CYBER
INSIGHTS

LloydSadd

NAVACORD®

AI-Driven Attacks and Deepfake Scams: A Rising Threat for All Organizations

Artificial intelligence (AI) is rapidly transforming the cyber risk landscape for businesses of all sizes.

In 2025, both AI-driven cyberattacks and deepfake scams have surged, targeting organizations across industries with a level of sophistication and scale never seen before. As digital operations and remote work expand, the attack surface for these threats continues to grow.

WHAT ARE AI-DRIVEN ATTACKS?

AI-driven attacks leverage machine learning and automation to:

- **Automate reconnaissance and vulnerability scanning:** AI tools quickly identify weak points in company systems and processes.
- **Personalize phishing and social engineering:** Attackers use scraped data to craft highly convincing, targeted messages.
- **Evade traditional security:** AI adapts attack methods in real time, bypassing standard detection tools
- **Accelerate attack speed:** Breakout times for cyber incidents are now often under an hour, giving defenders little time to react.

KEY STATISTICS:

According to Bobsguide

- **87%** of organizations experienced AI-driven cyberattacks in the past year
- **91%** of cybersecurity professionals expect these threats to rise significantly over the next three years

THE DEEPFAKE SCAM EPIDEMIC

Deepfakes are AI-generated audio or video content that convincingly mimics real people. In 2025, deepfakes are being used in:

- **Executive impersonation:** Fraudsters create fake video or voice calls from CEOs or CFOs, instructing employees to transfer funds or share sensitive data.
- **Phishing with video/audio:** Pre-recorded deepfake messages are sent via email or chat to add credibility to fraudulent requests.
- **Live video scams:** Attackers join video calls posing as company leaders, exploiting trust and urgency.

RECENT TRENDS

According to the World Economic Forum, deepfake fraud cases surged by an astonishing **1,740%** in North America between 2022 and 2023, with financial losses exceeding **$200 million** in the first quarter of 2025 alone. This dramatic increase reflects how accessible deepfake technology has become, enabling fraudsters to create convincing voice and video impersonations with minimal effort. The WEF highlights that these attacks have evolved from broad misinformation campaigns to highly targeted, precision strikes on corporate operations, often involving executive impersonation and payment fraud, posing a significant and growing threat to organizations worldwide.

WHY ARE THESE THREATS SO EFFECTIVE?

- **Low barrier to entry:** Free, easy-to-use AI tools allow anyone to create convincing deepfakes in minutes
- **Multichannel attacks:** Scams now exploit email, SMS, social media, and collaboration platforms - sometimes simultaneously
- **Difficult to detect:** Deepfakes can fool even cautious employees, and traditional cyber insurance often excludes deepfake-related incidents
- **Exploiting trust:** These attacks target the human element, leveraging urgency and authority to bypass normal verification.

WHAT CAN BUSINESSES DO?

- **Employee Training:** Regularly educate staff on the latest deepfake and AI-driven scam tactics. Use simulation tools to practice recognition and response
- **Verification Protocols:** Require multi-factor authentication and out-of-band verification for sensitive requests, especially those involving financial transactions.
- **Limit Public Data:** Reduce the amount of audio, video, and personal information available online about key personnel
- **Invest in Detection:** Deploy AI-based tools that can help identify manipulated media and anomalous behavior in real time
- **Review Insurance Coverage:** Work with your broker to understand policy exclusions and seek endorsements that address emerging cyber risks, including deepfakes

KEY TAKEAWAYS

1. AI-driven attacks and deepfake scams are not just a future threat -they are a present and growing risk for organizations of all sizes.
2. Traditional defenses and insurance policies may not be sufficient.
3. A layered approach - combining technology, training, and policy review - is essential to mitigate these evolving risks.

Staying informed and proactive will help your organization remain resilient in the face of these rapidly advancing cyber threats.

If you have questions specific to your business, or would like additional information, please reach out to your Lloyd Sadd Advisor.

LET US HELP YOU MANAGE YOUR RISK

Edmonton: 1.800.665.5243
Calgary: 1.866.845.8330
Kelowna: 1.800.665.5243

lloydsadd.com
info@lloydsadd.com