Beazley Logo

Article

# Social engineering: an analogue trick in a digital age

### What is social engineering?

Social engineering is used by criminals to trick employees into doing something that enables the criminal to defraud a company of money or to gain access to IT networks evading usual security protocols to steal funds.

Social engineering scams are becoming even more successful and seemingly authentic as hackers use personal information about the target, such as their name and phone number – usually easily available on social media. The rise of remote working and virtual meetings has led to an increase in online scams often using ‘deepfake’ videos and audio files impersonating senior executives requesting other members of staff to transfer urgent payments to ‘clients’.

Once the victim has fallen for the initial approach and taken the desired action, the fraudster will manipulate and mislead the unsuspecting Employee into voluntarily releasing funds or sharing valuable data. Social engineering scams can remain undetected for a long period of time, causing significant losses, embarrassment and potential reputational damage to both individuals and the organization.

### Why should you care?

European consumers are being targeted by increased attempts at social engineering attacks, according to ENISA Threat Landscape report 2025. “Phishing continued to be the primary method for initial intrusion, remaining an effective technique to carry out credential theft, session hijacking, payload deployment or command execution”.

### Human safeguards matter

Employee training and strong payment verification controls are critical. Process and sign off procedures are key. Businesses should ensure that requests to transfer funds, change payment instructions or release sensitive information are independently verified through a trusted channel, particularly when the request is urgent, unusual or involved senior leadership.

## Insurance can add a valuable layer of protection

Social engineering claims can fall into the grey area between crime and cyber exposures, leaving clients without adequate protection. A dedicated Commercial Crime policy covers digital crime, including fraudulent instruction coverage for losses resulting from theft, fraud or deception from social engineering can add a valuable layer of financial protection.

Find out more

For Crime offering: Commercial Crime | beazley

Home