Brown & Brown

PROPERTY & CASUALTY

AI Social Engineering
Through the Decades

By, Morgan Griffith and Shawn Harris

By the late 1970s, space-themed TV shows were everywhere, and one of the most recognizable was Battlestar Galactica. The story arc of robots being used to attack humanity is not only a tried-and-true storytelling vehicle for Hollywood but also represents the evolution of Cyber Fraud and Social Engineering.

Just as the robots were easily identified and recognized in the late 1970s, the methods of fraud were similarly rudimentary. Many of us still recall the first waves of the "Nigerian Prince" email scams.

However, using AI alongside the tricks of old social engineering has created a new era in which our eyes and ears can be used against us. It is vitally important to understand how the technology of 2025 has advanced and is being deployed by criminals in cyber fraud and social engineering schemes.

The Old Face of Cybercrime

Throughout the 1970s and 1980s, pioneering hackers demonstrated how persuasion and impersonation could bypass expensive physical and technical security controls. The techniques of dumpster diving for sensitive information, posing as maintenance works and manipulating call center employees to reveal passwords all established the foundations of what would later be categorized as social engineering.

The early 2000s marked a transformative period for social engineering; as organizations worked to increasingly digitize their operations, attackers shifted from more purely technical exploits to targeting the human element. Companies began witnessing more deliberate attacks, including spear phishing aimed at executives. Security experts responded by developing the first comprehensive social engineering frameworks and security awareness training emerged to address this growing threat.

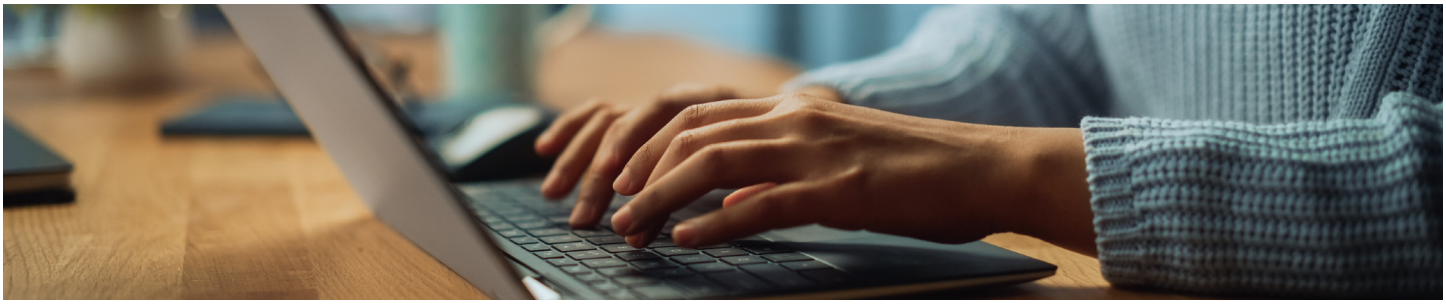
Examples

1. In the 1990s, Kevin Mitnick used social engineering to breach several companies, including Motorola, Nokia and Sun Microsystems, by persuading employees to reveal passwords and security information.[1]

2. In 2004 and 2005, social engineering tactics were used alongside technical exploits in a breach that exposed 40 million credit card accounts from multiple companies, eventually leading to Cardsystems' bankruptcy.[2]

1. Kevin Mick

2. Cardsystems



The New Face of Cybercrime

AI is dramatically transforming social engineering attacks by enabling cybercriminals to create more convincing and personalized deceptive content at an unprecedented scale and speed. The FBI has reported over $17.5 billion in losses from Business Email Compromise (BEC) schemes between June 2016 and December 2023, with AI technologies increasingly being used to make these schemes more convincing.[3] The Deloitte Center for Financial Services projects that AI-enabled fraud losses could reach $40 billion by 2027 across the United States.[4] Generative AI has enhanced cybercriminals' capabilities to create convincing, deceptive content in messaging, audio and video formats, making their schemes increasingly challenging to detect.

Modern AI tools enable attackers to build detailed victim profiles from public information for highly focused phishing. At the same time, voice cloning and deepfake technologies allow convincing impersonations of trusted contacts in calls and video conferences. AI-powered chatbots can simultaneously engage multiple victims, learning from interactions to improve their persuasiveness and adapt their approach based on targeted responses.

Automating these previously labor-intensive attacks has lowered barriers to entry for cybercriminals while simultaneously making detection more difficult as AI-generated content becomes increasingly indistinguishable from authentic human communication. Organizations now face the challenge of developing equally sophisticated AI-powered defenses while educating employees about these evolving threats in a technological arms race between attackers and defenders.

Examples

1. In 2024, fraudsters successfully tricked a British engineering company employee in Hong Kong into transferring $25.5 million. Authorities suspected that AI-generated deepfakes were used in a video conference to deceive the employee into making this substantial transfer.[5]

2. Also, in 2024, scammers combined deepfake videos with AI voice clone software to impersonate the CEO of a multinational holding company during a Microsoft Teams meeting. Their goal was to manipulate another company executive into providing money and non-public information. Fortunately, this attempt was unsuccessful.[6]

Combatting AI Social Engineering Attacks

In many ways, the new tools used by criminals call for a response from companies that not only utilize traditional social engineering training but also strategies that can assist in rooting out AI-deployed intrusions. Robust employee training and education are essential for identifying potential security risks and recognizing AI-generated deception.

