EMAIL PHISHING FRAUD

REMAX " HOT PROPERTIES "

By Philemon Yalamu (http://www.artech.com.pg/) -19/02/13

Have you ever received an email with subject above (*in RED*)? Well if you did, then this article would give you an overview of the dangers you've gone through. If you haven't, please read the article and use it to help you avoid being in the loop of being fooled.

Basically, the purpose of this article is to help those who have already being fooled into giving out their private information to spammers. However, it could also be useful for those who haven't received this email yet so they are aware.

Firstly, let me make it clear that one of the most effective tactics used by spammers lately is the hijacking or theft of legitimate user's email accounts for use in furthering spam campaigns.

I've recently received an email from a colleague with the same title. I know for sure that this is a spam however I wanted to confirm before writing up an article on this and post it on my blog (http://pyalamu.blogspot.com) so I clicked the link to read the header. After confirming, I decided to complete this article for the sake of others who would not be in the better position of understanding the risk. I have also forwarded the link to various emails particularly to those that are linked to the email I received. If you are one of those who read this article, please forward the link to your friends to help them protect their private information, especially their email credentials.

The demonstration I'm going to do would be presented using Gmail however, it's similar to other email listed in the article.

Here's how it goes;

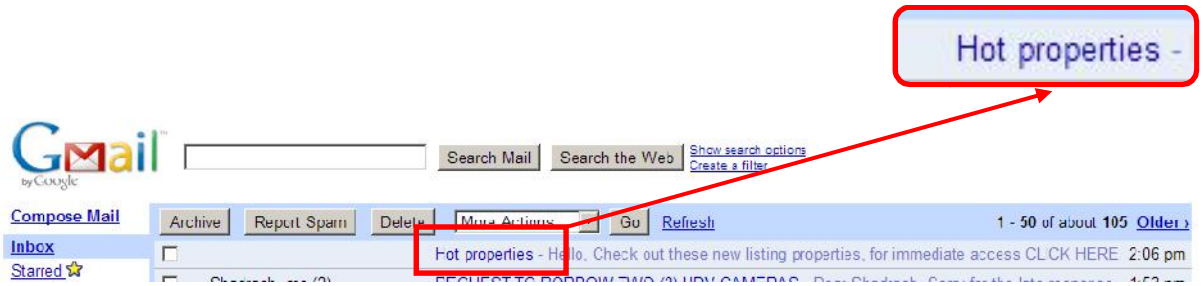
First, you receive an email. What you would have heard was, if you know the person who sent you the email, you can feel free to open it because it is probably not a spam. However, spammers are smart. They go around the other approach to get what they want.

Recently, there are emails circulating which have the title "***Hot properties***" or similar? The email comes from a known source or contact. This, I mean from someone whom you know within your contact listing. Considering the short brief above, you would realise that the

person sending you the email is someone whom you knew. Naturally, you would want to open the email because you knew the person sending you the email.

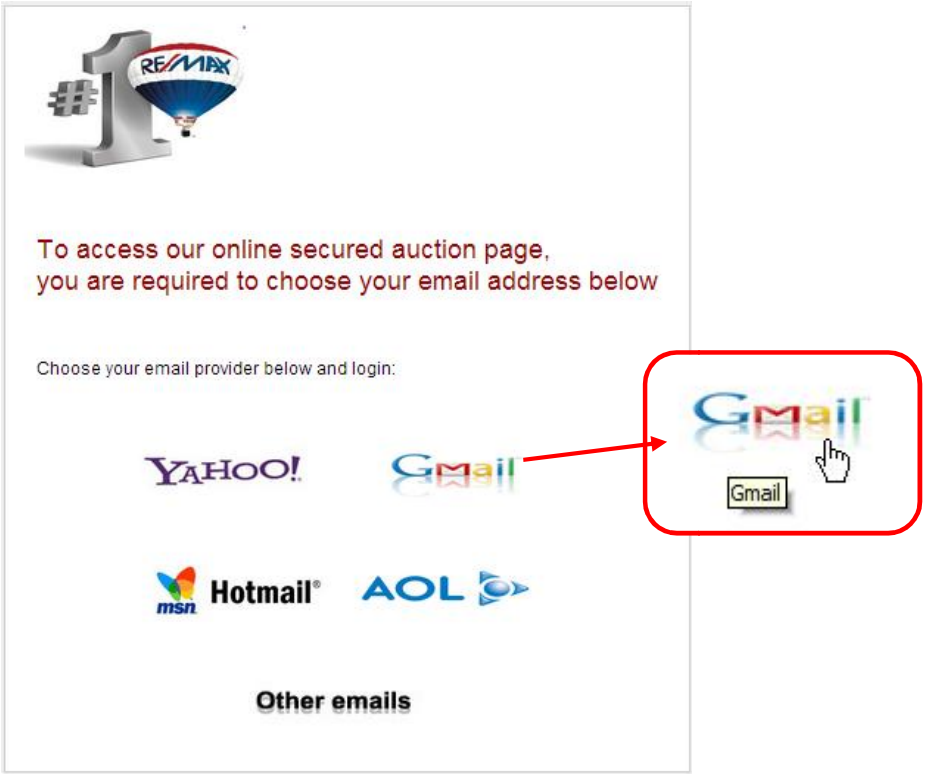
Ask yourself, did you open the email? If you said yes, that means you clicked on the subject to access the link.

