Has one of your friends apparently sent an email like this?

My sincere regrets for this sudden request, things actually got out of control on my trip to London. I was mugged,all my belongings including cellphone and credit card were all stolen at gun point. I need your help flying back home and paying my Hotel bills. Am cash strapped at the moment. I've made contact with my bank but the best they could do was to send me a new card in the mail which will take 3-5 working days to arrive here.

I need you to lend me some quick funds to sort my self out of this predicament, i will remit the funds as soon as i return. Western Union or Money-Gram is the fastest option to wire funds to me. Let me know if you need my details(Full names/location) to effect a transfer. You can reach me via my email because the hotel has internet access in the lobby I'm sorry for all the inconveniences. I just didn't know how else to contact you quickly.

Thanks

It's a scam. Here's what I do in response: I send my friend the following email (I sent this today to an OPC missionary in Uganda whose GMail account was hacked), and / or call him on the phone:

You should know that this email went out impersonating you using your email address.

I'm somewhat familiar with the scam below, because a number of my friends have been victimized by it. Most of my friends don't travel out of the country very often, but you do(!) so the email below might fool more recipients than normal. Normally the way the scam begins is by a hacker hacking into your real email account and sending false emails from your email account to people in your address book. Because it begins that way, the two key steps to fixing the problem are:

1) to change your email account's password, and

2) to double-check that email account's backup email address--the email address (like one

on Yahoo or some other domain name) which in this case GMail will use to communicate with you in case they cannot contact you through your GMail email address--GMail will send your password to you at that backup address if you ask GMail to remind you of your password. Scammers sometimes change that backup email address to one they have access to, so they can request your password if you change your password to keep the scammer out of your email.

Another thing you should do, if you believe the email below went to others in your address book (the "To" header of the email I received said "undisclosed-recipients:;" which means my email address was in its BCC (blind carbon copy) list, so I can't tell how many people received the scam email) is

3) notify everyone in your email address book that the email below is a scam.

How did the scammer hack into your email account? I've heard of several ways:

- they can run a program that tries millions of passwords out on your account's login form,
- or they can do "packet sniffing" on wireless networks that are not secure (they require no passphrase or encryption key) or use weak encryption (WEP encryption is weak encryption and software is readily available to break through its encryption quickly),
- or if they have access to the router / wireless access point (like they own the coffee shop), they can do "packet sniffing" too, which is where they examine the "packets" of HTTP traffic between your computer and the router and find your password in that traffic,
- or they can create a JavaScript link in (or just a script that runs in the HTML of) an email that steals your email account's password from a cookie in your web browser (this only works when you're viewing email in the same email account that is being hacked)
- or they can put JavaScript code in a web page that exploits a security flaw in your browser and thereby steals a cookie or your password directly from your email provider's page in ANOTHER TAB in the same browser window or perhaps in another browser window.

I mention all this detail because you're in Uganda, and it would be wise to take several further measures to prevent this from happening again:

4) Beware that on unsecured, or on WEP-encrypted networks, you should avoid logging into accounts you don't want hackers to get into.

5) Even at strongly-secured (WPA encryption) wireless and wired networks in public locations, be aware that you cannot always trust the owner of the network. Decide whether you trust the owner before using a password over the network.

6) Upgrade your web browser to its most recent version.

7) To deal with the first JavaScript hack method mentioned above, don't click on links in your email, and consider (depending on how paranoid you want to be) not opening other web browser tabs or windows where you'll enter a password while reading your email. Instead, if you want to be as secure as possible, you can open just one tab in one window, enter the password, do your work, then log out, (optionally clear your cookies, but I wouldn't do that), then close the browser window.

8) To deal with the second JavaScript hack method, don't enter passwords in one browser window or tab when you have another browser window or tab open. Especially avoid the situation where one tab has your bank account open, and the other tab has an untrustworthy (maybe local Ugandan) site open, because that is the sort of situation the second JavaScript attack exploits.

I know some of the above practices may be more restrictive than what you need to do in your situation, but I want you to be aware of the best recommendations I've read to deal with this sort of problem, and you can decide what you think best to do. I also have in mind, as you are more aware than I am, that sometimes criminals can get away with more in third world countries than they do here in the US.