Ransomware and Hacks Circulating in Files Attached to Email - How to Protect Yourself

August 2, 2017 - Using email to circulate viruses, Trojans and ransomware is nothing new. But lately we've seen an uptick in the number and type of documents being used to target victims. So we thought it was a good time to do a refresher story on the topic and provide some information about how you can protect yourself.

A lot of the more recent activity we've seen hasn't been in the form of links in email messages. Of course, we still advise readers not to click on links from unknown sources.

What we have seen are a lot infected file attachments to email messages. Many of these have been in the form of infected MS Word documents. These files typically have built in macros that can be activated as soon as the document is opened.

Fortunately, Microsoft Office products are shipped from the factory with a built in safety function. When you open an Office document that was sent to you as an email attachment, Office disables your ability to edit the document. It also disables any macros contained in the document. But you can still get into trouble.

Once a document is opened in this safe mode, you'll see a button that allows you to enable editing or macros. If you click on that button while looking at an infected file, you're in trouble. Your computer can be infected, your files can be locked up and you could find yourself facing a demand for ransom. You could also be in trouble if you have changed the default settings in Office or other programs which limit the capability of email attachments. Or worse, if you have employees that have made changes to the default settings without telling you first.

To be sure, Microsoft Office files aren't the only ones that can cause this type of damage. But they may be the most common. Because of the danger, it is very important to be careful about the type and source of files that you open. If you don't know the source of the file, don't open it. Pick up the phone and call the person who sent it to you to find out if the file is legitimate. And if you receive a compressed file via email (one with a .ZIP, .TAR, .RAR file extension or similar) you should never open the file unless you have verified the source first.

It is also important that you train your employees on this topic and have a computer use policy in place. That policy should include serious consequences for knowingly violating the policy.

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