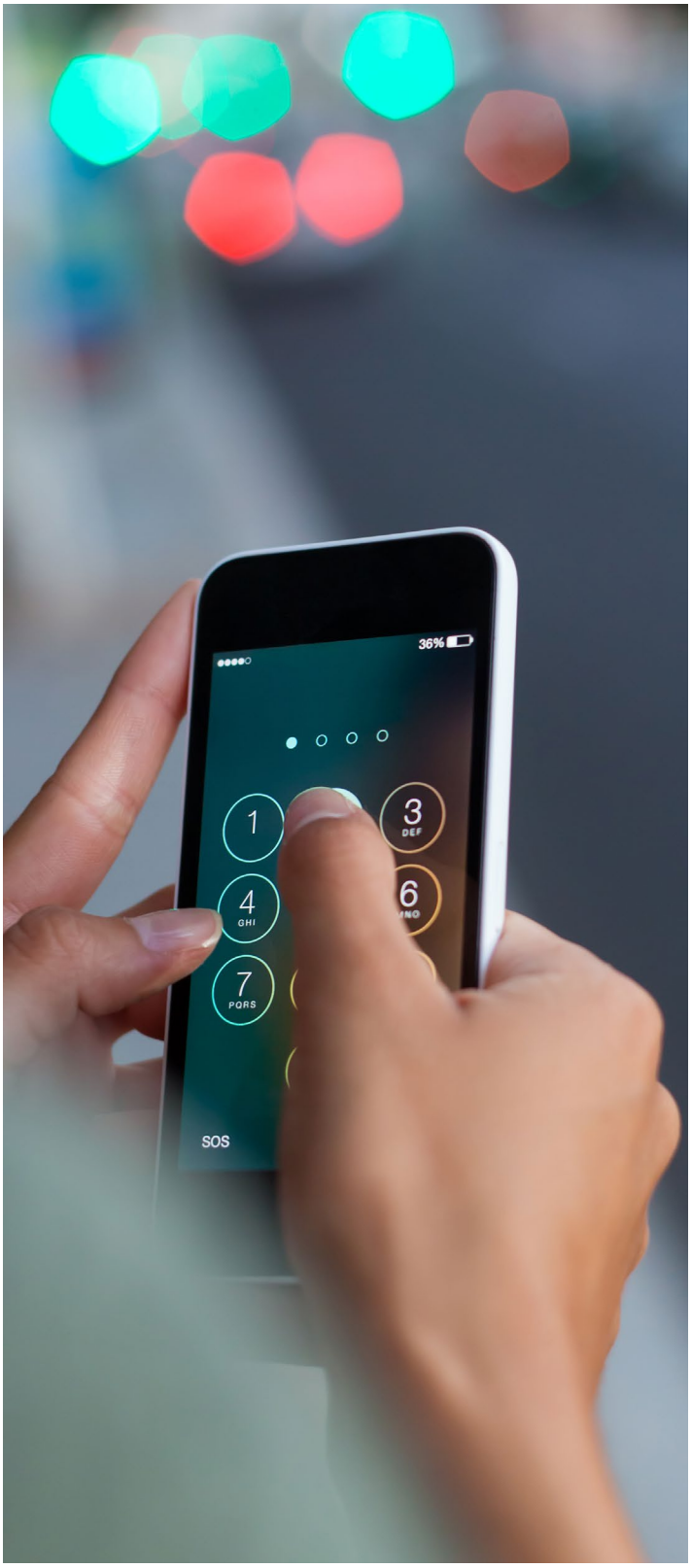
At the same time, companies should implement strict verification protocols for transferring financial and sensitive information. Monitoring financial accounts for irregularities

3. FBI PSA Reporting
4. Deloitte Figure
5. British Engineering Company Article
6. Multinational Holding Company Article

and implementing updated IT controls are essential components of a company's risk management strategy. Technical safeguards like multi-factor authentication and advanced email filtering systems provide additional protective layers, and companies should develop comprehensive incident response plans specifically addressing social engineering scenarios.

Investing in specialized social engineering insurance coverage is increasingly crucial, as traditional Cyber policies may not adequately cover losses from these human-targeted attacks. Commercial Crime policies can incorporate designated sublimits specifically tailored to address social engineering exposures, providing a discrete coverage allocation engineered to mitigate these sophisticated threat vectors. With the continued technological advancement of these types of attacks, carriers have increased the social engineering sublimit quantity over the last few years. This sublimit is a key component of Commercial Crime policies that companies and insurance brokers alike should be paying close attention to in today's environment.

Insurance carriers in the crime space are explicitly looking to see how companies have addressed these modern technological issues and will examine the controls and procedures in place when underwriting this risk. Robots are no longer clunky and obvious, and neither are many cybercriminals. Companies must look to the future as well to safeguard themselves.



Additional Sources:

Industry Letter - October 16, 2024: Cybersecurity Risks Arising from Artificial Intelligence and Strategies to Combat Related Risks | Department of Financial Services

How Brown & Brown Can Help

Connect with our Brown & Brown team to learn about our knowledge in your industry, how we build our risk mitigation strategies and how we can aid your business in building a cost-saving program.

Brown & Brown

Find Your Solution at BBrown.com