

Does Your Business Have Proper Controls Over Electronic Fund Transfers?



ARTICLE 11.05.15 DEAN DORTON

What controls does your business have in place to manage electronic fund transfers? How easy would it be for your Accounting Department to unknowingly participate in a fraudulent request to complete a wire transfer? Without adequate controls in place, your company could easily become the next victim of a common email phishing scheme. It is easy to think that your employees wouldn't fall for something like this, but it happens more often than you think.

A local company recently lost over \$85,000 because an employee in the Accounting Department received an email that appeared to come from one of the executives. Proper controls were not in place and funds were transferred. By the time anyone realized what had happened and the FBI could be contacted, the funds were gone and could not be recovered.

These types of scams have been around for a long time. However, the thieves are getting more sophisticated and actually put a great deal of effort into the process. It only takes a few vulnerable victims to make their effort pay off. There has been a large upswing in the number of attempts to defraud businesses – yes, even here in Kentucky!

Some attacks use a method called spoofing. Spoofing allows a sender to disguise their address and make it appear as though it came from someone else. For example, I could send an email and make it look like it came from your CEO. With the proper email security and SPAM filtering in place, most of these attempts do not make it through the filters. Properly managed email systems can recognize the spoof and block the message. More recent attempts involve the thieves actually registering a new domain name that is very similar to yours and setting up an email address that comes very close to that of your CEO or management. So close, it is very easy for your employees to not recognize the difference. Generally the email address is only one character off (e.g., jmiller@deannorton.com instead of jmiller@deandorton.com).

The best defense against these attacks is to ensure there are strong controls around your electronic fund transfer processes that require more than an email request to process the transaction. For example, it is a good idea to require written sign-off. Note that an email does not equal written sign-off. If situations arise where you do need to use email, the recipient should always start a new email message to the requester (never reply to the request email). A text message to the requester would also add an additional layer of confirmation. However, completion of a company request form would be best. A strong control would require dual sign-off for transfers, especially those over a certain dollar amount and for new vendors (or new transfers). The key point here is having a two-step process to help minimize any opportunity for fraud.

Don't put your business at risk by not having internal controls. For help evaluating and improving your information security and internal controls, please contact your Dean Dorton advisor or Jason Miller, Director of Business Consulting Services, at 859-425-7626 or jmiller@deandorton.com.

[View Jason Miller's Bio](#)