

Date: Click or tap to enter a date.

To: All Employees

From: Company Name.

Subject: Direct Deposit Fraud/Scam Alert

Company Name. wants to make our staff/team aware of a reoccurring scam involving direct deposit fraud. This phishing scam uses social media and other platforms to allow Cybercriminals to create fake email accounts that appear to be from an employee, and request direct deposit information changes to a fraudulent account of the Scammer's choice. The nature of these requests can bypass normal technical controls for malicious communications and other options, such as pay cards (Green Dot, American Express), digital wallets (CashApp, Venmo), and mobile banking (Chime, GO2Bank) allow Scammers to move funds quickly into other accounts, eliminating traceability.

As a means to do everything we can to protect our employees/team from fraud, Company Name. is implementing the following:

- Employees are required to make all direct deposit changes via the online employee self-service portal.
- The Self-Service portal requires stronger passwords that are difficult to crack, as well as using a multi-factor authentication process.
- When a direct deposit change is made via the Self-Service portal, you will receive an email alert and/or text alert that your information has been changed.
- If you are unable to make the change via the Self-Service portal, any change requests MUST be made in-person with Company Payroll Contact Name.. Our Payroll Partner, My HR Professionals, has been instructed not to accept direct deposit change requests that are emailed directly from employees to circumvent this particular type of fraud.

How to Protect Yourself

It is critical that you be proactive when communicating through email, either personally or for employment-related communication.

- If you receive a suspicious email, do not click on any links or open any attachments within the message.
- If you receive a phone call asking for bank account information, do not give out any information.
- If you receive a notification of a change that you did not authorize, contact [List contact's Info] immediately.

If you have any questions, please contact Contact Person. in the payroll office at Phone Number..