Powered By LexisNexis
Tribune's Newsday (6+ months) (United States), Section: Local
Monday 05 January 2026
794 words
97182 circulation

BOSS' URGENT MESSAGE COULD BE SCAM Look for unusual requests, such as buying gift cards

By Celia Young/celia.young@newsday.com
By Celia Young

celia.young@newsday.com

That urgent email from your boss might not be from your boss at all.

A fake boss scam is a form of fraud in which scammers pose as a company executive to trick an employee into sending money or sensitive information. It's part of a broader category of schemes known as business email compromise scams, which the FBI has tracked for more than a decade.

With the advent of artificial intelligence tools, scams like these are becoming easier to pull off, said Nick Nikiforakis, an associate professor of computer science at Stony Brook University who studies web security. AI allows scammers to generate convincing messages and even communicate with potential victims.

"It's definitely more scalable," Nikiforakis said. "You could be scamming thousands of people at the same time."

Here's how these scams work - and how to protect yourself.What is a fake boss scam?A fake boss scam is a type of scam where a fraudster impersonates your supervisor - or another higher-up - to ask for money. The money is often requested in the form of gift cards, wire transfers or other payment methods, according to the FBI. These scams can show up in your email inbox or in a text message, Nikiforakis said.

Scammers can use publicly available information to identify both their targets and the executives they're impersonating, said Lorrie Faith Cranor, a professor and director of the CyLab Security and Privacy Institute at Carnegie Mellon University. That might include LinkedIn profiles, company websites or organizational charts. Once a target is identified, the scammer usually sends an urgent message designed to look like it came from the target's boss. Why do these scams work? Fake boss scams create a sense of urgency and exploit power dynamics in the workplace, experts said. By posing as an authority figure, scammers pressure employees to respond quickly and overlook red flags.

"People under social pressure, or under different types of pressure, tend to make fast decisions - and fast decisions don't always lead to better decisions," said Sayeedul Islam, an associate professor of psychology at Farmingdale State College who studies workplace behavior.Who is most at risk?"All up and down the chain, people can be susceptible," Cranor said. "Even the CEO."

But certain groups may face higher risk. Employees at small businesses are especially vulnerable, said Claire Rosenzweig, president and CEO of the Better Business Bureau serving the metro New York, Long Island and mid-Hudson region. Smaller companies often lack the cybersecurity support of larger firms, and it can be more common for a boss to contact an employee directly via email or text.

New hires, contractors and gig workers may also be more likely to comply, Islam said. But older, higher-ranking

Powered By LexisNexis
Tribune's Newsday (6+ months) (United States), Section: Local
Monday 05 January 2026
794 words
97182 circulation

employees can pose a bigger risk to the business if they're targeted - since they may have the authority to move company money.How can you that it's ascam? Rosenzweig said to look for three key red flags:

n

Urgency: Scammers use pressure to push you to act fast. "The best way to protect yourself from a scam is to reject the frame of urgency that the attacker is setting," Nikiforakis said.

Unusual communication: If your "boss" is emailing from a new address or texting from an unfamiliar number, or if the tone doesn't match how they normally speak, stop and verify. Reach back out through a separate method that you know is real, Rosenzweig said.

Outside normal processes: Be particularly suspicious of any request that involves asking you to send money in a way your company hasn't done before, and of any asks that involve gift cards. "If your boss has never, ever asked you to buy a gift card, take a step back," Rosenzweig said.

What should workers do ifthey get a message?

Don't reply.

Responding to a scammer, even if you don't send them money, can get you put on a database that can be sold to other criminals, Nikiforakis said.

Instead, confirm the request through a trusted method - such as a saved office number or, ideally, an in-person conversation. If it's a scam, report it right away.

How to report a scam

Start with your workplace: Notify your employer and your IT department. Quick internal reporting can alert colleagues to similar threats.

File a consumer complaint: New Yorkers can report scams to the state attorney general's office online or by calling 800-771-7755. You can also submit the incident to the Better Business Bureau's scam tracker to help warn others in your area, Rosenzweig said.

Alert federal authorities: If money was lost, file a complaint with the FBI's Internet Crime Complaint Center. You can also report scams to the Federal Trade Commission at reportfraud.ftc.gov.

--- ENDS ---