# LGIT CYBER RISK ALERT – February 28, 2018

## Phishing for Employee Payroll Information

**LGIT has recently been made aware of this type of attack on a member. This attack unfortunately, resulted in the release of employee W-2 forms. After gathering the data, the cyber criminals in this case, started filing false tax returns based on the stolen employee data.**

This bulletin is to make LGIT members aware that cybercriminals use various spoofing techniques to disguise an email to make it appear as if it is from organizational executive or they compromise the email account itself to contact an employee in the finance/payroll department requesting a list of all employees and their W-2 forms. This Phishing attack is sometimes referred to as a Business Email Compromise (BEC) or Business Email Spoofing (BES). They achieve this by spoofing the "From" field and adding a "Reply-To" address or using a free email service account for the email address and spoofing the sender name. Another technique is to use a Typosquatted domain.

The W-2 scam is just one of several new variations to appear in the past year that focus on the large-scale thefts of sensitive tax information from tax preparers, businesses and payroll companies. Maryland's local governments are not immune. Cyber criminals have evolved their tactics to focus on mass data thefts.

The key to reducing the risk from W-2 phishing scams and BEC is to understand the criminals' techniques and deploy effective mitigation processes. There are various methods to reduce the risk of falling victim to this scam and subsequently disclosing sensitive information or executing a fraudulent wire transfer.

**Some of these methods include:**

• Limit the number of employees within a business who have the authority to approve and/or conduct wire transfers and handle W-2 related requests or tasks

• Use out of band authentication to verify requests for W-2 related information or wire transfer requests that are seemingly coming from executives. This may include calling the executive to obtain verbal verification, establishing a phone Personal Identification Number (PIN) to verify the executive's identity, or sending the executive via text message a one-time code and a phone number to call in order to confirm the wire transfer request

• Verify a change in payment instructions to a vendor or supplier by calling to verbally confirm the request (the phone number should not come from the electronic communication, but should instead be taken from a known contact list for that vendor)

• Maintain a file, preferably in non-electronic form, of vendor contact information for those who are authorized to approve changes in payment instructions

• Delay the transaction until additional verifications can be performed

7225 Parkway Drive, Hanover, MD 21076 · Phone 443.561.1700 · TF 800.673.8231 · FX 443.561.1701 · www.lgit.org

- Employers who receive or fall victim to the W-2 scam should review guidance at Form W-2/SSN Data Theft: Information for Businesses and Payroll Service Providers. For general questions, visit: https://www.irs.gov/identity-theft-fraud-scams/identity-protection

Fortunately, LGIT provides Cyber Coverage with XL Catlin as a Value Added Product meaning at no charge to our members. LGIT will also pay up to $25,000 toward your deductible for claims approved by XL Catlin. Members with less than a 100,000 population have a $25,000 deductible and $50,000 for members with a population of 100,000 or more. Therefore, Members with under a 100,000 population have no deductible ultimately.

The Cyber Policy is with XL Catlin providing both first party and third party liability coverages with a $1,000,000 limit per occurrence for all coverages combined.

Third Party Liability Coverages include Media Liability, Privacy & Security, Privacy Regulatory Defense, Awards and Fines, and Payment Card Industry Fines and Costs.

First Party Coverages include Business Interruption & Extra Expense, Data Recovery, Cyber Extortion and Data Breach Response & Crisis Management Coverage which is the main reason many secure this coverage.

Data Breach Response & Crisis Management Coverages include the costs to notify customers/citizens of a data breach, costs to hire IT forensics experts, public relations consultants, implement credit monitoring and identity restoration services resulting from your obligation to comply with a privacy law.

What to do when a breach, loss or a liability claim occurs. At your earliest, call the XL Catlin Breach Hotline number at 1-855-566-4724 for immediate triage assistance. They have a team of cyber IT and legal experts.

Then email your claim details to proclaimnewnotices@xlcatlin.com.

To apply for this free cyber coverage with only five basic questions, please go to http://lgit.org/747/Cyber-Coverage.

In two to four weeks when your coverage starts, you then will have access to free Cyber Risk Management loss control services at https://cyberriskconnect.com/. Services include a Cyber Claims Roadmap, Response Services, Response Partners, Risk Manager Tools, News Center, Learning Center and Privacy Training.

For any questions, please contact Scott Soderstrom, email scott@lgit.org or 443.561.1700.