Spear-Phishing Alert:
HR and payroll departments should be on the lookout.

“Spear-Phishing” is not as fun as it sounds. On a weekly basis you probably receive dozens of phishing emails looking to gain access to you or your employees private information. Unless you truly believe a Nigerian Oil Baron wants to give $20 million sight unseen, you’ve likely already sniffed out these obvious fraud attempts and have simply deleted the emails.

With tax season in full swing the IRS is reminding employers to be on the lookout for malicious attempts to access private employee data. “Spear-Phishing” differs from regular phishing scams because they involve more coordinated and personal efforts to gain access to private financial data. These types of scams are common this time of year because we often grow accustomed to handing out so much private information during tax season that it’s easy to let our guard down.

Up 400% from last year, these types of attacks can appear to be from legitimate sources such as your bank, internet provider, or even the CEO of your company. Upon closer examination you will see that it is not actually your bosses email address or the website of your bank.

“This is a new twist on an old scheme using the cover of the tax season and W-2 filings to try tricking people into sharing personal data. Now the criminals are focusing their schemes on company payroll departments,” said IRS Commissioner John Koskinen. “If your CEO appears to be emailing you for a list of company employees, check it out before you respond…”

What can you do to protect your business?

As a red-flag that a communication is not from a legitimate source, be on the lookout for any of the following:

1. There is an immediate sense of urgency
   a. Ex. Confirm in the next 24 hours or lose access to your account...

2. Having to click on a link or download a document embedded in an email.

3. The communication includes personal information about you and/or your company making it look genuine.
   a. Note: In the era of social media getting this kind of information is often just a click away.

4. Be wary of emails from companies you didn’t opt in to receive emails from.

5. Look for poor spelling/grammar use, or website addresses that don’t quite look right.

Consider doing the following to protect your business:

1. Change passwords regularly.

2. Have multiple passwords.

3. Test employee’s awareness by sending out your own phishing emails to see how they respond.

continued on page 2
4. Update your spam filters so they don't make it to your inbox in the first place.

5. When in doubt, call the company you do business with to verify it's legit.

For more information, see what the IRS has to say [here](#).

### Compliance Spotlight…

**OSHA 300A: No injuries in 2015. Do we have to post it then?**

As a reminder, Federal OSHA requires that employers with more than 10 employees post a copy of OSHA's form 300A in a common area where employees are likely to see it along with other required employee notices. If you haven’t done so already, the form needs to stay up from the beginning of February through the end of April.

A common question that comes up is, “Do I still need to post it if we did not have any recordable serious injuries last year?”

The answer is yes; however, you will not be subject to a monetary penalty if this is your first violation. Why post it then? To make sure that you did not have any recordable injuries, the inspector is allowed verify this by conducting employee interviews, reviewing workers’ comp claims, as well as auditing employee medical records. Likely a headache you will want to avoid.

Wondering if an injury is recordable under the new rules? Check out OSHA’s FAQ page by clicking [here](#).

### About the Author/Disclaimer:

Tom Rider is Manager of Member Services for Western Building Material Association. He is committed to being a valued resource to its members particularly on regulatory compliance issues affecting building material suppliers. Unless stated otherwise, this regulatory newsletter is written by him. He is a lawyer, but respectfully he is not your lawyer (unless you have been in his office and signed a contract). This communication is not intended as legal advice, and no attorney client relationship results merely by reading it. Please consult your own attorney for legal advice. If you are a WBMA member and would like to contact Tom with questions and/or comments: tom@wbma.org

---

### Quote of the Month:

“We should not only use the brains we have, but all that we can borrow.”

---

### Upcoming Events:

#### Educational Opportunities:

- **April 5th**
  - *Intro. To Bldg. Material Sales* (Boise, ID)

- **April 6th - 7th**
  - *Estimating Workshop* (Boise, ID)

- **April 28th**
  - *Safety Mgrs. Workshop* (Olympia, WA)

#### Dates to Remember:

- **April 18th – 20th**
  - *NLBMDA Legislative Conference, Washington D.C.*

- **October 2016**
  - *Part 2 of WBMA’s Leadership Series: Financials for Non-Financial Managers*

- **November 7-9**
  - *WBMA’s 114th Annual Convention, Red Lion Jantzen Beach, Portland OR*

Visit us on the web at: [www.wbma.org](http://www.wbma.org)