DON'T FALL PREY TO ONLINE "419" SCAMS

FACEBOOK, MYSPACE, E-MAIL…DON'T GIVE YOUR MONEY TO THE CRIMINALS!!

We've all seen the spam e-mails…someone with poor spelling and grammar is sending you a letter, claiming to be a staff member of some deposed (but good) African politician, trying to get money out of the country so that the evil government can't seize it. Of course, if you help him, you'll get a cut of the cash. Sounds good, right?

These scams are called "Nigerian" or "419" scams, for the Nigerian Criminal Code section for obtaining property by false pretenses (a.k.a. fraud). They have been circulating around in one form or another since the 1920's, and have evolved over time. They can come from any country, and have any kind of backstory (including the ever-popular Canadian lottery scam)—but the end result is always the promise of loads of cash for you, so long as you give up some cash up front.

The scary part is how personal they have become. The newest incarnation involves someone hacking into your Facebook account and posting messages telling your friends that you're stuck in London. Sometimes they claim your wallet was stolen, sometimes they claim you're in some kind of legal trouble… either way, they want your friends to wire money via Western Union to London (or some other foreign city) to bail you out. And of course, they've changed your password so you can't get into your account to stop them.

If one of your friends on Facebook (or MySpace, or any other similar site) suddenly starts posting messages about being stuck somewhere abroad and needing cash urgently, *stop*. THINK. Call the person first, even if you think they are likely to be abroad. Chances are they're sitting at home, right in their living room. **NEVER wire money abroad via Western Union or any other third-party service unless you can verify EXACTLY who it's going to.** If you want to send money because you believe the person might legitimately be in trouble, do it via bank transfer, direct into that person's account.

Many people have been victimized by this scam, some losing thousands of dollars. The scam preys on the good nature of caring friends and relatives, and seems all the more believable because it's coming from your trusted friend's account.

If you, or anyone you know, has fallen victim to this scam, or has had their account hacked at all, there are options. Facebook has a page where you can report the hacking of your account or a friend's, at https://ssl.facebook.com/help/contact.php?show_form=419_scam2. Don't be fooled by the page's name ("419 Scam") - it can be used anytime an account has been hacked.

There are some protective measures you can take. If you don't already have one, add a secondary e-mail address to your account, so that if it becomes compromised you can still get in. And never click on a link in an e-mail and then login, even if it seems to be from the website it claims to be—phishing e-mails have gotten quite sophisticated. Even if the URL that shows up at the top of the screen is the correct and not a spoof URL, that doesn't mean that your password isn't being copied. Some phishers simply send a fake e-mail that, when the link is clicked, the real webpage opens up with a hidden "window" overlaying it that catches anything you type or click. **ALWAYS type the URL in yourself**.

For more information, visit the following websites:
Snopes - http://www.snopes.com
MSNBC's Red Tape Chronicles: Facebook ID Theft Targets Friends - http://redtape.msnbc.com/2009/01/post-1.html
Facebook Security Group - http://www.facebook.com/security

A MESSAGE FROM THE CITY OF LANCASTER'S PUBLIC SAFETY OFFICE