Insider Threats

Not all security risks come from hackers outside the organisation. Sometimes the danger comes from within. Insider threats can be intentional, such as theft or sabotage, or accidental, like mishandling sensitive data. Both can have devastating consequences for a business.

Types of Insider Threats

Malicious Insiders

Disgruntled employees or contractors may deliberately steal data, damage systems, or leak information for personal gain or revenge.

Tip: *Report unusual or suspicious colleague behaviour immediately.*

Careless Mistakes

Well-meaning staff can also create risks by misplacing devices, sending files to the wrong person, or ignoring security procedures.

Tip: *Follow company policies for data handling and storage at all times.*

Excessive Access

Employees with more access than they need can unintentionally (or intentionally) misuse it. Limiting permissions reduces the damage insiders can cause.

Tip: *Access should always be restricted to only the files and systems required for the role. This is called "Least privilege access".*

Detecting and Responding

Insider threats can be harder to spot than external ones. Being alert to unusual activity, like unauthorised access attempts or irregular downloads, helps protect the organisation.

Tip: *Stay vigilant and report any security concerns without delay.*