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

Yui Kee Computing Ltd.

Newsletter

November 2015

Contents

Chong Hing Bank Detects a Fraudulent Website

<web-link for this article>

Chong Hing Bank Limited ("CHB") has issued a warning about a fraudulent website “http://chbnkgrp.com/en/” that imitated the CHB website. CHB has no connection with the fraudulent website and the Police are investigating.

Victims should contact CHB Customer Services Hotline at (852) 3768 6888 and any local police station or the Cyber Security and Technology Crime Bureau of the Hong Kong Police Force at (852) 2860 5012.

CHB reminded its customers to ensure they are connected to a valid CHB website when they want to access CHB internet banking services. The website address is www.chbank.com and CHB's banking security advice is here.

More Information

- Chong Hing Bank Detects a Fraudulent Website
- Fraudulent website related to Chong Hing Bank Limited
- Internet Banking and Mobile Banking Security

AVAR 2015 Conference Preview

<web-link for this article>

The Association of Anti-virus Asia Researchers (AVAR) will hold their 18th conference on 2nd - 4th December, in Danang, Vietnam. The AVAR Conference has been held around the region, from Korea to Australia to India, but this will be the first time in Vietnam.

Many of the leading anti-virus researchers from around the world will be attending and speaking. The keynote speakers are Mikko Hyppönen, Dennis Batchelder and Righard Zwienenberg. Hyppönen will explain the only two problems to solve to secure our online future: Privacy and Security. Batchelder is the Director of Research for the Microsoft Malware Protection Center (MMPC). Zwienenberg will be discussing how cooperation between competing anti-virus companies has shaped the industry and how that cooperation should develop.

The speeches cover a broad range of technical areas, from Android (Igor Muttik and Jorge Blasco, Jan Sirmer and Ondrej David, Siegfried Rasthofer and Carlos Castillo), keyloggers (Pablo Atilio Ramos and Diego Perez Magallanes), Cloud (Philipp Wolf and Matthias Ollig, Siegfried Rasthofer and Carlos Castillo), Internet of Things and embedded devices (Maik Morgenstern, Peter Kálnai and Jaromír Hořejší), Ransomware (Samir Mody and Gregory Panakkal), Advanced Persistent Threats (Kalpesh Mantri and Yogesh Khedkar, Razor Huang, Ivan Macalintal & Hai-Tri C. Le) to Windows (Benjamin S. Rivera and RonJay Kristoffer R. Caragay, Vlad Craciun and Cristina Vatamanu).

More social issues are also covered. Juan Andres Guerrero-Saade will show the perils of Intelligence Brokerage, Hong Jia and Feiran Liu willo expose the Threat Intelligence behind “XcodeGhost”, Liu Zhao will report on new Social Engineering tricks, and Jean-Ian Boutin will explain the vulnerabilities of Russian accountants.

There will be a Gala Dinner on the first evening, and the AVAR Annual General Meeting will take place immediately after the close of the conference.

More Information

- Association of Anti-virus Asia Researchers International Conference 2015

Hong Kong Introduces Electronic Cheques

<web-link for this article>

From 7th December 2015, nine banks in Hong Kong will offer Electronic Cheque (e-Cheque) services. The launch has been organised by the Hong Kong Monetary Authority (HKMA) and the Hong Kong Association of Banks (HKAB), and the participating banks are Agricultural Bank of China, Bank of China (Hong Kong), Chiyu Banking Corporation, Fubon Bank (Hong Kong), Hang Seng Bank, Nanyang Commercial Bank, The Bank of East Asia, The Hongkong and Shanghai Banking Corporation and Wing Lung Bank.

The e-Cheque service allows traditional cheque writing and deposit to be replaced by entirely online procedures. The e-Cheques are governed by the Bills of Exchange Ordinance have the same legal status as paper cheques. Once the service is rolled out, customers of the nine participating banks will be able to issue e-Cheques using their internet or mobile banking account. All Hong Kong banks will be able to accept deposits of e-Cheques, either through their internet or mobile banking service or the e-Cheque Drop Box service provided by the Hong Kong Interbank Clearing Limited. Hong Kong Dollar, US Dollar and Renminbi e-Cheques will be available.

The e-Cheque itself is a PDF file with the digital signature, backed by PKI, of the issuing bank. The Payer is required to authenticate using two factor authentication (2FA) when issuing e-Cheques. e-Cheques will be non-transferable, and cannot be made out to Cash.

All e-Cheques, whether submitted via the payee's online account or directly, are presented via the Hong Kong Interbank Clearing Limited so multiple presentment is prevented. Clearing is same-day for e-Cheques presented before 17:30.

The security of e-Cheques appears to be at least as good as paper cheques. Like paper cheques and unlike online banking transfers, the Payee does not have to reveal their account details to the Payer. The HKMA brochure promoting e-Cheques also claims, "The payer may consider encrypting an e-Cheque before delivery to further improve security", without specify the encryption procedure or security benefit. The obvious procedure would be to encrypt the e-Cheque PDF file using the Payee's public key, so that a third party intercepting the message would not be able to attempt to present the e-Cheque themselves, or see any details on the e-Cheque.

The HKMA borchure also incorrectly claims, "It can be issued anytime anywhere". As the Payer must connect to their bank to issue the e-Cheque, a working internet connection is required, and the banks servers must be operational.

More Information

- Launch of Electronic Cheque (e-Cheque) publicity campaign
- HKMA e-Cheque Brochure
- Text-only HKMA e-Cheque Brochure
- Legislative Council Brief Electronic Transactions Ordinance (Amendment of Schedule 1) Order 2014

Bank of China Fake Website Redirection

<web-link for this article>

The Bank of China (Hong Kong) Limited (BOCHK) has warned that the domain www.bankofchinagroup.com redirects to the genuine BOCHK website (http://www.bochk.com/) without authorisation. The case has been reported to the Hong Kong Monetary Authority and the Hong Kong Police. Victims should contact the BOCHK at 3988 2388, and report to the Police or contact the Cyber Security and Technology Crime Bureau of the Hong Kong Police Force at 2860 5012.

This is not the first time that a fake BOCHK domain has been redirected to the genuine BOCHK site. In August 2015, this newsletter reported redirection of www.bochkgroup.com. The HKMA reported that www.bochkgroup.com was "a fraudulent website".

The purpose of redirecting a copycat domain name to the genuine site is not clear. If the intent is fraudulent, some possibilities are:

- Reconnaissance: The browser of a victim that uses the link makes an ordinary request to the fake domain, and the site responds with a 302 redirect error. However, the ordinary request includes information about the browser, operating system, IP address (and therefore general location) of the victim.
- Making a fake site more realistic: Fake sites often copy many pages from the genuine site, so that a browsing victim finds the site convincing. Redirection could be used so that, for one page (e.g. the banking login page) the user remains on the fake site and all other requests are redirected to the equivalent page on the genuine site. This appears not to be the situation in this case, because the redirection does not preserve the relative location on the site.
- Selective Targeting: The fake site may redirect most users to the genuine site, but retain those judged most suitable to be fraud victims, perhaps selected by time, location or other information.

More Information

- Fraudulent website related to Bank of China (Hong Kong) Limited
- Alert on an unauthorised website
- HKMA Warns of Fake BOC Webpage

VTech Data Breach Exposes Personal Data of Hundreds of Thousands of Children

<web-link for this article>

Hong Kong electronic toymaker VTech has admitted that an unauthorized party accessed VTech customer data housed on their Learning Lodge app store database on November 14, 2015. Learning Lodge allows VTech's customers to download apps, learning games, e-books and other educational content to their VTech products. The data breach includes the first name, gender and birthday of about 227,000 children and names, email addresses, passwords, and home addresses of 4,833,678 parents. The children's records can be linked to their parents, so effectively the full identity and home address of the children is exposed.

The "unauthorized party" responsible for the November 14 breach apparently contacted tech journalist Lorenzo Franceschi-Bicchierai of Motherboard who asked the creator of Have I been pwned? and web security blogger Troy Hunt to verify the data breach. Lorenzo also contacted VTech, but did not get a reply until days afterwards, on November 27. VTech released a press release on the data breach the same day.

When asked what the plan for the data was, the hacker responded "nothing" and claims to have only provided the data to Motherboard. If this is true, then the hacker is a whistleblower that has revealed VTech's negligent data protection.

Unfortunately, other attackers might have accessed the VTech data the same way. The hacker revealed that they gained access to the database using a SQL injection attack (SQLi). Such attacks have been common knowledge for a decade, and are easy to implement. There is even a a cartoon about SQL injection.

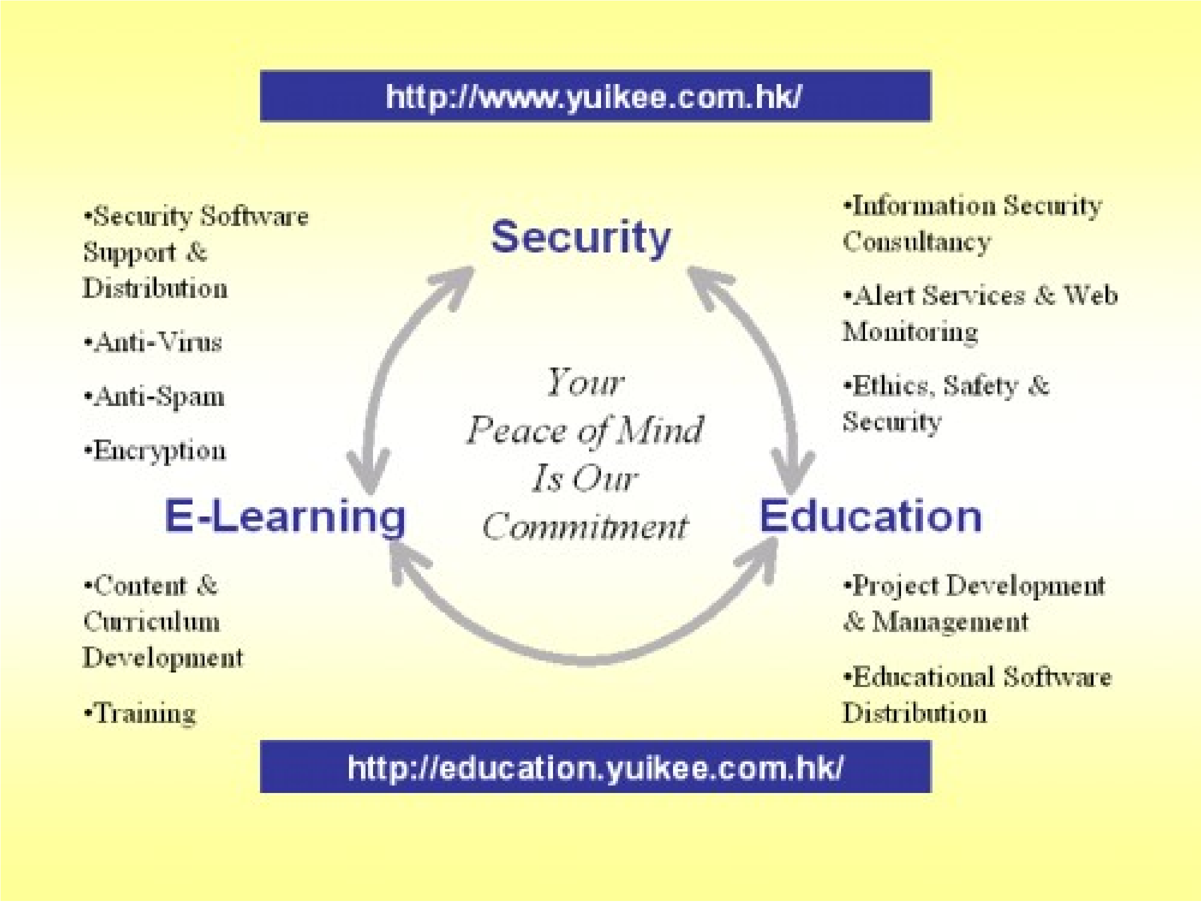
VTech has emailed its Learning Lodge customers concerning the breach. In the email, VTech emphasises that credit card, banking information, identity card numbers, social security numbers, and driving license numbers were not in the database. The potential for misuse of the data that has been revealed, however, is still enormous.

More Information

- Millions of families hit in toymaker VTech hack – including 200,000+ kids
- VTech Statement: Data Breach on VTech Learning Lodge
- When children are breached – inside the massive VTech hack
- One of the Largest Hacks Yet Exposes Data on Hundreds of Thousands of Kids
- Lorenzo Franceschi-Bicchierai
- About Motherboard
- Have i been pwned?
- xkcd: Exploits of a Mom

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

- Content & Curriculum Development
- Training

Education

- Project Development & Management
- Educational Software Distribution

http://education.yuikee.com.hk/