Yui Kee Computing Ltd.

Newsletter

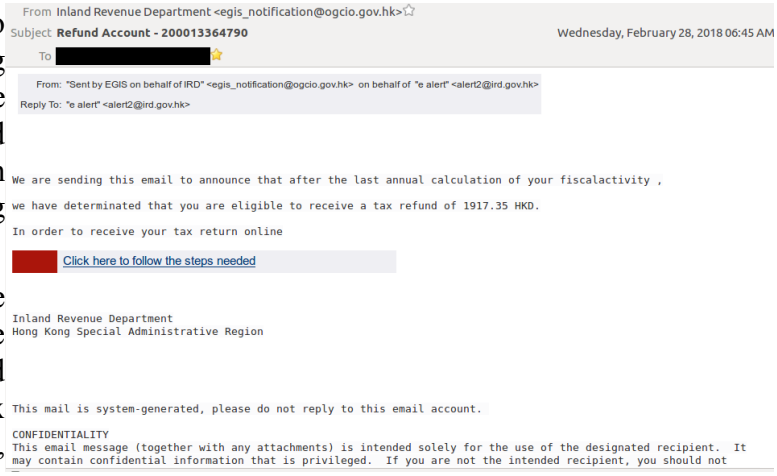
March 2018

Contents

Hong Kong Taxpayers Targeted with Fake Refund Phishing Email

<web-link for this article>

A fake tax refund email linking to a website imitating the Hong Kong Inland Revenue Department (IRD) style and requesting personal data has been received by a number of Hong Kong recipients.


From Inland Revenue Department <egis_notification@ogcio.gov.hk>
Subject Refund Account - 200013364790
Wednesday, February 28, 2018 06:45 AM
To [redacted]
From: "Sent by EGIS on behalf of IRD" <egis_notification@ogcio.gov.hk> on behalf of "e alert" <alert2@ird.gov.hk>
Reply To: "e alert" <alert2@ird.gov.hk>

We are sending this email to announce that after the last annual calculation of your fiscalactivity ,
we have determinated that you are eligible to receive a tax refund of 1917.35 HKD.
In order to receive your tax return online
Click here to follow the steps needed

Inland Revenue Department
Hong Kong Special Administrative Region

This mail is system-generated, please do not reply to this email account.

CONFIDENTIALITY
This email message (together with any attachments) is intended solely for the use of the designated recipient. It may contain confidential information that is privileged. If you are not the intended recipient, you should not

Illustration 1: Fake email announcing tax refund

The message informed the recipient that they were eligible to receive a tax refund and should follow a link to receive the tax return*[sic]* online. The webpage, hosted on a Korean shopping mall website and still accessible at the time of writing, uses the Inland Revenue Department logo and style, and asks for personal and credit card information, including the CVV number. This could be used to make fraudulent charges against victims' credit cards.

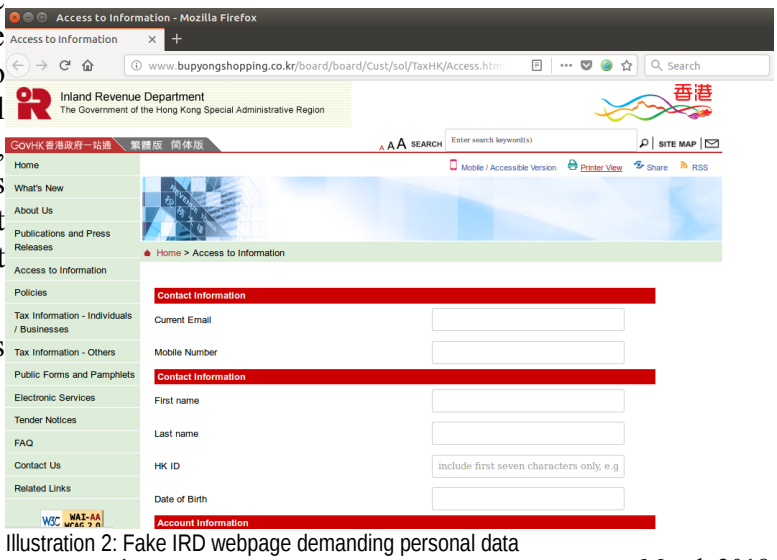


Illustration 2: Fake IRD webpage demanding personal data

There are many clues that this is a fraudulent message:

- Tax authorities do not often make unrequested refunds to taxpayers. This alone should make most recipients suspicious.
- Various text errors in the email: 'fiscalactivity' should be two words, using 'tax return' instead of 'tax refund'.
- The email From address is egis_notification@ogcio.gov.hk, but the has its own domain, ird.gov.hk, and routinely uses it for sending messages.

