

IDENTIFY SENDER

© Darry D Eggleston, 813.677.2871, DarryD@darryd.com

Click on the blue, underlined text to go to its linked reference.



You receive an email from someone who should be a friend, but something tells you that it might be someone *phishing*.

Phishing, pronounced “fishing,” is a scam to steal valuable information such as credit cards, social security numbers, user identifications and passwords. Also known as “brand spoofing,” an official-looking email 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, some info 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 emails 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, email is the bait.

How do you tell who the email is coming from?

1. RIGHT-click on the email line (**Figure 1**) and then Left-click on the “Properties” line.

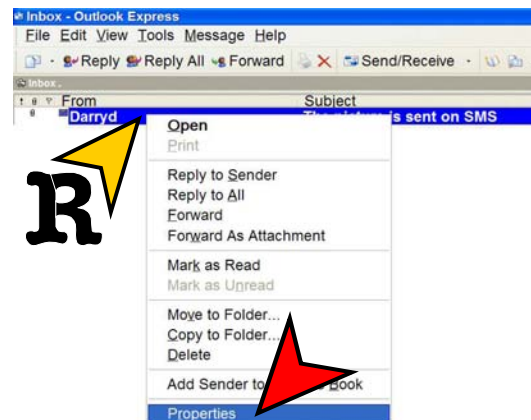


Figure 1

The sender's name and email address shows in the resulting pop-up window (Figure 2).

The sender can call himself anything, but the email address will reveal who it really is.

In this case, the sender is spoofing my email name, but the email address is not mine. (See mine at the top of this article.)

3. IF you click on the "Details" tab, you will see more details about the sender (Figure 3).

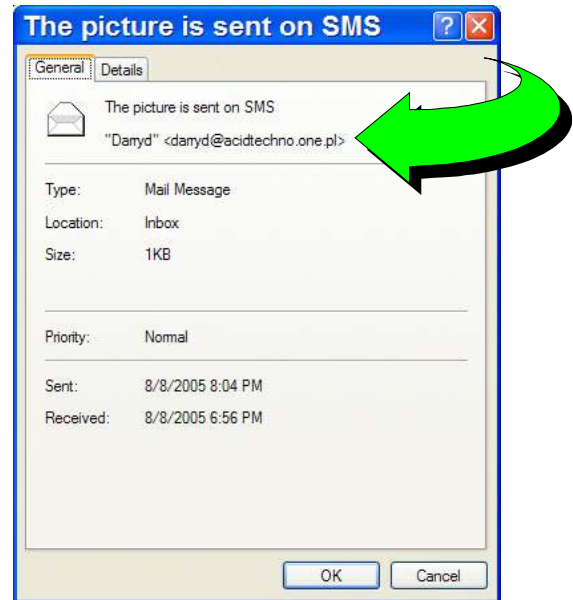


Figure 2

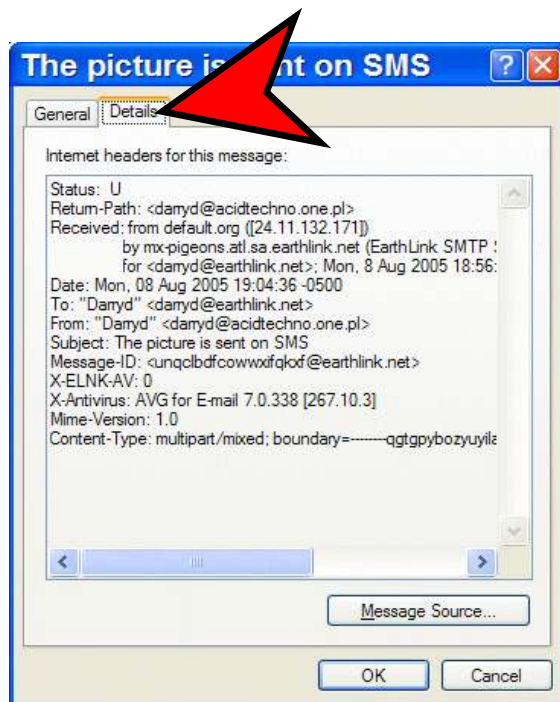


Figure 3

4. If you click on the "Message Source" button at the bottom-right of the Details window (Figure 3), you'll see more info (Figure 4).

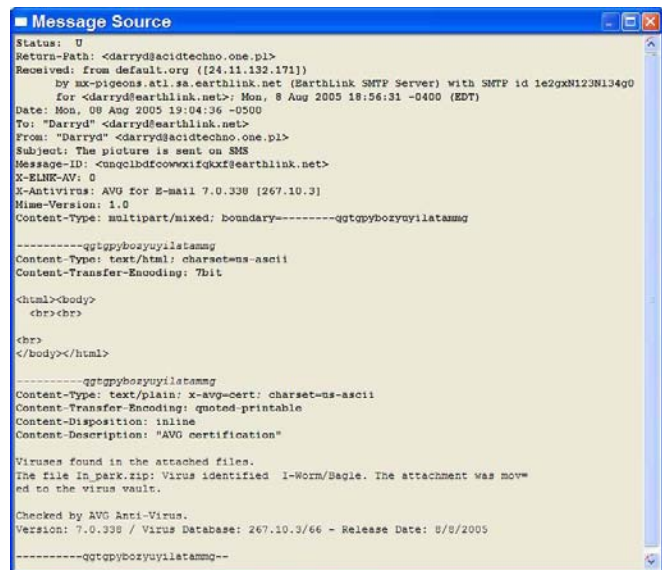


Figure 4