



## Security Tip: Don't Let AI Fool You

Artificial Intelligence (AI) is transforming the way we work, but it's also giving cybercriminals new tools to make scams more convincing than ever. Today's phishing emails, text messages, phone calls, and even videos can be powered by AI, making them harder to spot and easier to believe.

### How Cybercriminals Use AI

Cybercriminals use AI to create highly personalized scams that can appear legitimate and trustworthy. AI can help them:

- Create realistic phishing emails tailored to specific individuals
- Mimic the writing style of managers, coworkers, or executives
- Generate convincing fake voice recordings and videos (known as deepfakes)
- Produce professional-looking messages at a large scale and in multiple languages

These tactics are designed to create trust, urgency, and emotion, increasing the likelihood that someone will click a link, share sensitive information, or approve a fraudulent request.

### Where Do They Get Their Information?

Many AI-powered attacks rely on information that is publicly available online. Social media posts, company websites, press releases, and job postings can all provide valuable details to cybercriminals.

Something as simple as:

- Sharing your job title or responsibilities
- Mentioning software your organization uses
- Posting photos that reveal employee badges or workstations
- Sharing organizational updates online

can help attackers create more convincing scams.

### How to Protect Yourself

✅ **Think before you click.** Be cautious of unexpected emails, texts, or messages, especially those requesting sensitive information.

✅ **Verify requests independently.** If someone asks for money, passwords, account information, or urgent action, confirm the request using a trusted phone number or communication channel.

✅ **Limit public information sharing.** Be mindful of what you post online about your role, workplace, or internal processes.

✅ **Watch for urgency.** Messages that create fear, pressure, or a sense of emergency are common social engineering tactics.

✅ **Trust your instincts.** If something feels unusual or too good to be true, take a moment to investigate before responding.

## **Remember**

AI may make scams more sophisticated, but cybersecurity still starts with people. Taking a few extra seconds to verify a request and think critically can prevent a costly mistake and help keep both your information and our organization safe.

**When in doubt, slow down, verify, and report suspicious activity.** 🔵