

# Cyber Security

The UK Financial Conduct Authority (FCA) received 116 reports of material cyber security incidents in 2021, a fifth of which involved ransomware. This is a 52% increase from 2020. This news is set against a backdrop of increasing cyber security concerns in light of the conflict in Ukraine.

Organisations need to ensure that the fundamentals of cyber security are in place. But that doesn't just mean firewalls and patching. Staff also play a vital role in protecting systems and information from cyber criminals. So it is important that everyone within an organisation understands the risks and takes steps to mitigate them.

## #1

### Protect data and devices

Electronic devices, such as **laptops and smartphones, must be kept secure**. For example, make sure you use strong passwords and that your malware protection is up to date.

Always follow your firm's procedures regarding remote access and the use of electronic communications.

## #2

### Be alert to scams

**Don't click on links or open attachments**, even on internal emails, unless you are sure that they are legitimate.

Email and SMS scams can be personalised and sophisticated, so if you are in any doubt about an electronic communication, get confirmation that it is genuine.

## #3

### Report concerns

If you think that an information security breach may have occurred, or you are concerned that risks are not being properly managed, **report the issue immediately**, following your firm's procedures.

If a breach occurs, prompt reporting can help to reduce the impact.

