CHUBB®

Social Engineering Fraud: A Growing Crime Problem

New Technologies, New Risks

Artificial intelligence has changed the way that criminals are targeting corporations. Deepfakes and other business email compromise attacks are broadening companies' exposure.

Deepfakes But Real Losses

Criminals today use deepfake technology to clone voices and video so realistic that even those who work most closely with executives being impersonated cannot tell that the images or audio have been computer-generated.

Are Private Companies & Not-for-Profit Organizations prepared?

The Federal Bureau of Investigation's 2024 Internet Crime Report notes that business email compromise – the general name given to scams in which cybercriminals impersonate executives or other leaders to trick employees into releasing money or sensitive information – accounted for more than $2.7 billion in reported losses last year in the U.S., spread out over more than 21,000 reported incidents.

More than half of executives surveyed said that their companies have already been impacted by AI deepfake activity.[1]

Social Engineering Fraud Risk Management

Private Companies and Not-for-Profit Organizations can take steps to mitigate their risk and also transfer some of the impersonation risks to insurance.

Strengthen security protocols, learn about best practices, and see loss scenarios in Chubb's Guarding Against Email Social Engineering Fraud booklet. Additionally reference Chubb's "Write It Down" Guidelines, which provide a framework for documenting vendor management processes to help prevent social engineering fraud.

Insure against social engineering fraud with coverage built into ***The ForeFront Portfolio®***:

- Includes coverage for a range of social engineering fraud losses, including executive impersonation, vendor/supplier impersonation, and client impersonation.
- No requirement for vendors and/or suppliers to carry crime insurance to trigger coverage.
- Coverage for impersonations made in any form, whether communicated in person, on the phone, over email or online.
- Optional language that allows the social Engineering Fraud retention to be reduced by any applicable amounts paid by a Cyber policy.
- Social Engineering Fraud Coverage limits offered on a per occurrence basis.
- Primary limits up to and beyond $1m may be available subject to underwriting. Excess capacity is also available.

Loss Scenarios

The Deep Faked CEO and Band of Accomplices

The treasurer of a manufacturing company receives an urgent email from the CEO inviting her to a video call about a confidential matter. During the call, the treasurer sees what appears to be the CEO, along with other faces and voices that the treasurer recognizes as colleagues. The imposter explains that an immediate wire transfer is needed to finalize a critical business deal. Trusting the authenticity of the video call, the treasurer completes the transfer. Later, they discover the real CEO was unaware of the transaction, and cybercriminals had used deepfake technology to impersonate the CEO.

Pressure from Executive

An accounting employee receives fraudulent emails from a partner of the company, claiming he is traveling and urgently needs several wires sent within the next few days to complete a real estate transaction. The fraudsters had gained access to the partner's online email account and sent messages directly from it. To avoid detention, they created rules in the email system to automatically route all correspondence automatically to a hidden mail folder, ensuring the partner never saw the emails requesting the wires. Trusting the legitimacy of the emails, the accounting employee sends the wires, which are later routed from the U.S. bank account to an overseas account controlled by the fraudsters. The fraud was discovered when the bank calls the partner to confirm details about one of the wires.

[1] Chubb Risk Decisions 3600, Emerging Risks That Can Impede Sustainable Company Growth

11/2025