Crooks Using Fake Virus Notifications to Spread Computer Viruses

August 18, 2017 - This has been a tough week for email… at least for me. At the beginning of the week, my ISP decided to implement some new SPAM screening tool which seemed to block most of the legitimate email I was receiving. Then they decided that something in my email signature looked a lot like SPAM, so they started blocking my outgoing email. On another email address that I use, I started getting bombarded with SPAM. So it was no real surprise when I received a notice that two email messages that I received this morning had been quarantined for an unspecified reason. Fortunately for me, I didn't just click on the links in the message without taking a close look.

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);
})();
```

The message that I received looked like a real message from my ISP. It was nicely formatted and there were no spelling or grammatical errors. It came from "Email Administrator." Although I hadn't seen that before, my ISP typically sends messages like this from "System Administrator." It was a pretty close approximation.

The message told me that I had received two large email messages that were quarantined… I assume they wanted me to think they had attachments infected with a virus. The actual body of the message read as follows:
You have 2 new quarantined messages as of Aug 15, 2017 12:00 AM (UTC) : Action Required - Your email will stop receiving new mails because you have used up the storage limit and the pending emails will be deleted after 24hrs. Kindly follow the link below:

The links below were to supposedly release the messages to my inbox or to report the messages as "NOT JUNK," whatever that means. I suspect that clicking on either link would have put me in a world of hurt.

In smaller print at the bottom of the page were two more links. One for an "acceptable use policy" and another for a "privacy notice." My bet is that both of these would also lead to issues.

This sort of thing isn't new. Scam artists are always looking for ways to lure victims. Clicking links in messages like this could lead to your computer being infected with a virus or Trojan, or even having your computer locked up with ransomware. In my case, had the message arrived a few days earlier, even I might have clicked on it. That's because I was dealing directly with my ISPs technical support team working on email issues. What I learned here is that your present circumstances really can make you more vulnerable to cybercrime, even if you are typically very careful.
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