

Deepfakes in the Workplace

Deepfakes are AI-generated videos or images designed to look real but created to deceive. As the technology improves, spotting what's fake is becoming harder.



How Attacks Happen



Fake Executive Requests

Attackers can create convincing videos of CEOs or managers instructing staff to transfer money or share sensitive information. Because the message appears to come from leadership, employees may act without question.

Tip: *Never act solely on video instructions — always confirm by phone, email, or in person.*

Spreading Misinformation



Deepfakes can also be used to harm reputations by showing employees, leaders, or companies saying or doing things that never happened. These fakes can cause panic, confusion, or reputational damage.

Tip: *Report suspicious or odd-looking videos immediately so they can be investigated quickly.*



Why They're Dangerous

Deepfakes exploit trust in visual content. People are wired to believe what they see, making these attacks especially effective in fast-moving workplaces.

Tip: *Treat unusual video requests with caution and verify before acting.*