

# Outlook Express PHISHING

© Darry D Eggleston, 2006, [DarryD@darryd.com](mailto:DarryD@darryd.com)



*Phishing*, pronounced “fishing,” is a scam to steal valuable information such as credit cards, social security numbers, user ID (identification) and passwords. Also known as “brand spoofing,” an official-looking e-mail is sent to potential victims pretending to be from their ISP, retail store, etc., and that due to internal accounting errors or some other pretext, certain information must be updated to continue the service.

A link in the e-mail message directs the user to a Webpage that asks for financial information. The page looks genuine, because it is easy to fake a valid Web site. Any HTML page on the Web can be copied and modified to suit the phishing scheme. Such e-mails can be sent to people on selected lists or to any list, expecting that some percentage of the recipients will actually have an account with the real organization. The term comes from “fishing,” where bait is used to catch a fish. In phishing, e-mail is the bait.

Here’s how to discover and to deal with it.

1. Here is an example message (Figure 1).

Ask yourself, “Why would they give me a laptop?”

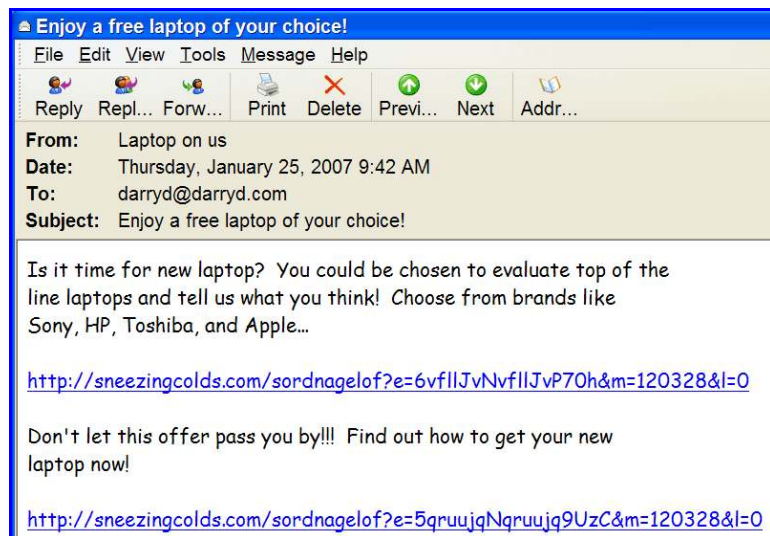


Figure 1

2. To find the sender's address (Figure 2):

1 RIGHT-click on the Sender's visible address.

2 Look at the sender's address.

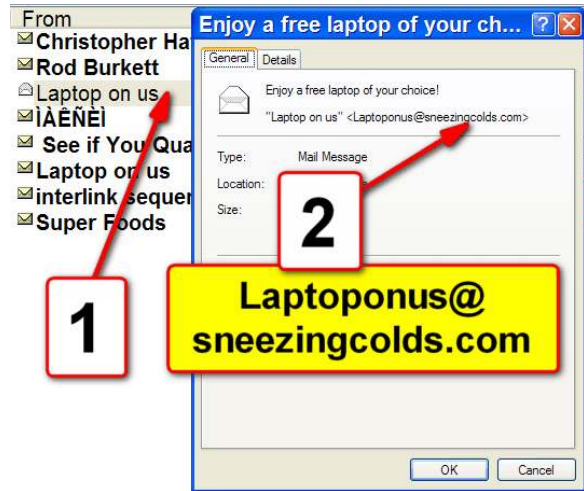


Figure 2



Figure 3

3. Phishers are not stupid. They **often** create websites to “validate” their e-mail addresses (Figure 3).

Clearly, their goal is to get your e-mail address — and more.

4. Sometimes, when they originate in a foreign country, you can spot them because of their poor use of English (Figure 4).

