

Insider threats

An insider threat occurs when someone with legitimate organisational access uses that access to harm the organisation. These threats are particularly dangerous because they come from trusted individuals who already have system permissions, making them harder to detect than external attacks.

The three main types of insider threats:

- Malicious insiders
- Negligent insiders
- Compromised insiders

Key takeaways:

- **Implement least privilege access** - employees only get access to what they need
- **Complete all cybersecurity and data protection training that is required of you** - make sure you understand your organisation's policies on data access and acceptable use
- **Not all insider threats are deliberately malicious** - You can cause security incidents through carelessness, such as falling for phishing scams, using weak passwords, sharing credentials, or bypassing security protocols.
- **Security is everyone's responsibility** – we all must remain vigilant and report anything that can cause a data breach