FedEx Phishing Scam Making the Rounds

January 15, 2013 - A new phishing scam started last month. This one currently comes wrapped in an email message that appears to be from FedEx. It is a notification that a package couldn't be delivered. It gives a package tracking number and provides a link to more information. But to the wary eye, it also provides a few clues that the message didn't come from the company that supposedly sent it. The bottom line is that you don't want to click on that link.

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);
})();

FedEx is aware of the scam and has setup a web page to give consumers more information. The page includes a couple of sample mail messages.

I personally found out about the scam when I received a mail message just yesterday. As it turned out, I was actually expecting a package delivery from FedEx which had not yet arrived. But this notification seemed a little off.

The first clue was that the FedEx logo didn't seem right to me. I'm by no means a FedEx logo expert but I've seen it on their trucks and packages enough to know that this one didn't match up. So I looked at the letter a little more closely. Three things stood out.

The letter was addressed, "Dear Customer,". Since they were sending me a package, they had to know my name. That just seemed wrong.

The second thing was that the notice informed me that the since they couldn't deliver the package to me, it was now at

my local post office. That simply didn't make any sense to me. Why would it be at my post office instead of at FedEx's offices? Eventually I would think that whoever is sending these messages might figure this out and make a change.

Finally, I took a close look at the email address that the message came from. While the name read FedEx, the mail address ended in "boise.net". That's probably the most compelling evidence that FedEx didn't send it.

Needless to say, I didn't click on the link. I simply deleted the message. For anyone who does click on one of these links, there could be some real issues.

Phishing scams like this often result in malware infecting the recipient's computer after clicking on a link. IF the computer is on a private or home network, it can infect other computers on that network too. In some cases, once malware is installed, it begins logging key strokes, collecting passwords, bank account numbers, credit card numbers, etcâ€¦ Eventually, it transmits all of this information back to the crooks who launched the scam.

One of the more troubling aspects of this particular scam is that it is likely to fool owners and employees of businesses. If a crook decides to use the scam in conjunction with malware that collects bank account information, some businesses could find their accounts wiped out. And unlike consumer bank accounts that are protected from this type of loss, businesses could find that they are on the hook for 100% of any loss that they suffer as a result.

So, as we always tell our readers, make sure that you have antivirus and antiphishing software installed on all of your computers and that the virus definitions are up to date. And if you receive a message like the one we mention here (regardless of which delivery company sends it), look at it very closely before you click on any links. If you have any doubts at all, then call the company that supposedly sent it. If the tracking number is good, they'll tell you. And if it is bad, you could save yourself a lot of pain and agony.

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