



Small Business Bulletin

June 2026

How Small Businesses Can Protect Their HR Teams From AI-driven Scams

Artificial intelligence (AI) is rapidly changing how small businesses recruit, communicate with and manage their workforce. Whether it's AI-assisted resume screenings or automated scheduling and onboarding tools, this technology offers efficiency gains that are especially valuable for lean teams. However, the rise of AI has also introduced a growing risk: increasingly realistic and scalable scams targeting HR teams. For small businesses, where a single individual may manage hiring, payroll and employee data, one successful scam can pose considerable financial and reputational consequences.

AI has enabled scammers to move far beyond the poorly written phishing emails of the past. Today's attacks may include highly polished messages that reference real employees, convincingly written job applications, audio clips mimicking a business owner's voice or even live video interviews with AI-generated faces (also known as deepfakes). These tactics are particularly effective against small businesses because fast decisions, informal communication styles and limited oversight can create openings for deception. Understanding how these scams work and putting simple safeguards in place can significantly reduce related risks.

Consider the following six tips to help avoid AI scams:

Understand how AI has changed scams. AI allows scammers to create realistic emails, resumes and even voices that closely mimic real people within a business. Small businesses should expect scams to look professional and personalized, making consistent processes more important than gut instinct.

Strengthen hiring measures. Fake applicants may use AI-generated resumes, documents or deepfakes to appear legitimate. Small businesses should verify identities through secure platforms and ask experience-based interview questions that require detailed, real-world answers.

Verify leadership requests. Scammers often impersonate business owners or executives to push urgent payroll or data changes. Any unusual request should be confirmed through a second channel, such as a phone call or in-person conversation, before taking action.

Build simple, consistent HR processes. Clear approval steps help reduce risks, especially when only one or two people manage HR tasks. Requiring dual approvals for payroll changes or access updates makes scams much harder to execute successfully.

Train HR staff to spot AI red flags. Regular, short trainings can help HR staff recognize evolving AI scam tactics, such as overly polished communication or urgent pressure. Employees should be encouraged to report concerns early and reassured that verifying requests is a best practice, not a delay.