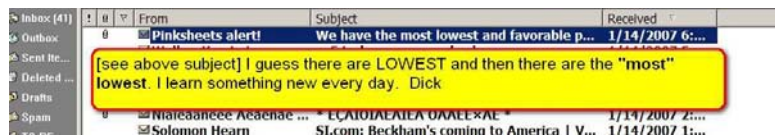


Figure 4

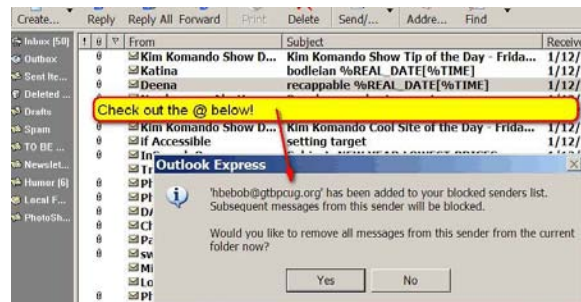


Figure 5

5. Sometimes, a *phisher* will “spoof” an organization that the e-mail receiver is likely to recognize. In this example, the phisher has used the domain of the Greater Tampa Bay PC User Group < <http://GTBPCUG.org> >.

6. Using well-known Internet-access providers, phishers get a lot of unwary people to click on a link and expose themselves to attack (Figures 6 & 7).

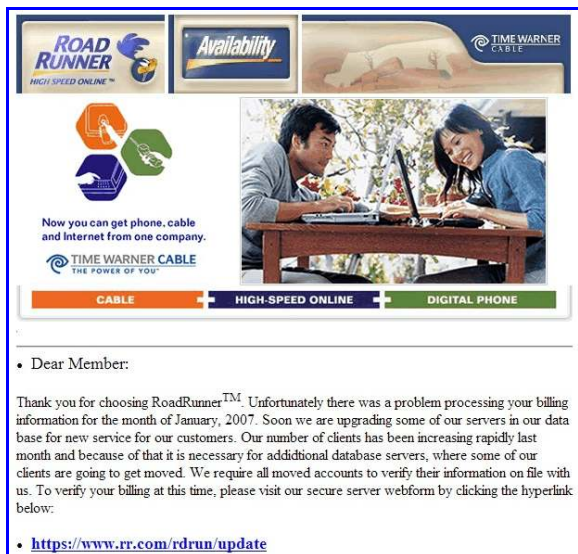


Figure 6

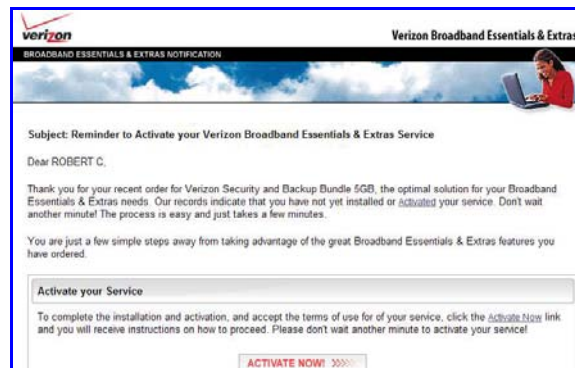


Figure 7

7. Sometimes, the offer is just too good to believe; but, doing what I told you to do in paragraph 2, you'll see what the real sender's address is (Figure 9).

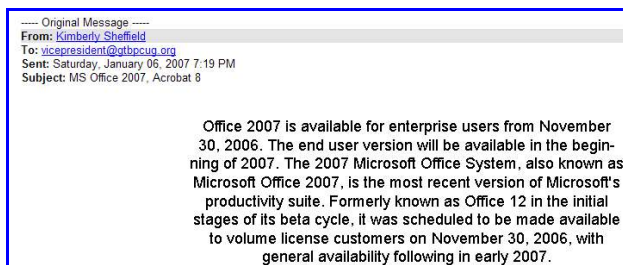


Figure 8



Figure 9

8. What to do? Delete the message or block sender. Whatever you do, try to avoid opening the message; but, if you do, do *not* click on any links.

Again, if the offer seems too good to be true, it almost certainly is.