Phishing Attacks Target Companies to Give Up Employee W2 Information

February 9, 2017 - It's tax season again and that also means it's time for scam artists to come out of the woodworks. This year phishing attacks that target companies, fooling them into turning over the W2 information on all of their employees are on the rise. This type of attack can be quite effective and very damaging. Whether you run a company of your own, work in the HR department, or just have access to W2 information for your company's employees, here is what you need to know.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

W2 phishing attacks work like this. An email message that appears to come from someone in senior management (CEO, CFO, COO, etc.) is sent to someone in Human Resources. That message requests W2 information for all employees, or for a subset of employees. The message is marked "urgent" and asks the person receiving it to attach the information to their reply.

As soon as the person who receives the message replies - normally with a spreadsheet of the requested information attached - data breach laws are triggered. If your company employees people in multiple states, then the laws of each of those states are triggered.

Fortunately, this type of breach is totally avoidable but it will require some training for employees. Companies need to have policies in place that require voice verification of any requests for the personally identifiable information of employees. This means that when such a request is received, the person receiving it needs to pick up the phone and call the person making the request to make sure it is valid. Better yet, if the person making the request is in the same office, get up and have a face to face conversation.

Additionally, it is a very bad idea for any HR department to send this type of information as an unencrypted file attachment over email. At the very least, the data should be encrypted and the decryption key should be sent in a separate message or provided over the phone. Even if the request turns out to be legitimate, as soon as the data is shipped over the internet in unencrypted form, it is vulnerable.

Companies should also limit access to this type of information by their employees. And anyone who is granted access to W2 information needs to be trained first on the procedures for handling it.

Falling for one of these phishing attacks could be very costly. Companies could be sued by their employees, face some very bad publicity and could possibly have employees leave as a result of the breach. There is also the potential for government investigations and civil fines.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS