senior executives

Strategic training for senior leaders responsible for organisational risk. Understand cyber risk, governance issues and how to manage it.

Board cyber training

All training provided by National Cyber Security Centre.

Nominate a cyber contact

Tell us who the cyber contact is in your business so we can share relevant updates on recent attacks and guidance to prevent them.

Speak to us

If in doubt, speak to your relationship team for advice on training or potential attacks.

Santander

Did you know?

1 in 3 SMEs will not survive a cyber attack.

Scaling businesses are 4x more likely to experience a cyber attack.

70-74% medium/large businesses reported a cyber breach or attack. Only **32% have a business continuity plan** that includes cyber security.

8 out of 10 SMEs experienced a cyber attack last year, showing that cyber security doesn't always keep up with business growth.

Attacks making headlines

M&S – ransomware attack

- £300m losses in operating profit
- £700m wiped from stock prices in first 2 weeks
- 2.5 months to return to partial online operations

Jaguar Land Rover – ransomware attack

- 5000 supply chain organisations impacted
- £2bn cost to economy
- 6 to 7 weeks downtime