Yui Kee Computing Ltd.

Newsletter

March 2014

Contents

Suspicious Website samstyle.tk Suspended

<web-link for this article>

A website, "www.samstyle.tk" that could be used as a proxy for connecting to bank websites has been shut down. Chong Hing Bank Limited ("CHB") noted that its website could be accessed with the URLs "http://www.samstyle.tk/index.pl/00/http/www.chbank.com/tc/personal/index.shtml" and "http://www.samstyle.tk/index.pl/00/http/www.chbank.com/en/personal/index.shtml" and alerted the Hong Kong Monetary Authority (HKMA) and the Police on 03 March 2014. The HKMA also received a similar report from Fubon Bank (Hong Kong) Limited, about the URL http://www.samstyle.tk/index.pl/00/http/www.fubonbank.com.hk

At the time of writing, the site is inaccessible and DNS and Whois records have been removed. A Google search suggests that the proxy could have been used to access any website, including a YouTube video, so this might have been setup for another purpose, and used for banking sites without the owner's knowledge or permission. However, it would be extremely unwise to connect to a banking website through a proxy, as the proxy could capture the login credentials for misuse. Users are advised to connect to bank, and other sensitive websites, directly by typing in the address in their browser, to use an encrypted connection (https:), to check the SSL certificate and to report suspicious websites or emails.

The Police are investigating, anyone who has used the proxy for sensitive information or financial transactions should contact the bank concerned and any local Police Station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

More Information

Suspicious website: www.samstyle.tk
Suspicious website: www.samstyle.tk
Chong Hing Bank Limited : Aware of Fraudulent Website
Aware of Fraudulent Website

HKMA Warns About Fake Hang Seng Bank Website

<web-link for this article>

The Hong Kong Monetary Authority (HKMA) has warned about a fake Hang Seng Bank webpage, with the address http://hangspb.com/bank.hangseng.com/1/2/personal/private-

banking/private-banking.html. Hang Seng Bank has no connection with the fraudulent webpage, and the Police are investigating.

At the time of writing, the fraudulent webpage has been removed, but the web server is still active, showing a test page. The domain hangspb.com was registered to someone claiming to be "Rob Niz" of West London in August 2013.

Anyone who has entered information or conducted financial transactions on the fake webpage should contact Hang Seng Bank at 2822 0203 and any local Police Station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

More Information

Fraudulent website: http://hangspb.com/bank.hangseng.com/1/2/personal/private-banking/private-banking.html

User Education: Are Banks Helping Customers Stay Secure?

