

## Phishing Scams - How To Detect Them

Since the Internet began, it has been an incredible way to do business, socialize, increase knowledge, blog, and even commit crime. In fact, no other venue in the world has given the cyber criminal such a huge hunting ground for his or her next victim. Sadly, many people are Internet illiterate and do not seem to recognize the dangers associated with this type of activity and many suffer for it. The Nigerian 419 scam is one of the most prevalent. It lures people into thinking that, if they help some family smuggle millions of dollars out of their country, they will in turn pay them (the intended victim) a portion of the proceeds. The victim will, of course, have to pay various "fees" to help get the money transferred. These fees will often drain the victim's accounts before they realize it. These would be thieves are even brazen enough to call their victims and share sad stories with them. This is designed to continue to lure the victim in. There have been a surprising number of people who do not think about what they are doing and fall for it. In a number of cases that I have read about, the victim even goes to the country in question to get his money, only to suffer the final humiliation of being run back out of the country by the country's "officials" who are actually part of the scam ring. A couple of the stories I read indicated that the victims were in fear of their lives. Some of the other victims were even murdered. One important point to remember is that U.S. banks are required to report unexpected or suspicious account activity which, in turn, causes the government to investigate such banking activity. It is my understanding that this type of banking transaction is illegal and could very well land the victim in jail. Most of the time, this scam starts out via e-mail. These e-mails can begin by informing the victim that they have won a fabulous prize or cash in a national lottery or, as in the example above, can be a plea for help in moving large sums of cash out of some war torn country (there are a number of variations to this story). These e-mails look real, sound real, and some of the more sophisticated ones have the real company or organization's logo on them. In all the cases that I am familiar with, they inform the victim that he will have to pay some "fees" in order to get his "check". This, by itself, should be a red flag to anyone who gets themselves involved in these types of scams. No lottery that I am aware of will force the "winner" to pay fees to get their winnings. Though there are no hard and fast rules to detect a scam, here are a few red flags to watch for. Do they ask for fees? Does the actual url match the one in the e-mail?(Most of the time, it won't.) Many of these e-mails are sent in html (so they can present the company logo as in the national lottery scams). Place your mouse pointer on the link without clicking it. More often than not, the link displayed in the url repeater will not be the same. Another red flag should be in how the e-mail is addressed to you. Another, and probably more important red flag, is this: Do they ask for your financial and personal information? This, by itself, should alert you that something is amiss. Any e-mails you get from any financial institution should be treated with a healthy dose of suspicion. If you have any doubts forward these e-mails to the company's fraud department. Never, click on the links supplied in these e-mails and never reply to them! Even if legit, you should adopt the practice of opening a new window and going directly to the site from there. In the case of the lottery or Nigerian scams, simply delete them or report them as spam.

## About the Author

Ryan Smith is the author of the hot, new, blog "The 10 Commandments of ID Theft Protection" Learn more at <http://www.e-profitsubmissions.com/wordpress>

Source: <http://americanahost.com>