(Approx. 534 words)

Phishing Expeditions

By Dorothy Fitch, Editor, Green Valley Resort Computer Club, AZ

April-August 2019 issue, Green Bytes

www.ccgvaz.org

Newsletter (at) ccgvaz.org

February's *Green Bytes* included an article about "Phishing" ([click here to read it](https://ccgvaz.us16.list-manage.com/track/click?u=fc5b48c8cad5d194a77f4cb54&id=b651766ec1&e=2857111c01)).

A "phishing" email is one that attempts to obtain your personal account information to use for unauthorized purposes. When I included that article in *Green Bytes*, I hadn't personally received a phishing email. But this month I did -- twice! Both appeared to be from familiar companies (Amazon and American Express), but there were several clues that they were attempts at phishing. Here is how I knew.

1.  Both messages came to an email address I use for a non-profit organization. I know that the email address these messages came to have never had an account or been associated in any way with either Amazon or American Express.

2.  Both messages looked as though they had come from the named company. The logo and color schemes were appropriate. They both were similar in that they said that my account had been disabled or locked. They both wanted me to update or confirm my account information. (No way was I going to do that!)

You can safely click the images below to enlarge them. They won't take you to a website.



3. Then I looked at the email address of the sender.



The Amazon email was sent from support@inbox.com.
The American Express email was sent from support313526X@true.com.
Neither of these email addresses appeared to have any connection to the companies they were supposedly from.

4. I looked at the link in the email from American Express (but I didn't click it!).
If you hover your mouse pointer over a link, you can see before you click where it will take you. Just look at the lower left of your computer screen to see the link information.

The link in the American Express link was this (note the letters amx in the link):

Although I didn't click on the link, I was brave [stupid?] enough to go to [www.ahmetcaglar.com](http://www.ahmetcaglar.com/) to see what was there (so you don't have to do it!). When I got there, Google suggested that it translate the website into English (it was in Turkish), so I did.

What did I find there? The bio of a Turkish computer science student! He used his name for his website. I guess he doesn't care about keeping under the radar. Perhaps he was just experimenting with a concept without any intention of causing harm, but we'll never know....

I found it very interesting to take a closer look at these phishing emails. The lessons for everyone are:

* Look at the sender's email address. Does it seem to really be from the individual or company you expect?
* Don't click on any links, if you aren't 100% sure who the email came from.
* Absolutely do not give out any account information to anyone who contacts you.
* If you want to verify if an email is for real, call the company; don't reply to the email. You can probably see if your account has been locked by going directly to the company's website, the way you normally would, and see if all is well.