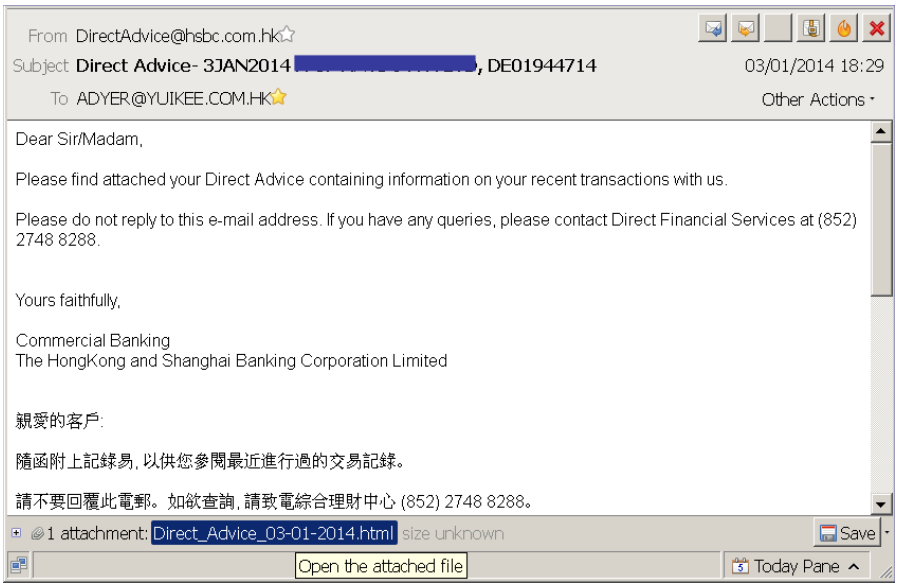
<web-link for this article>

Allan Dyer

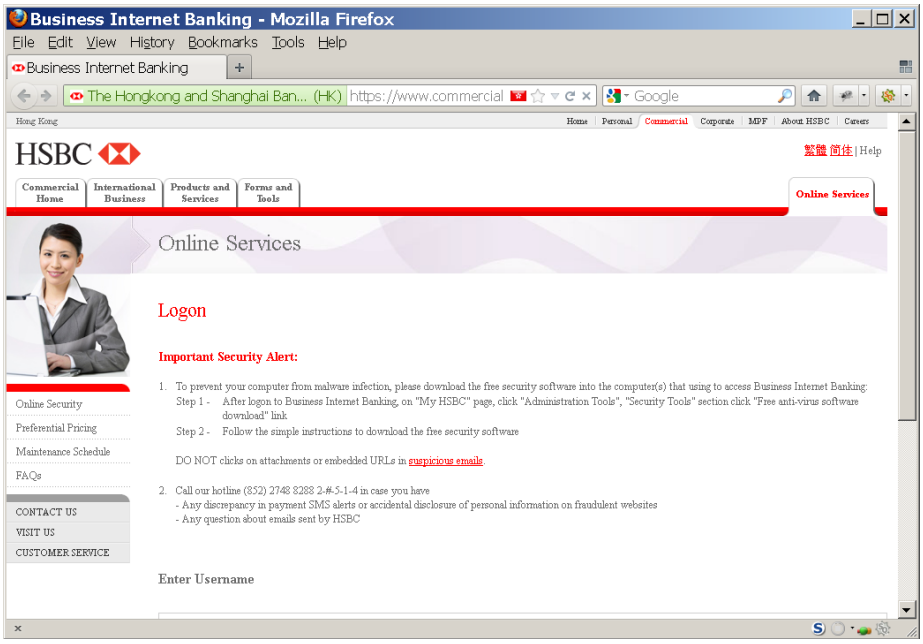
One of the most persistent vulnerabilities in information security is the end user. End users can be socially engineered into taking all sorts of unwise actions; such as selecting weak passwords, revealing sensitive information, or compromising their computers by opening suspicious attachments or following suspicious links. Educating users is a continuing challenge, and to have any chance of success we need to present simple, consistent rules for users to follow.

This makes my recent experience as an end user of online banking services at a major bank somewhat disappointing.

I received an email notifying me about recent transactions for a commercial bank account I manage. The email claimed that the information was in the attached file. Is this suspicious?



Behaving as I would advise a suspicious user to behave, I typed the URL of the bank into my browser and looked for their advice about emails. On the logon page I found the clear instruction:



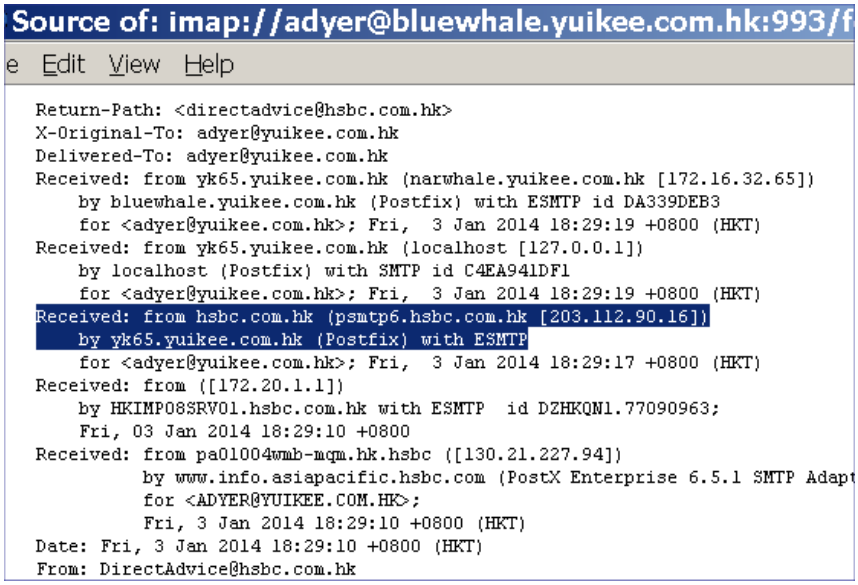
> DO NOT clicks on attachments or embedded URLs in suspicious emails.

Note that my browser has highlighted the name of the bank with a green background, indicating that the website has proved its identity with an Extended Validation SSL certificate.

Then, acting as I would NOT advise a user to behave, I opened the attachment. It showed a webpage with the title "Secure Envelope" asking for my password. There is no indication to the end user why this is a Secure Envelope, or any assurance that it came from a trusted source.

I decided to report the email to the bank, so I called the hotline number on my bankcard (no point in calling the number listed in the email, that might be answered by a fraudulent sender). When I explained about the email, the hotline staff told me that:

- An email with a link is not from this bank, please delete it
- The bank sends eStatements from the address commercial.estatement.and.eadvice@hsbc.com.hk



However, I had also examined the email headers. Almost everything in an email message can be easily forged, but the Received: header lines are added by each server the message passes through, so, by looking at the Received: header added by your gateway mailserver, you can identify the address of the computer that sent the message with a good degree of assurance. The relevant Received: header of this message (highlighted in the image) shows an address of the bank. Therefore, either the message was genuine (and everything the hotline staff had told me was untrue), or the bank had a major security incident and criminals were using bank systems to send unauthorised messages.

In a follow-up email, I provided a copy of the suspicious message and asked the questions:

1. Are these "Direct Advice" messages genuinely sent by the bank?
2. If they are, why do they promote the risky practice of entering a password into an unverified email attachment?
3. How will you be improving your advice to customers and your interactions with customers?

The bank replied in a phone call, confirming that the message was genuine. They also clarified that the password to access the Direct Advice was not the eBanking password, but a distinct PIN just for this purpose. Finally, they could give me no feedback from the related department, because they don't talk to customers directly.

To be clear, being notified when there is an incoming payment is a service I find useful. However, when I selected that service on the bank website, I did not expect the notification to be delivered in a manner that the security advice on the same website and from the hotline staff said was suspicious. Unauthorised access to a payment notification does not sound particularly dangerous, but a criminal could craft a similar notification that asked the user to install a new [fake] security certificate, thus compromising all future communication with the bank.

Successful user education depends on supplying users with simple, consistent rules they can use. The bank here has failed and is therefore putting their customers at risk.

HKMA Warns of Unauthorised Bank Websites

<web-link for this article>

The Hong Kong Monetary Authority (HKMA) has issued a warning about suspected fraudulent websites with the domain names "www.fleetnationalbk.com" and "www.fleethknational.com" and claimed to be run by "Fleet National Bank, Hong Kong". The HKMA has clarified that "Fleet National Bank, Hong Kong" is not authorized under the Banking Ordinance to carry on banking business or the business of taking deposits in Hong Kong, and does it have the approval to establish a local representative office.

The Police are investigating, and anyone who has used the sites should contact any local Police Station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

The two websites are hosted in Germany and the USA, and have very different designs and features, suggesting that they are run by two separate fraudsters. There was a Fleet National Bank in the USA, that was taken over by the Bank of America in 1995, some branches may still be trading under the old name and the fraudsters might be attempting to use a name familiar to their targets for phishing attacks.

A list of authorized institutions is available on the HKMA's website (www.hkma.gov.hk) and can also be checked by callin the HKMA public enquiry hotline 2878 8222.

HKMA Warns of Fraudulent Webpage on Belt Manufacturer Website

<web-link for this article>

The Hong Kong Monetary Authority (HKMA) has issued a warning about a webpage on the website of a Hong Kong-based manufacturer. They reported that the webpage at http://www.fmetal.hk/Backup/ redirected visitors to an official BNP Paribas website, but, at the time of writing, the webpage had been replaced with a hasty copy of the manufacturer's home page.

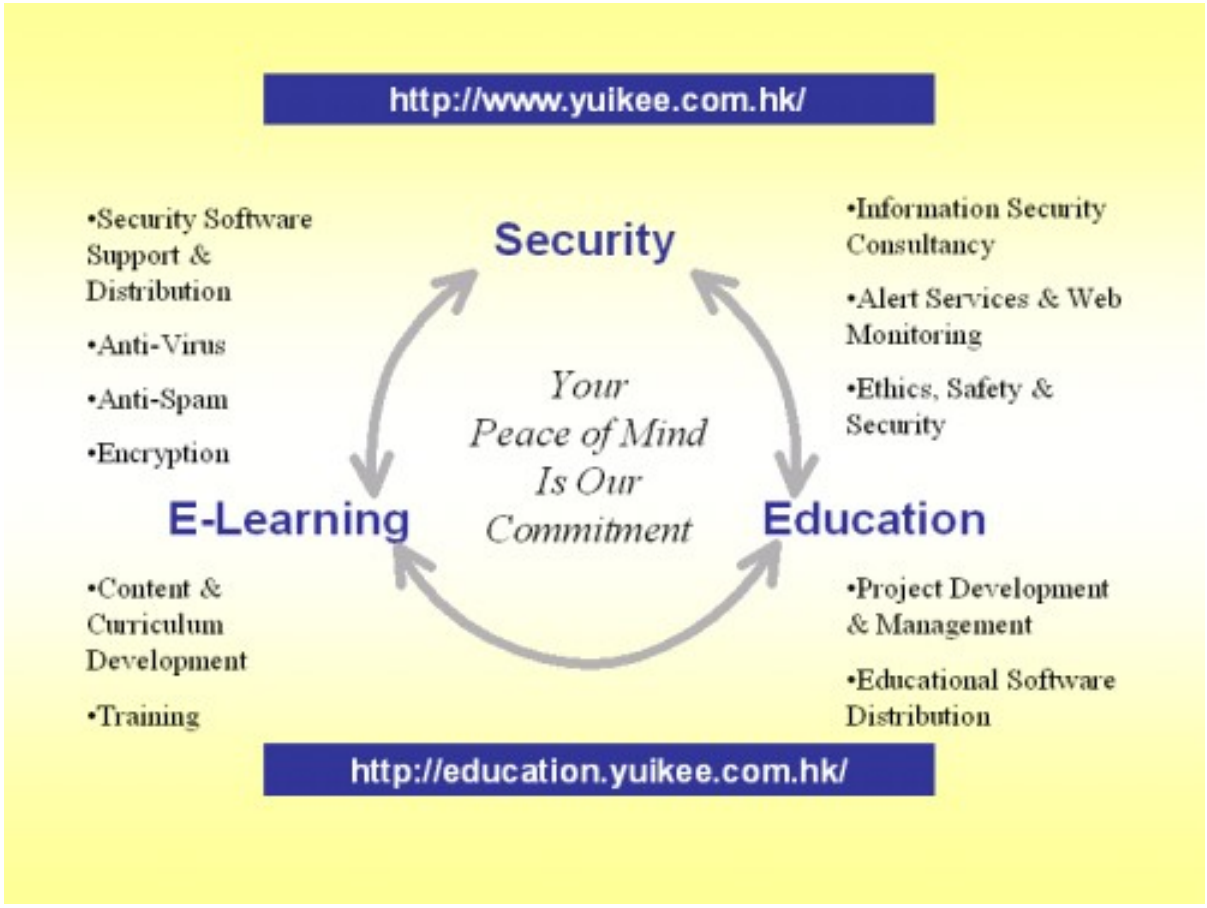
If you have provided personal information to the site, or conducted any financial transaction through it, please contact BNP Paribas at 2825 1116 and any local Police Station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

More Information

Fraudulent website: http://www.fmetal.hk/Backup/

YUI KEE 銳基電腦顧問有限公司 Anti-Virus, Network Security & Education

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/


http://www.yuikee.com.hk/
Security
•Security Software Support & Distribution
•Anti-Virus
•Anti-Spam
•Encryption
•Information Security Consultancy
•Alert Services & Web Monitoring
•Ethics, Safety & Security
Your Peace of Mind Is Our Commitment
E-Learning
Education
•Content & Curriculum Development
•Training
•Project Development & Management
•Educational Software Distribution
http://education.yuikee.com.hk/