Yui Kee Computing Ltd.

Newsletter

October 2015

Contents

Fake Citibank Website Taken Down

<web-link for this article>

Citibank (Hong Kong) Limited has warned about a fraudulent webpage http://hkhuaqipm.com/col.jsp?id=101 featuring "Hong Kong Citi Group International Auction 香港花旗國際集團拍賣有限公司" and contained the names "Citi Hong Kong, 香港花旗" as well as the office address and phone number of Citi in Hong Kong. Citi has no relationship with the supposed company or webpage. The page is being investigated by the Police, and the Hong Kong Monetary Authority has been informed.

At the time of writing, the page had been replaced by a site closure notice saying that the Government Network Monitoring Department (政府网监部门) had demanded the closure.

Victims should contact Citi bank at 2860 0333, and report to the Police or contact the Cyber Security and Technology Crime Bureau of the Hong Kong Police Force at 2860 5012.

More Information

- Fraudulent website related to Citibank (Hong Kong) Limited
- Statement on "Hong Kong Citi Group International Auction" company and website

Standard Chartered Phishing Takedown

<web-link for this article>

Standard Chartered Bank (Hong Kong) Limited has warned about a phishing email and linked website that target its customers. The email contains a link labelled S2BWeb.Admin@s2bmail.standardchartered.com which connects to a webpage http://www.standard-charteredssoappl.com/login/index.html. The webserver was not available at the time of writing, but it previously fraudulently purported to be Standard Chartered's "Straight2Bank" portal for business clients.

Victims should contact call the Bank's 24-hour customer service hotline at (852) 2886 8868 (press 2 - 6 - 0), and report to the Police or contact the Cyber Security and Technology Crime Bureau of the Hong Kong Police Force at 2860 5012.

Standard Chartered reminded its customers that it will not request customers' personal information (including user names and passwords) by email. Passwords, such as One-Time passwords, are also never requested by the Bank over the phone. Customers should only log into Standard Chartered Online Banking through the Bank's website www.sc.com/hk , or https://s2b.standardchartered.com for Straight2Bank, and not through hyperlinks embedded in emails or third party websites. They should ensure they are connected to a valid Standard Chartered's website before keying in any confidential personal data.

Standard Chartered did not elaborate on how to check a website is valid, some points to look out for are:

- Don't follow links in emails. Type the address yourself, or use your own bookmark from a previous visit.
- Be aware of the domain name in the address. When typing, look out for miss-spellings and confusing names. In this case, the fraudsters registered standard-charteredssoappl.com so that the bank's name was part of the domain name. Good browsers bold the base domain name to make it easier to recognise when a fraudster is using, for example, www.bigbank.**evilfraudsters.com** is easily recognised as nothing to do with BigBank Ltd.
- Check that you have a secure connection. Browsers display a lock icon to indicate when there is an encrypted connection between the website and your browser, do not enter sensitive data (passwords, personal information) unless the connection is encrypted).
- Check that the certificate for the site was issued to the owner of the site you want to visit, and that the certificate was issued by an Authority you trust. For an Extended Validation certificate, a good browser will show the name of the site owner in green next to the lock icon.
- Remember the normal features of the site you are visiting and double-check if there are any changes. If your bank has been using an Extended Validation certificate, and then, one visit, it only has an ordinary certificate, that is suspicious.

More Information

- Standard Chartered alerts customers of fraudulent w ebsite
- Phishing e-mail related to Standard Chartered Bank (Hong Kong) Limited

Fake Malayan Banking Berhad Website at Two Hong Kong Addresses

<web-link for this article>

Malayan Banking Berhad has warned that a company named "马来亚金融金融投资理财有限公司" or "马来亚金融" ("Malayan Finance") is conducting its Internet finance businesses via two webs sites with the domain names of www.mlyjr.com and www.malaiyajinrong.com and that the sites fraudulently use Malayan Banking Berhad's information.

The websites are both hosted at Hong Kong IP addresses, and were still operational at the time of writing.

Victims should contact Malayan Banking Berhad at (852) 3518 8781 or (852) 3518 8717 and the Cyber Security and Technology Crime Bureau of the Hong Kong Police Force at 2860 5012.

More Information

- Malayan Banking Berhad Clarification Announcement on Certain Websites and their Contents
- Fraudulent website related to Malayan Banking Berhad

HKMA Powerless to Prevent Use of Its Logo for Online Fraud

First published: 31st October 2015

The Hong Kong Monetary Authority (HKMA) first warned about a fraudulent website, http://www.hkicgroup.com/, in February 2015 yet the site remains operational at the time of writing. As reported in our February newsletter, the site claims that the so-called "HKIC Group" is regulated by the HKMA, and displays the HKMA logo, but the HKMA denies the claim and warns that "HKIC Group" is not authorised to operate as a bank in Hong Kong.

Seven months later, we reported on the HKMA warning about a remarkably similar site, http://www.kowloonglobal.com, and noted that the original site was still operational. At that time, neither the Police or HKMA commented because of n ongoing Police investigation. The http://www.kowloonglobal.com site ceased operation sometime between 21 September 2015 and 13 October 2015. The Police confirmed that they had completed their investigation on 13 October 2015.

We asked the HKMA why the http://www.hkicgroup.com/ site was still operational, still displayed the HKMA logo, and whether they had contacted the UK authorities (where the site is hosted) to have the site taken down. The HKMA responded:

> The HKMA does not have a law enforcement role. When fraudulent websites come to our attention, it is our practice to report them to the Police and issue a press release to alert the public to the risk. These press releases are kept on our website for reference. The Police generally do not comment on cases that are subject to investigation.

It is apparent that the HKMA has no means of controlling the misuse of their logo, if the website is hosted overseas. Users need to be aware that anything they see on a website can be easily copied by fraudsters to make fake sites look more convincing, and fake sites can be set up very quickly, often disappearing after only a few hours. This case is remarkable because a fake site that is known about by the relevant authorities continues to operate after seven months, and after the conclusion of a Police investigation.

More Information

- HKMA Warns about so-called "HKIC Group" website
- HKMA Fails Whack-a-mole with Fraudulent Websites

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/