DIRECT DEPOSIT FRAUD ALERT!

With the holiday season upon us, be on alert for an increase in payroll scams. Throughout the last few years, we have seen an increase in direct deposit fraud. Cyber-criminals impersonate employees by spoofing an employee's email address, using an employee's compromised email account, or by using a similar new/made-up email address that does not actually belong to the employee.

A FEW SUGGESTIONS TO PROTECT YOUR COMPANY & EMPLOYEES:

1. Require employees to fill out a direct deposit setup/change form
2. If you receive a direct deposit change request by email, confirm the change directly with the employee. Do not reply to the email as a means of confirmation. ***Speak directly with the employee in person or call them to confirm their request.*** Do not call a phone number listed in an email - instead use a phone number you have on file.
3. If your employee has access to make direct deposit changes through WebHCM, be sure you can either approve, or at least be notified, so you can verify the change directly with the employee
4. Instruct employees to forward suspicious emails/personal info requests to your IT or HR department.

innovative
BUSINESS SOLUTIONS