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?

UK consumers are being targeted by increased attempts at social engineering attacks, according to a report by BioCatch. With Phishing attacks in the UK rising by 140 percent in 2025, businesses and individuals need to be aware.

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 Int’l Crime offering: Commercial Crime (non US) | beazley

For US Crime offering: Fidelity and Crime | beazley

The information contained herein is intended as general risk management information. It is made available with the understanding that Beazley does not render legal services or advice. Although reasonable care has been taken in preparing the information contained herein, Beazley accepts no responsibility for any errors it may contain or for any losses allegedly attributable to this information.

The descriptions contained herein are preliminary and for informational purposes only. The product is available on an admitted basis in some but not all US jurisdictions through Beazley Insurance Company, Inc., located at 30 Batterson Park Road Farmington, CT 06032, and on a surplus lines basis through licensed surplus lines brokers underwritten by Beazley syndicates at Lloyd’s. The exact coverage afforded is subject to and governed by the terms and conditions of each policy issued. The publication and delivery of the information contained herein is not intended as a solicitation for the purchase of insurance on any US risk. Beazley USA Services, Inc. is licensed and regulated by insurance regulatory authorities in the respective states of the US and transacts business in the State of California as Beazley Insurance Services (License#: OG55497).

Home

©Beazley Group | LLOYD's Underwriters