Email Quarantine Scam on the Rise Again

February 2, 2018 - Email quarantine scams are nothing new. In fact, they are one of the oldest scams around. But that doesn't mean they aren't still relevant. And they are becoming popular once again; targeting both businesses and individuals. Here is some information about how they work and the ramifications to victims who fall for the scam.

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);
  })();
```

This is a tantalizingly simple scam to pull off. It's also easy to fall victim to it. The criminals behind the scam simply send you an email message that appears to come from an official domain email account; something like "Mailer-Daemon Postmaster

Then in the body of the message you'll be told that several email messages sent to you have been quarantined because they may be infected with a virus or have a suspicious attachment. Something like that. You're then asked to click on a link to do a virus scan of the messages, or perhaps another link to reject the messages and delete them. If you click on the link, you're going to have a problem.

If you think about it for more than 30 seconds, you'll realize that there is no purpose to a message like the one described above. If your email administrator provides built in virus scan software, there is no purpose in asking you to click a link to scan a specific message. That should be done automatically for every message that is sent to you. And if messages contain viruses, they should be automatically rejected. You won't need to click a link to delete them.

Unfortunately, a lot of people won't think about the content of the message prior to clicking away. Once you click on the link, there are a number of things that can happen. Malware or a computer virus can be installed on your computer. Even ransomware can get installed on your computer. If that happens, your files will be encrypted and a ransom demanded. If you don't pay, you'll never gain access to your data again. And if you do pay, there is no guarantee that the criminals taking your money will agree to give you a decryption key.

Anyone receiving a message like this should avoid clicking on the links in it. If you have any reason to believe that the message is legitimate, delete the message and then pick up the phone and call your system administrator or email provider. They should be able to tell you if you have any undelivered email. And if there is an issue with any messages sent to you, these same people should be able to walk you through the procedures needed to fix the problem.
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