Supply Chain Attacks

Hackers don't always target organisations directly. Instead, they exploit third-party vendors, partners, or service providers to gain access. Because businesses rely heavily on external software and suppliers, supply chain attacks are becoming one of the fastest-growing cyber threats.

How the Attacks Work

Compromised Software Updates

Attackers inject malicious code into legitimate software updates. When companies install them, they unknowingly spread malware across their systems.

Tip: *Always update software from official, trusted sources.*

Stolen Vendor Credentials

Hackers may steal or buy login details from vendors, then use them to infiltrate client networks. Since the credentials belong to a trusted partner, the attack often goes unnoticed.

Tip: *Limit vendor access to only the systems and data they need.*

Exploiting Service Providers

From cloud platforms to delivery services, attackers look for weak security in providers to move up the chain and reach larger organisations.

Tip: *Vet vendors carefully and ensure they meet your company's security standards.*

Reducing the Risk

Even trusted vendors can be compromised, so ongoing monitoring is critical.

Tip: *Track third-party activity closely and act quickly on unusual behaviour.*