# Journalists, Media Execs & On-Air Talent Are in AI Phishing Scammers' Crosshairs

DETROIT, MI, UNITED STATES, July 25, 2025 /EINPresswire.com/ -- In the wake of a breaking Axios report on AI-driven phishing scams impersonating journalists to deceive executives and PR professionals, cybersecurity company Hush is issuing a sharper warning: journalists, media executives, and on-air talent are now the targets themselves.

Attackers are using AI to impersonate trusted voices, pitching "exclusive interviews" from outlets like The New York Times or CNN, and weaponizing the public digital footprints of media professionals. "Bad actors rely on personal details—publication history, contact info, colleagues—to craft believable bait," said Mykolas Rambus, CEO of Hush. Axios reports phishing attempts have jumped 17% since September, driven by AI's ability to generate tailored, realistic messages[1].

The threat is not just hypothetical. According to the International Women's Media Foundation, 30.7% of local U.S. journalists report facing digital violence, including online harassment. 37.7% have been threatened with or experienced physical violence while reporting. And 26.9% have faced legal threats as part of their job. These findings, drawn from hundreds of reporters across key swing states, point to an escalating climate of danger heading into the 2024 election season.

Hush data further shows that journalists carry a uniquely high-risk profile: the average media professional has 58 exposed vulnerabilities across data brokers, social platforms, public records, and family connections. These breadcrumbs provide scammers with everything they need to mount convincing, targeted attacks.

"Even as public trust in journalism wavers, impersonation scams now threaten to erode newsroom safety and credibility from the inside out," said Rambus. "If your name, colleagues, and career aren't protected digitally, neither is your outlet."

The risk is growing worldwide. The U.S. Press Freedom Tracker reported over 25 assaults on journalists in 2023 alone, with 80% carried out by private individuals, not police. At least 12 U.S. journalists were arrested or charged for basic reporting tasks. And the European Centre for Press and Media Freedom (ECPMF) found that online attacks made up nearly 25% of all threats to women journalists in 2023—including at least 20 rape or death threats, 60% of which occurred online.

In response, Hush's AI-powered privacy platform (www.gethush.ai) actively removes exposed data from brokers, social media, and the deep web—offering real-time protection trusted by media houses, PR firms, and communications consultants alike.

Hush recommends media organizations take the following steps:

- Conduct digital exposure audits for on-air talent, editors, and PR leads
- Deploy continuous privacy monitoring to catch new exposures as they emerge
- Extend protection to immediate family, a frequent backdoor for scammers

"As AI phishing evolves, only personal-level defense keeps trust intact," Rambus added. "Reputation is a journalist's most valuable asset, don't let AI weaponize it."

Learn more at www.gethush.ai.

[1] Axios. (2025, July 17). PR scams impersonate journalists using AI. Retrieved from https://www.axios.com/2025/07/17/pr-phishing-scams-fake-journalists-ai

Hush Team
Hush
+1 866-806-0932
email us here
Visit us on social media:
LinkedIn
Instagram
YouTube

---