



COVID AND PHISHING

Phishing is a highly effective technique for the distribution of malware of all kinds. Phishing is the term applied to emails designed to catch your interest and get you to click a link for more information. You may get information, but you will certainly get malware.

You do have to give cyber criminals credit for their adaptability and speed. But remember, their intent is evil, to steal something of value from you, so let's not give them too much credit.

Phishing catches your attention with a subject line about something that concerns you or something you want to know more about. Yes, this is broad and the subjects change and fluctuate. Until about 14 months ago no one except epidemiologists and other medical researchers had heard of Covid-19. So not a good topic for phishing.

But then..... in a short space of time everyone wanted information on Covid-19. And a new phishing email subject line was born.

And did it ever attract attention. People clicked on those links like it was free money.

As Covid-19 came more into the public eye, the phishing emails adapted with new subject lines. For instance, is it safe to go to public places, or how to go to public meetings and be safe from Covid-19. Or anything to do with masks. Do you need one? Are masks a plot? Is Covid-19 a plot? Is Covid-19 real? And so on.

Now, the times have changed again, and the subject lines have changed with the times. Now we are no longer looking for basic information on the virus.

But how about, information about the vaccines? Do the vaccines work? What if I don't take it? What news sources are to be trusted? Is one vaccine better than another? What are the side effects? Can the vaccine cause sterility? And on and on.

Hot topics have pivoted again. Have the new variants been seen in this country? Are there new symptoms? Are the vaccines effective against the new variants? All of virus variants, or only specific ones?

Corollaries of the Covid-related phishing emails are about the stimulus programs. Has the new stimulus been passed? For how much? When will I get my money?

And so on and so one and so on. By now you should get the message. The topics will be things of interest and will change with the times.

But avoid the impulse and do not click on a link in any email, even if it appears to come from a reliable source or a friend. Delete those emails immediately. If you want information, open your browser and go directly to a reliable site that you trust.

Want to learn more about cyber security and education, contact AIM Cyber at info@AIMglb.com or call (888) 773-1920.