Now, regardless of the exact subject and content of the email, clicking the link would take you to a site that requires your authentication to access their provided service once you sign in with your email account credentials.

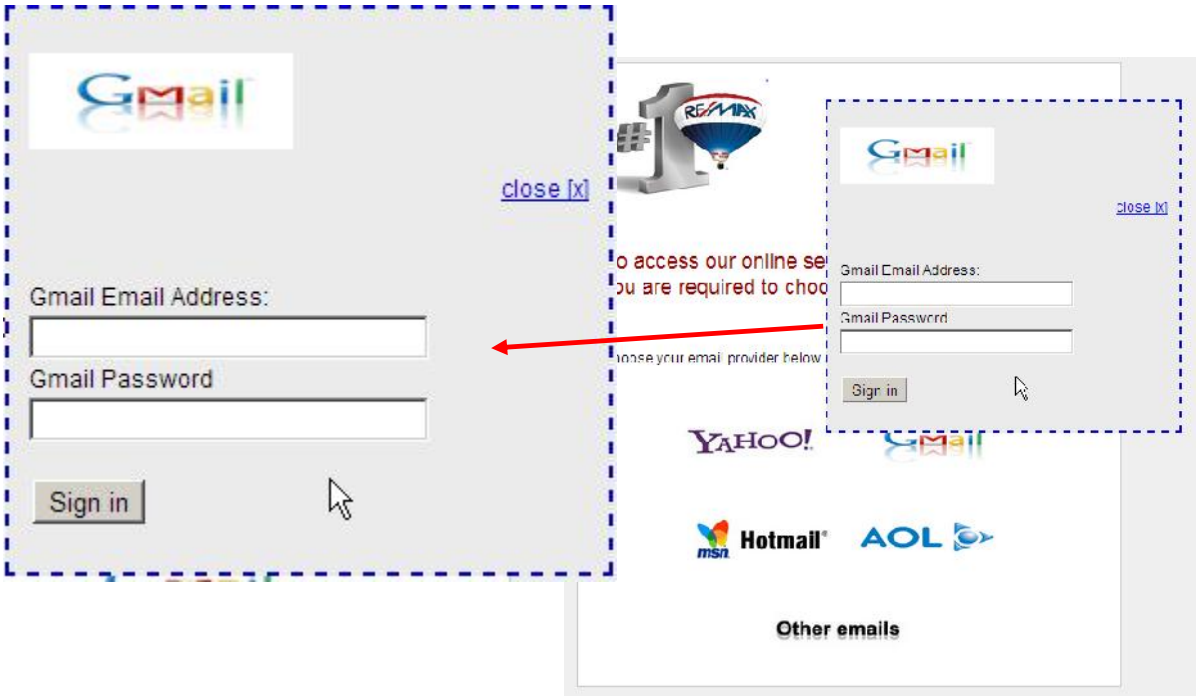


I assumed you are one of those who have clicked the link. If you haven't received such email yet, you might probably receive one soon because it's on its way to your electronic mailbox.

So, when you clicked on the subject "**Hot properties**" or similar, have you been taken to a page similar to the one below?



Have you tried to go further by clicking any of those email providers' logo (*Yahoo, Gmail, Hotmail, AOL, Other emails*)? If you did, were you prompted with a pop-up window like the one below?



I'm pretty sure for most of you, you probably would say, Yes, I did sign in for some unknown reason. That is normal and it's natural for most users. I believe, a psychologist could explain further on this behaviour.

Normally, you would enter your details and press the sign-in button to log in assuming that the signing will grant you access to the provided service mentioned in the email you got.

The thing that is convincing after you sign would be the access to the site providing the proposed service. For the case here, entering your user credentials would grant you access to the Re/ MAX listing site. To you, it would be convincing because through signing in you gained access to the site however behind the scenes (*from within the back-end*) what happened was you provided your login details to the spammer through the script hidden within the source codes.

The spammers do know that you would come up with suspicions when things go wrong especially when you enter your login details and they do not log you in so they fake a login page that will redirect you to a page that tries to convince you that things are fine. Sometimes, the links take you to a fake site with the exact site name. Other times, it takes you to a temporary page showing an error message and redirects you to go to the legitimate pages and sites using provided links.

Above all, the end result is that the spammer now had access to your email account whilst at the same time you are now carried away with exploring the RE-MAX website looking for

these “Hot Properties” and you no longer bothers about what you have done to yourself and all your friends, family or contact in your contact listing.

Feel free to forward the link to your friends to help them secure their private information. Visit my website (*http://www.artech.com.pg/)* for other helpful tips and free tutorials.