

Phishy Tales

How to spot an eMail scam

By Bill Hely

The word "phishing" has become something of a buzz word, yet many casual Internet users still do not know what phishing really is or how to identify it. In this article I will use a simple but actual email to demonstrate the most common form of phishing.

But first, a little background.

Computer and technology dictionary *Webopedia.com* defines phishing as:

"The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft."

On the origin of the word, Webopedia says:

"Phishing, also referred to as brand spoofing or carding, is a variation on 'fishing', the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting".

OK, but how do you distinguish between a phishing eMail and a real message from, say, your bank or credit card provider?

A phishing message may look very legitimate, with all the right corporate logos and so on. Even some of the links in the eMail may be the real thing. Although there are often tell-tales such as poor spelling or bad grammar, many examples of this scam do appear to be perfect in every respect. The only way to see what is really going on is to look "under the covers". More on that in a moment.

What the scammer is trying to do is get you to click on a link that will take you to a website which is different to the one to which you expect to be taken. At the fake web page the scammer will try to get you to enter sensitive information, commonly credit card, on-line banking, PayPal or eBay account details.

Now, it's important to understand that there are two types of eMail formats:

- **Plain Text:** Exactly what the name implies. A plain text eMail cannot contain formatting codes, such as those for bold, italic, underline, font-face variations and so on; nor can it contain images. It's not just that the plain text eMail *doesn't* contain such capability, but more to the point it *can't*. The format simply doesn't allow it.
- **HTML:** This type, however, can contain images and fancy formatting. But the most important feature (when considering embedded threats) is that a HTML format eMail can contain *hyperlinks*. Hyperlinks are something you have seen often—a word or phrase (on a web page, for instance) that is clickable. By convention hyperlink text is usually blue and underlined, but it doesn't have to be.

So with plain text emails, what you see is what you get. If the text of a hyperlink reads www.CitiBank.com then in a plain text email the Citibank website is exactly where it will take you.

But all is not so transparent with hyperlinks in HTML email. With HTML the only way to tell where a hyperlink will really take you is to look at the HTML code that underlies the

Phishy Tales

link. And "No", you cannot tell by hovering your mouse cursor over the link and looking at the status bar. The status bar message can be removed or faked very easily.

Another trap to be aware of...

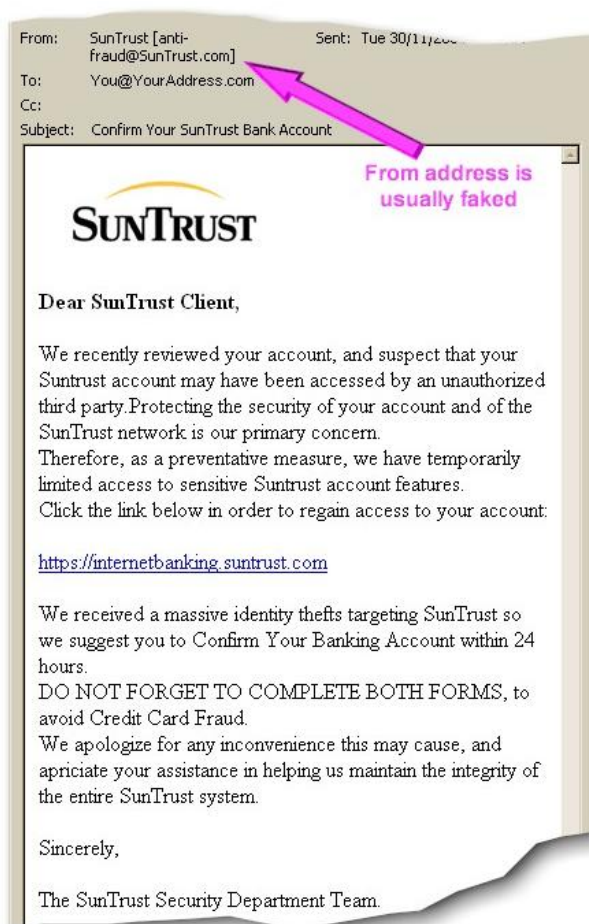
I said above *"It's not just that the plain text eMail doesn't contain [hidden formatting codes], but more to the point it can't."*

My point was that a HTML eMail that doesn't appear to contain any formatting is still not a plain text eMail. The plain text format and the HTML format are quite different things and one cannot become the other merely by the inclusion or omission of obvious formatting.

Whether you can see it or not, the HTML eMail does contain embedded formatting codes. A common trick of scammers is to make a HTML eMail look like plain text, so that any hyperlinks it contains will be taken at face value.

Far too often people will just assume that a message is plain text if it doesn't contain any images or fancy formatting, and it is rendered in a plain serif typeface. Not so. The HTML message, which by its very nature allows link deception, can easily be made to look like a text message to the unwary.

OK, enough of that. Let's turn now to how we can expose the phisher, *blow his cover*, so to speak.



All eMail client programs of which I am aware provide some means for you to look at the underlying formatting code. In Microsoft Outlook, for instance, you can right-click on the body of the message and select "View Source" from the pop-up menu.

