

The graphic in the fraudulent e-mail masks the actual URL, which as you can see in the example, is not the one depicted on the graphic itself.

A genuine URL for a secure Website begins with “Https.”

Also, once you have completed the link to the secure site it will be confirmed by the image of a padlock located as an icon in the bottom right hand corner of the Browser window. If this is not there you have not accessed a secure site.

The URL address provided on the graphic in the fraudulent e-mail appears genuine and actually is up to the point that it links to a U.S. Bank Website folder called “confirmation.” Everything in the address from that point is bogus. If you type the bogus URL address into the address block in your Browser and try to access that link, you will notice that you link with a page on the real U.S. Bank Website that says “Page Not Found.”