Yui Kee Computing Ltd.

Newsletter

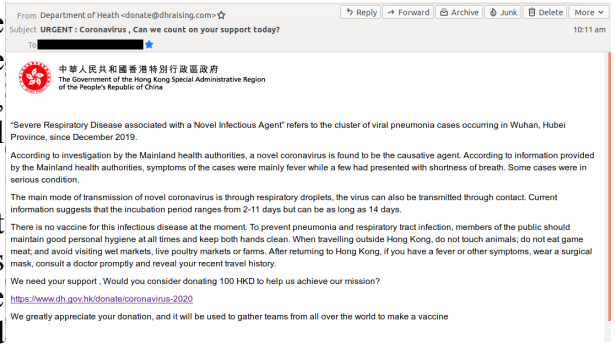
February 2020

Contents

Coronavirus Phishing

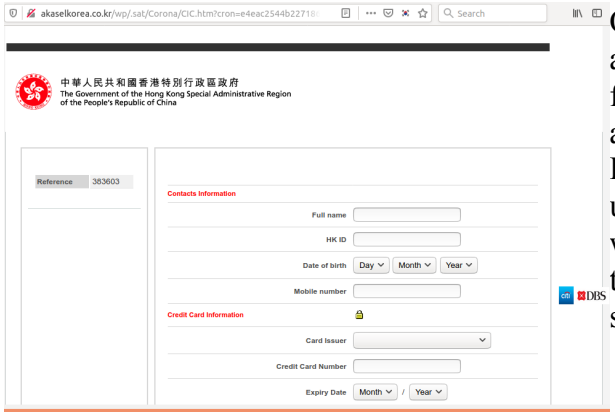
<web-link for this article>

Don't let a health crisis become a cybercrime crisis too. A fraudulent email, purporting to be sent by the Hong Kong Department of Health, has been received by a number of .hk email addresses.



Fake Department of Health Email

The message briefly describes the current novel coronavirus outbreak, and then solicits donations "to gather teams from all over the world to make a vaccine", with a link labelled https://www.dh.gov.hk/donate/coronavirus-2020 but actually going to http://akaselkorea.co.kr/wp/.sat/Corona/ . That webpage has a form, with HK Government-branding, to collect credit card information and other sensitive personal data. The page is hosted on an insecure website of a Korean Metallography supplies company.

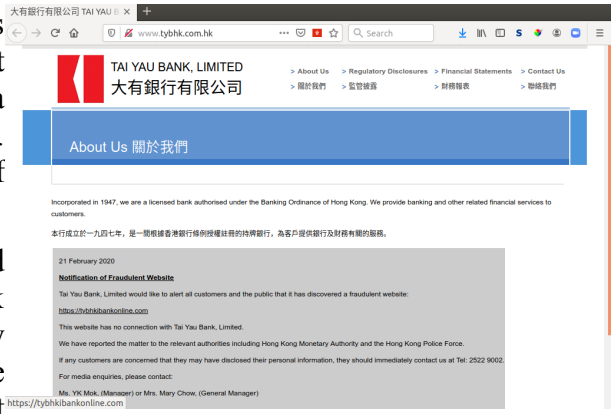


Fraudulent donation webpage

Obviously, it would be very unwise to enter any credit card or personal information on the fraudulent page. Users should remain vigilant about online threats, even during this Global Health Emergency. Be suspicious of unsolicited emails, check the sender's details, watch for discrepancies between links and their labels, verify information with trusted sources.

Don't Go To This Site (Link Provided)

<web-link for this article>



Tai Yau Bank warning page, with live link to malicious site

In a questionable move, Tai Yau Bank has published an active link to a fraudulent website on their website, contained in a warning about the fraudulent website. Fortunately, the site was blocked at the time of checking.

The warning was dated 21 February 2020 and posted on the home page of the bank (screenshot). The Hong Kong Monetary Authority issued a press release about the fraudulent website on 25 February 2020. Most organisations issuing warnings about fraudulent or dangerous websites present the URL without making it an active link, some take the extra step of replacing the scheme (http or https for a website) with an invalid variant, usually hxxp or hxxps. This prevents unwary users accidentally clicking on the link, and using an invalid variant avoids the problem of "helpful" software automatically making the plain-text an active link simply because it matches the pattern of a URL.

The fraudulent domain (tybhkibankonline.com) was registered in October 2019 at a Russian registrar in the name of an American company with an invalid Russian address, and an invalid contact email address.

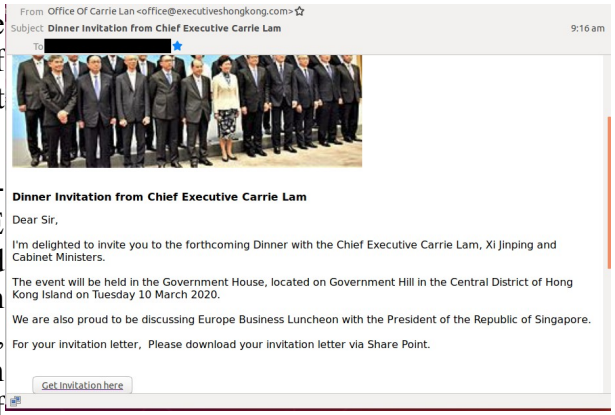
Victims should contact Tai Yau Bank at 2522 9002 and the Cyber Security and Technology Crime Bureau of the Hong Kong Police Force at 2860 5012.

More Information

- Fraudulent website related to Tai Yau Bank, Limited
- Tai Yau Bank, Limited
- The "hxxp" and "hxxps" URI Schemes

Phishing for Chief Executive Fans

<web-link for this article>



Phishing email tagetting high-status CE contacts

A number of Hong Kong email addresses have received an invitation, supposedly from Chief Executive Carrie Lam (CE) to a dinner at Government House.

It apparently targets people who are high-status or arrogant enough to believe the CE would choose them to meet with herself and President Xi Jinping, and obsequious enough to overlook the errors in the message. Notably, the Chief Executive's name is misspelled in her email address, and the address of Government House is not on Government Hill. There is also the expectation that the recipient would be so eager to be there, they would choose to eat and socialise in a crowd during an infectious disease outbreak.

The link to "Get Invitation here" leads to a website attempting to imitate a Microsoft Sharepoint login. presumably with the objective of harvesting high-value login credentials.

Users should be suspicious of unexpected emails; and do not follow links in unverified messages.

An open question is how the attackers chose the target list. General phishing campaigns use topics that are attractive and believable to many, and are sent indiscriminately. However, the topic here is narrowly targetted at people who believe they might be invited to dine with the CE, this makes it far more likely to be a spear phishing campaign. They are normally sent to a list that is highly relevant. Does this indicate that a list of the CE's email contacts has been leaked or stolen?

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/