I've selected the scam eMail I'm going to use in this tutorial because it is a simple example without too much HTML formatting to complicate matters. The original eMail as it appeared in Microsoft Outlook can be seen at left.

In a moment I'll show you the HTML code associated with that eMail. Don't worry if you don't understand HTML code at all—I'll explain the few important parts.

First, just a bit of general information about formatting codes to help you make sense of what you see.

In HTML code, anything that is between <angle brackets> is called a "tag". A tag is the actual code that

tells the web browser how to display the message text. In this simple example there are only a few tags in use, and only one of them is important to us.

Phishy Tales

Here is a list, with brief explanations, of the tags in use in the example eMail. These items will make a lot more sense when considered in association with the actual code lines listed further on.

<code><img src=</code>	Following the equals (=) sign will be the location of an image that is to appear at this point on the page. The tag must then be "closed" with a right-angle bracket <code>></code> . See Lines 1 and 2.
<code>
</code>	A line break. Several together is a series of line breaks. E.g. line 3.
<code></code> and <code></code>	The text that appears between them will be in bold type. See line 4.
<code><a href=</code>	Indicates an Internet hyper-link. The web address that follows the "href=" term is the "target" web address; that is, the web page to which your browser will be taken if you click this link. After the target web address, the tag must be "closed" with a right-angle bracket <code>></code> . This tag must also be terminated with a <code></code> tag (see lines 16-18). Anything that appears between the <code></code> and the <code></code> is simply a comment, regardless of the fact that it may look like a web address. <i>This is the one really important point and an appreciation of it is critical to the following analysis.</i>

Now here's the actual HTML code that makes up the eMail message pictured above. As stated above, to see this code in MS Outlook you right-click on the body of the message and select "View Source" from the pop-up menu.

NOTE: I have added line numbers for ease of reference, but they are NOT part of HTML code.

```
1. <img src=
2. "http://www.suntrust.com/images/Common/release3/logo_home.gif">
3. <BR><BR>
4. <b>Dear SunTrust Client,</b><BR><BR>
5.
6. We recently reviewed your account, and suspect that your
7. Suntrust account may have been accessed by an unauthorized
8. third party.Protecting the security of your account and of the
9. SunTrust network is our primary concern.<BR>
10.
11. Therefore, as a preventative measure, we have temporarily
12. limited access to sensitive Suntrust account features.<BR>
13.
14. Click the link below in order to regain access to your account:<BR><BR>
15.
16. <a href="http://www.toyworld.org/SunTrust/">
17. https://internetbanking.suntrust.com
18. </a>
19. <BR><BR>
20. We received a massive identity thefts targeting SunTrust so
21. we suggest you to Confirm Your Banking Account within 24
22. hours.<BR>
23.
24. DO NOT FORGET TO COMPLETE BOTH FORMS, to
25. avoid Credit Card Fraud.<BR>
26.
27. We apologize for any inconvenience this may cause, and
28. appreciate your assistance in helping us maintain the integrity of
29. the entire SunTrust system.<BR><BR>
30. Sincerely,<BR><BR>
31. The SunTrust Security Department Team.<BR>
```

Incidentally, note the misspelling of "appreciate" on line 28. There are other errors also, such as a missing space in "party.Protecting" on line 8, and lines 20-21 are poor English. Real financial institutions rarely make such obvious errors.

Phishy Tales

Now, it is lines 16 to 18 that are critical to our investigation of this scam. Line 17 is apparently a link that suggests we will be taken to "internetbanking.suntrust.com". There is no reason to be suspicious of the address itself because it is after all in the SunTrust domain and thus on their website. But...

Line 17 is not inside a tag, as denoted by an opening < and a closing >. The tag that indicates the real target of the link is on the previous line, line 16. The text "https://internetbanking.suntrust.com" on line 17 is just that—nothing but text. It could just as easily read "Find Nemo here" and it would have the same effect. The real target of the link is, as line 16 indicates, "http://www.toyworld.org/SunTrust" because it is in the "<a href" tag. And ToyWorld.com is obviously not SunTrust Banking!

The moral of the story:

Do not trust APPARENT links in HTML email. Either check the underlying code as described above, or cut and paste the apparent link directly into your browsers address line. If you click on it, you could end up at a scammer's webpage that looks legitimate, but will be anything but.

Further, don't just assume that a message that looks like plain text really is; it may be HTML designed to look like plain text.

In short, a prompt like "Click here" could take you to anywhere—you probably already appreciate that. But www.CitiBank.com could also take you to anywhere. Like "Click here", it is just text, despite the fact it looks like a legitimate web address.

-oOOo-

Bill Hely is a technologist, consultant and author living in Brisbane, Australia. For most of the last two decades his professional focus has been on advising and supporting small business operators in Information Technology and Office Productivity. He is the author of several books on technology for the business operator, including the Bible of Internet and computer security *The Hacker's Nightmare*™.

To comment on this article please use the "Support" link at the bottom of the <http://HackersNightmare.com> main page.

Comments, suggestions, expressions of appreciation
— and especially testimonials —
are most welcome.