HINSHAW

Alerts

Defeating Direct Deposit Phishing Attacks

April 16, 2019
Cyber Alert

Download of PDF of the alert

Risk Management Question

What steps can lawyers and law firms take to guard against phishing attacks that try to re-route direct deposit paychecks to a scammer's bank account?

The Issue

Lawyers are not the only marks of scammers; administrative and support staff have become targets, too. This new phishing scam usually takes the form of sending a legitimate looking email to an unsuspecting human resource employee, purporting to be from another company employee or supervisor, with instructions to change bank account and routing information for direct deposit paychecks. The email is written convincingly and professionally, and warns that the sender is going into a meeting or is otherwise unavailable, thus dodging verbal confirmation of the new routing information. After the human resource employee implements the instructions, the employee's paycheck is sent to the wrong bank account, causing financial harm to both the employee and the firm.

Risk Management Solution

Take the following steps to help defeat direct deposit phishing attacks:

- Compare the sender's email address to the sender's known company email address.
- Implement policies requiring all direct deposit instructions to be confirmed verbally and/or in-person with the affected employee.
- To avoid rushed changes, and if permitted by law, set a deadline of at least one week prior to the next paycheck for employees to ask for direct deposit changes.
- Don't act on instructions sent from an employee's personal email account.
- Discuss with your IT Department additional options that may be implemented to spot and prevent phishing attacks.

The best defense is a good offense. Educate your employees on a regular basis about how to spot and prevent new phishing techniques and remind them to be careful out there.

Attorneys

Steven M. Puiszis

Service Areas

Law Firm Cyber Alerts

Lawyers for the Profession®