PUBLICATION

Cybersecurity Awareness Month 2025: Businesses Should Prepare for Deepfakes

Authors: Justin S. Daniels
October 08, 2025

Employees train on the rule "think before you click" when it comes to combating phishing emails. As cyber threats evolve, we need a new one entitled: Don't believe everything you see or hear. Deepfakes – AI-generated fake audio and video that look and sound increasingly real – are rewriting the playbook on fraud, sabotage, and reputation management. What started as a novelty has transformed into a serious risk for chief legal officers – one that is capable of disrupting a stock price, an M&A deal, or tricking an employee into wiring millions of dollars. This alert provides businesses with practical steps to develop a deepfake response plan.

October is recognized as Cybersecurity Awareness Month, a time when organizations across the country focus on strengthening defenses and educating employees about digital threats. This annual observance provides an ideal opportunity for companies to revisit and reinforce their strategies for handling emerging risks like deepfakes, ensuring that everyone from executives to frontline staff is prepared to identify and respond to these sophisticated attacks. By aligning deepfake preparedness efforts with the broader cybersecurity initiatives promoted during this month, businesses can foster a culture of vigilance and resilience against evolving threats.

What Are Deepfakes, Really?

A deepfake is an AI-generated video, audio, or image that mimics a real person so convincingly that it can pass casual inspection. You've probably seen the entertaining versions: Tom Cruise doing magic tricks on TikTok or Morgan Freeman narrating things he never said. In 2024, it had far more serious consequences impacting businesses: an employee in Hong Kong approved a $25 million transfer after a video call with what looked and sounded like his leadership team. The only problem was that the "executives" approving the transfer were fake.

The Nightmare Scenario for Business

Consider the following scenario: a deepfake video of your CEO surfaces online. In it, she announces the company's biggest product is unsafe. In a few hours, it has gone viral; your reputation is under attack, and customers and reporters are blowing up your inbox for comment. That might be the moment you realize you do not have a deepfake response plan. A good plan helps you retain evidence of the fake and has established communications protocols. However, the response time required is minutes and hours, not days.

The key questions become:

- Who in your company verifies authenticity when a deepfake surfaces?
- What's your playbook for responding publicly?
- Do you even have one, or are you drafting press releases at 2 a.m. while company reputation is under siege?

Just as organizations have breach notification protocols, they now need a documented **deepfake response plan**. Absent a coordinated plan, the response risks being fragmented, slow, and more damaging than the attack itself.

Practical Steps for Companies

Addressing deepfakes requires the same rigor as cybersecurity and crisis management. Companies should:

1. **Test a Response Plan**: Include deepfake scenarios in tabletop exercises. Ensure legal, PR, IT, and security teams know their roles.
2. **Strengthen Verification Controls**: Do not rely on a single method of authentication. Build redundancy into processes involving financial transactions or sensitive communications.
3. **Evaluate Detection Tools**: AI-based detection technology is improving, but still imperfect. Pair tools with strong internal processes.
4. **Educate Executives and Employees**: Training must reflect that video and voice can no longer be assumed authentic. Awareness is essential for first-line defense.
5. **Prepare Communications in Advance**: Draft templates for public statements and regulator communications. Rapid response reduces uncertainty and speculation.
6. **Limit Available Content**: Encourage executives to limit the amount of raw audio and video material posted online, reducing opportunities for misuse.

Deepfakes signal a shift in how organizations must manage trust. The phrase "seeing is believing" is no longer a safe assumption. Whether the goal is fraud, reputational harm, or market manipulation, these attacks can create material consequences in minutes.

The companies best positioned to withstand these threats will not be those with the most advanced detection tools, but those that have already rehearsed a response, implemented redundant verification methods, and educated their people. Deepfakes are not just another cybersecurity risk. They strike at the core of corporate credibility. Preparing now is far less costly than trying to rebuild trust after a deepfake.

For more information on how to prepare a plan to mitigate your risk, contact Justin Daniels or any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team.

October is National Cybersecurity Awareness Month

Observed annually in October, Cybersecurity Awareness Month is a collaborative effort between the public and private sectors to raise awareness about cybersecurity. It was launched in 2004 by the U.S. Department of Homeland Security (DHS) and the National Cyber Security Alliance (NCSA).

Throughout Cybersecurity Awareness Month, we will provide proactive tips and information in order to mitigate your cyber risks.