

Classic Facebook Phishing

While cyber threats continue to advance in new and intimidating ways, classic phishing methods are still a favorite among bad guys. Let's take a look at a recent Facebook-themed phishing attack and see if you can spot the red flags:

The email appears to come from Facebook and starts with "Hi User". The body states that there is an issue with your account that you must log in to resolve. The email includes a link to "verify" your account and ends with the line "This link will expires in 72 hours, We appreciate your attention to this matter." If you click the link, you are taken to a phony look-alike Facebook login page. Any information that you enter on this page is delivered straight to the bad guys.

How many red flags did you see? Remember the following tips:

- Question everything. For example, your name is part of your Facebook profile, so why is the email addressing you as "User"?
- Look for a sense of urgency. In this example, the email gives you 72 hours to verify your account. Remember, the bad guys rely on impulsive clicks.
- Pay close attention to the grammar and capitalization. For example, the words "This link will expires in..." should be "This link will expire in...". Also in that same line, the word "We" is in the middle of a sentence, so this should be lowercase.

Stop, Look, and Think. Don't be fooled.