



## Be aware of phishing

By CK Wong 2006.05.29

<http://www.ck-wong.ca/Technologies/be%20aware%20of%20phishing%2020060529.pdf>

### Introduction

Phishing is a technique used by the cyberspace con artist to get your personal identity. This begins by getting your email address and then uses the email address to send you a phony email to ask you to sign on. Once they capture your account number and password, they can retrieve your profile and manipulate your account. This article provides a list of watch out for you.

### From the beginning ....

It is always begin with your email address. If you use the Internet, it would be hard not to expose your email address. You should protect your email address carefully. The common method to harvest these email address are either proactively crawling over the cyberspace to capture people's email address or obtain it from someone engaged in this type of business. The less your important email address exposed, the safer you are. For someone who has professional need to use their email address this become much more important.

The following are some of the suggestion to segregate your email address spaces to reduce the exposure.

1. Use a specific email address that you deal with the banks or financial institutes but nothing else. This will lower the probability that your email address is being harvested. This will be your protected email address.
2. Get another email address either from Yahoo or Google or somewhere. This will be your utility email address. This will include register with other web site, put out a on sale message on a news group, etc.
3. In your email program, if it supports rules, separate those emails sent to you using the utility email address from the protected email address.
4. If you receive an email asking you to phone in or visit a web site to validate your account, you should be at high alert. Most of the time, just ignore it. Most financial institutes do not do this.
5. If you need to call or visit the organization call or visit their regular phone number or web address not the one provided in the email.

Please note that the con artist uses the graphics and copy the web page design from the forged web site. There is no difference on the appearance. However, if you view the source, you will see some of the links are pointed to somewhere else other than the forged web site.

## **When not to read the email**

It is dangerous to read some email if your email program support scripting because it could do some damages. It is always preferred to disable the macro or scripting ability in your email program and enable it on case by case scenarios.

The best is not to read it when it comes from someone you do not acquaintance to. Once the email is read, it could release virus. So make sure your email program has the anti-virus scanning ability. If you do not have one, you may want to consider the free AVG anti-virus package from <http://www.grisoft.com/doc/1>.

Good luck.