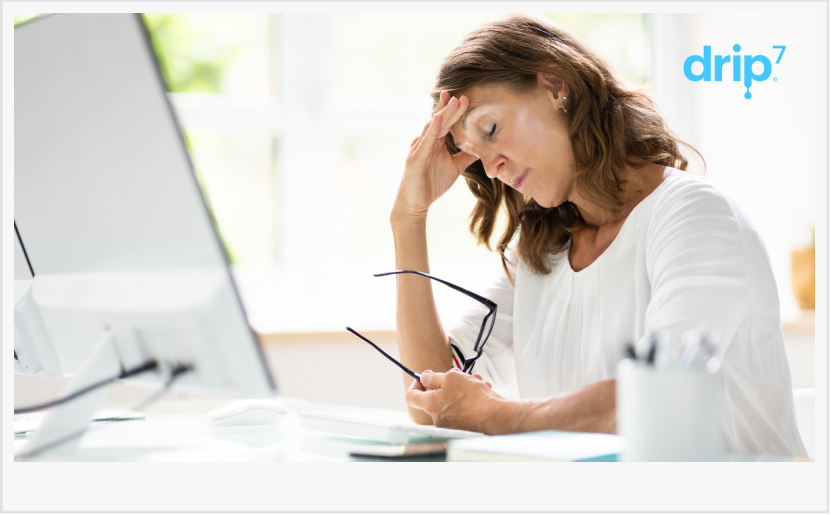
Top Cybersecurity Mistakes Employees Make Are Rapidly Changing with AI, According to Drip7

SPOKANE, WA, UNITED STATES, April 7, 2026 /EINPresswire.com/ -- The most common cybersecurity mistakes employees make every day are rapidly evolving with the rise of artificial intelligence (AI)—rendering traditional, once-a-year security awareness training increasingly ineffective. Drip7, a leader in microlearning-based cybersecurity education, is helping organizations address these emerging risks by focusing on the human behaviors most targeted by today's AI-driven attacks.



While human error has long been the leading cause of cybersecurity incidents, new research shows the nature of that risk is shifting. Industry data indicates that 60–74% of breaches involve human factors. (Brightside AI) With the rapid adoption of AI, these risks are now more scalable, more convincing, and more difficult to detect than ever before.

"Employees aren't making more mistakes—they're facing more sophisticated deception," said Heather Stratford, CEO of Drip7. "AI has fundamentally changed what a cybersecurity mistake looks like, and organizations must adapt their training accordingly."
As artificial intelligence becomes embedded in everyday workflows, human-related risks are being amplified. As noted by renowned cybersecurity expert Bruce Schneier, AI does not eliminate human error—instead, it accelerates and amplifies both the impact and speed at which those errors are exploited.
This reality underscores a critical challenge for IT and security leaders: routine user mistakes are no longer isolated incidents—they are entry points for increasingly automated and intelligent attacks.

How AI Is Changing Everyday Cybersecurity Mistakes
Drip7 has identified a new employee-driven risks shaped by AI-powered threats:

1. Highly Personalized Phishing at Scale
AI-generated phishing emails now replicate tone, context, and writing style with remarkable accuracy, making them significantly harder to detect. In some campaigns, over 82% of phishing emails are now AI-generated, increasing both their volume and success rate. (Zensec)
At the same time, a growing confidence gap persists—employees believe they can identify phishing attempts, but real-world testing continues to show otherwise. (TechRadar)

2. Trusting AI-Generated "Authentic" Communications
AI has effectively eliminated traditional red flags such as poor grammar or formatting errors. As a result, malicious messages are now more believable and harder to distinguish from legitimate communications.
Research indicates that only a minority of users can reliably identify AI-generated phishing attempts, creating a significant detection gap. (New York Post)

3. The Rise of Shadow AI and Unsecured Tools
Employees are increasingly adopting generative AI tools for productivity—often without IT visibility or governance. According to IBM, rapid AI adoption without proper oversight can increase both breach likelihood and overall breach costs, creating new and unmonitored data exposure risks.

4. Faster, More Convincing Social Engineering Attacks
AI enables attackers to scale social engineering attacks across email, voice, and even deepfake impersonation—creating urgency and pressure that leads to rushed decision-making.
Cybercriminals are already leveraging AI to impersonate executives and trusted contacts, tricking employees into transferring funds or sharing sensitive credentials. (The Wall Street Journal)

5. A Persistent Gap Between Awareness and Behavior
Despite increasing awareness, employee behavior has not kept pace with evolving threats. According to the Verizon 2025 Data Breach Investigations Report, the human element is involved in over 70% of breaches—highlighting how employee actions remain a primary driver of security incidents even as threats become more advanced. (Verizon)

The Expanding Impact of Human Risk in an AI Era
Human error continues to be a dominant factor in cybersecurity incidents, with some estimates attributing up to 95% of breaches to human-related factors such as poor cyber hygiene and social engineering. (Huntress)
Phishing remains one of the most common and effective attack vectors, and its sophistication continues to increase alongside AI advancements. (TechMagic)
"The challenge isn't just awareness anymore—it's adaptation," Stratford added. "AI is outpacing traditional training models, and organizations must rethink how they prepare employees to respond in real time."

From Awareness to Behavior: A New Approach to Security Training

Drip7 emphasizes that traditional compliance-based training is no longer sufficient in today's threat environment. Instead, organizations must adopt continuous, behavior-driven learning models that reflect how modern attacks actually occur.
Research supports this shift, showing that static or annual training programs fail to keep pace with evolving threats and do not effectively reduce risky behavior over time. (UpGuard)

Sources:
(Brightside AI) https://www.brside.com/blog/security-awareness-training-statistics-2025-100-studies
(Zensec) https://zensec.co.uk/blog/2025-phishing-statistics-the-alarming-rise-in-attacks/
(TechRadar) https://www.techradar.com/pro/security/us-workers-think-theyre-pretty-good-at-spotting-phishing-emails-but-the-reality-is-quite-different
(New York Post) https://nypost.com/2025/10/03/tech/most-adults-couldnt-differentiate-between-authentic-ai-phishing-emails/
(IBM) https://www.ibm.com/reports/data-breach
(The Wall Street Journal) https://www.wsj.com/articles/ai-drives-rise-in-ceo-impersonator-scams-2bd675c4
(Verizon) https://www.verizon.com/business/resources/reports/
(Huntress) https://www.huntress.com/blog/data-breach-statistics
(TechMagic) https://www.techmagic.co/blog/blog-phishing-attack-statistics
(UpGuard) https://www.upguard.com/blog/human-factors-in-cybersecurity

Drip7 Press Team
Drip7 Inc.
+1 509-703-5400
email us here
Visit us on social media:
LinkedIn
