BOSS IMPERSONATION SCAM

Fraud.org | Published by Fraud.org staff

With record numbers of people working from home due to COVID-19, scammers are capitalizing on the disconnect between employers and their employees. Last month, New York Attorney General Letitia James sounded the alarm about the "Boss Scam," in which fraudsters who are impersonating a real executive target employees and trick them into purchasing gift cards under an array of scenarios. Posing as the boss, the scammers contact workers by phone or email, and — feigning a work emergency — put pressure on the employees to act quickly.

The scam works because fraudsters assume their targets are more likely to engage with phishing emails sent from a familiar person in a position of authority. Posing as the boss puts pressure on the worker, prompting them to act with a greater sense of urgency and — against normal better judgment — skip due diligence. The Federal Bureau of Investigation estimates that $2.3 billion has been lost to these email scams over the past three years. Scammers use public information from companies' websites and LinkedIn profiles to personalize their communications and add legitimacy.

One consumer in New York reported to Fraud.org that a scammer contacted her via phone claiming to have her boss on the other line. They then instructed her to purchase eight Google Play gift cards worth $100. The consumer purchased four in total before being warned it was likely a scam by a helpful cashier. A consumer in Texas was also contacted by someone telling him his boss was on the other line. The scammer impressed upon him that, if he did not pay quickly, his boss would be subject to expensive fees. The scammers instructed him to take the money from his cash register and put it into his personal bank account. The consumer then sent the scammer the money from his cash register and the entirety of his bank account, totaling $1,360, via MoneyGram. The scammers immediately took the money, and the victim was unable to get it back.

While it's hard to push back at someone you think is your boss, here are some tips for spotting and avoiding this scam:

- **Just because an email says it's from your boss, it may not be.** If you are in doubt about the authenticity of an email request, call your boss on the telephone and verify the request before taking any action.

- **Don't click on links or attachments.** Scammers may use attachments or links that look official (labeled as "invoices," "purchase orders," or some other official-sounding name) in order to install malware or take over a computer for ransomware attacks.

- **Slow down and do your research.** Scammers may use aggressive tactics like urging you to act quickly and threatening you with repercussions to your job. Slow the conversation down. Give yourself time to verify the information they provide and contact your employer on your own.

- **Know that no legitimate business takes payment through gift cards.** Money sent via these hard-to-track methods cannot be easily recovered. If someone calls you asking for payment via gift cards, it is almost certainly a scam.

If you suspect that you or someone you know has become a victim of the "Boss Scam" or any other fraud, report it at once. You can file a complaint at Fraud.org via our online complaint form. We'll share your complaint with our network of law enforcement and consumer protection agency partners who can investigate and help put fraudsters behind bars.