Payroll Impersonation Fraud

What is it?

Fraudsters target individual employees by directing the employees to update or confirm their payroll information via a fake payroll platform that spoofs their employer's actual payroll platform. In some cases, the fraudster may claim the employee must do one of these: view a confidential email from human resources or the payroll department, view changes to the employee's account, or confirm that the account should not be deleted. In any case, when the employee logs in from a link or attachment in the email, the fraudsters then use the stolen employee credentials to change payment information in the real payroll platform.

How It's Done

Fraudster targets an employee by sending a phishing email that impersonates the employee's human resources or payroll department, as well as the company's payroll platform. The email directs the employee to log in to confirm or update payroll information, including bank account information.

Employee clicks the link or opens the attachment within the email and confirms or updates the payroll information.

The fraudster then uses the stolen login credentials to change payment information to an account controlled by the fraudster or a money mule.

Avoid Being a Victim

- ✓ Employers should alert employees to watch for phishing attacks and suspicious malware links.
- ✓ Employees should be directed to check the actual sender email address, rather than just looking at the subject line, to verify that the email came from their employer or payroll service provider.
- ✓ Employees should not reply to any suspicious email; instead have them forward the email to a company security contact.
- ✓ Employees should not enter their login credentials when clicking on a link or opening an attachment in an email.
- ✓ Employer self-service platforms should authenticate requests to change payment information using previously known contact information. For example, requiring users to enter a second password that is emailed to an existing email address, or to use a hard token code.
- ✓ Employer self-service platforms also should reauthenticate users accessing the system from unrecognized devices, using previously known contact information.
- ✓ Set up alerts on self-service platforms for administrators so that unusual activity may be caught before money is lost. Alerts may include when banking information is changed, and multiple changes that use the same new routing number or identical account numbers.
- ✓ Employers should consider validating employees' new Direct Deposit information by sending ACH prenotification transactions.

jbt Bank on a Smile.

jbt.bank