OMG! Did you see this picture of you?

Both Facebook and Twitter have been plagued by several phishing scams that involve a question that piques the user's interest and then directs them to a fake login screen. Typically, the user receives a message, such as "Did you see this picture?" with a link also included. The user clicks the link, and it prompts them to enter log-in credentials on a fake log in screen.

On Facebook, for example, members might receive a message in their inbox, or a message on their wall, that directs them to another site which looks identical to the Facebook log-in page. Just last week, Twitter users recently began receiving tweets that asked "OMG! Is it true what they said about you in this blog?" The link directed the user to a screen that looked just like the Twitter log-in page, but was instead a phishing site. Of course, once you've entered your user name and password into one of these fake sites, the criminals engineering the con have easy access to your account. Sullivan said another recent version of this scheme included messages requesting users update account information, which then took them to fake log-in screens.

This is a classic phishing ploy, according to Cluley. Hackers may be looking for your account information in order to send spam, or pose as you in order to pull off a 419 scam like the one mentioned above. In order to avoid having this happen, make sure you check the url before entering your log-in information. If your browser bar says anything other than Facebook.com or Twitter.com, leave the site immediately.

The other potential in this scam is spyware infection, said Cluley. The tiny url function makes this even easier for scammers because you can't see the link you are clicking.

"You click on a link that is infected with spyware, and it can steal credentials, bank information, all kinds of useful information about the different accounts you may have," he said.

Bottom line: If a link or a message seems suspicious; click at your own risk.