PAYDATA™
WORKFORCE SOLUTIONS

Payroll (Direct Deposit) Diversion Fraud is on the Rise

The Internet Crime Complaint Center (IC3), a division of the FBI released a public service announcement I-091818-PSA regarding the practice of payroll diversion by cyber-criminals. This announcement identified employees whose online self-service portal credentials were compromised, typically through a phishing attempt, and the criminal would change the direct deposit bank account of the employee to a loadable debit card in their possession. Unfortunately, once funds are sent to a debit card, the criminal can withdraw them without a trace.

Another case of payroll diversion that we have seen. While you may be thinking that you are safe because either your employees do not have access to a self service portal, or they do, but do not have the ability to change their direct deposit account. Let me inform you that you are not without risk.

All a criminal needs to do is identify where the individual works. This can be done in a number of ways, such as simply looking up the person on social media, Facebook, LinkedIn or possibly through a compromised email account. In any case, once the criminal knows where the person works, they will send an email to the payroll department asking to change their direct deposit account. (Please note: PayData does not respond to employee email requests)

The email may originate from a legitimate email account, sometimes the criminal has access to the employee's actual account, but it could come from a similar account name. Let's say the employees name is Louis Smith and the employee has an email account of lousmith@yahoo.com. The criminal could make their own yahoo account with an email of lousmith@yahoo.com (you probably did not catch it, but I substituted an uppercase i in place of the lower case L), lousmth@yahoo.com (leaving out a letter that could be overlooked, lou.smith@yahoo.com (added the dot), and so on. A return email address could even be displayed as lousmith@yahoo.com, but the email is actually being sent from xyz@scam.ru.

How to protect yourself from both of these scams?

First off, if you receive a direct deposit account change other than handed to you by the employee, take the extra minute to call the employee (not email because that could be what is compromised) to confirm the account change. If your employees do have the ability to make direct deposit changes via their portal, then be sure you either have the ability to approve such change or at least be notified of such changes.

If you should fall victim to a loss, then be sure you file a complaint with the IC3. You will also want to reach out to your bank as there is a slim chance that all of the funds have not been withdrawn from the debit card.

While on the topic of cyber-criminals, this is also the time of the year of W-2 phishing. Never send an unprotected W-2 via email, whether it is the "employee" requesting it or the "CEO" of the company via email. As stated above, that email request is quite possibly not from the person who you think it is. Always get a verbal confirmation of any requests, and if you have to send the document via an electronic means, be sure it is secured with a password that was verbally given to the recipient. Do not email the password because that just defeats the purpose.

At PayData we strongly believe in protecting our clients confidential data, and our systems are tested and updated on a regular basis. We also undergo an annual SSAE 16 audit.