Better Business Bureau Phishing Scam Targets Business Owners & Managers

December 4, 2012 - There is a phishing scam making its way around the internet that is targeting business owner and managers. The scam shows up in the form of an e-mail that is supposedly from the Better Business Bureau. The message may say that a consumer has submitted a review or filed a complaint about the recipient's business and contains either a link or an attachment. But the message is a fraud.

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);
})();

ACCESS has seen some of these messages. Those that we've seen with an attachment have a file that is named with a false "case #". The file is compressed and requires a program such as WinZip or WinRAR to open. A closer examination of the compressed file reveals and executable file that is designed to infect the recipients' computer system. It can be assumed that the variation of the message that contains a link would download a similar file to anyone clicking on the link.

All of the messages that we are aware of contain a phrase indicating that the message is time sensitive and requires a response. Many of them contain the BBB logo and other formatting that make the messages look legitimate. Since no business owner wants to have a bad review of their business published online, they have a compelling reason to open the messages.

Most BBB's are aware of the issue and there is a national investigation under way. More than 100 websites have been shut down as a result, according to a BBB press release, but there is virtually no barrier to entry for anyone wanting to participate in this scam. Therefore, it is really up to the individuals receiving these messages to fight back.

Anyone receiving this type of message should do several things. First, if you are concerned that the message is

legitimate and you don't want to immediately delete it, then look up the phone number for the BBB office that supposedly sent the message to you. Do the lookup yourself and don't rely on any information contained in the body of the message.

Second, refrain from clicking on any links or attachments in a message that you believe may be suspect. If you have already clicked on such a link or attachment, then run an antivirus sweep of your computer promptly. The BBB is also warning that you should closely check your credit card accounts and banks statements for unauthorized transactions. NOTE: If you have a business bank account this is especially important because even though consumer bank accounts are protected by law if the crime is discovered within a timely manner, businesses are expected to maintain reasonable security standards to prevent fraud. If your business account is drained as a result of this type of scam, you will likely be on the hook for the total amount of your loss.

Third, the BBB is asking that suspect messages be forwarded to phishing@council.bbb.org.

As a final note, even having antivirus software with up to date virus definitions is no guarantee that you won't become infected. In one of the messages that we examined today, our antivirus software didn't detect anything even though the definitions were only a few hours old.

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