More technical recipients might note further clues:

- The message was sent from 32063.hostserv.eu [185.178.192.43], a server in Switzerland.
- The link points to http://primobaciobaci.co.kr//wordpress/wp-content/plugins/hello2.php, which is not a Hong Kong Government website.
- The link redirects to http://www.bupyongshopping.co.kr/board/board/Cust/sol/TaxHK/Access.html, an apparently unauthorised page on the aforementioned Korean shopping mall site.
- Other pages on the Korean shopping mall site also show distinct signs of unauthorised activity. The page http://www.bupyongshopping.co.kr/board/board/ contains a hacker pseudonym and an obscenity directed at Korea.

Could the Hong Kong Government do more to block similar fraudulent emails?

The message was sent with the envelope From of www-data@ogcio.gov.hk, from the host 32063.hostserv.eu [185.178.192.43]. The Government has published SPF records for OGCIO:

```
ogcio.gov.hk    text = "spf2.0/pra include:spf-2.im.cis.gov.hk include:spf-
2.egis.gov.hk include:spf-2.ogcio.gov.hk include:sentry-eds.com ~all"
ogcio.gov.hk    text = "v=spf1 include:spf-1.im.cis.gov.hk include:spf-
1.egis.gov.hk include:spf-1.ogcio.gov.hk include:sentry-eds.com ~all"
```

And IRD:

```
ird.gov.hk      text = "spf2.0/pra include:spf-2.im.cis.gov.hk include:spf-
2.egis.gov.hk ~all"
ird.gov.hk      text = "v=spf1 include:spf-1.im.cis.gov.hk include:spf-
1.egis.gov.hk ~all"
```

These records clearly specify which servers are permitted to send email for those departments, and they do not include the server the fraudulent message was sent from. Therefore, receiving email servers can check the SPF record and decide to reject the connection.

However, the Government has chosen to specify '~all' in the SPF records. This is a policy recommendation for the recipients of softfail: i.e. to allow mail whether or not it matches the parameters in the record. A softfail policy is usually implemented for a transitional period, while an organisation is still working on ensuring all its email users are following its policy.

Perhaps it is time for the Hong Kong Government to change its SPF policy to '-all', a hard fail.

More Information

- Fraudulent email purportedly issued by Inland Revenue Department

Will eID Suceed Where e-Cert Failed?

<web-link for this article>

The Hong Kong Government released a Legislative Council Panel on Information Technology and Broadcasting discussion paper on 12 March 2018 about its plans for introducing an eID for all residents as key infrastructure in its "Smart City" plans.

The eID project was first announced in the Chief Executive's 2017 Policy Address, which said that it will be provided to all Hong Kong residents and will allow them to use a single digital identity and authentication to conduct government and commercial transactions online. In November 2017, the Secretary for Innovation and Technology, Mr Nicholas W Yang gave a written answer to Hon Charles Mok, revealed that the system would be launched by 2020 and adding the detail that eID will be used in a virtual form on mobile applications or other Internet platforms, and will not use smart ID cards as carrier to eliminate the limitation of using card readers and computers.

The discussion paper says that the eID would be made available for free for all Hong Kong residents to apply and use on voluntary basis. It will support digital signing with legal backing under the Electronic Transactions Ordinance (Cap. 553). The long-term goal is to make it mandatory for all government departments and public bodies to support the use of eID. The Government intends to actively promote public and private organisations to adopt eID and they will make technical provision to open up APIs. They will adopt security standards that are widely recognised internationally to ensure that the eID system is secure and reliable, consult the Privacy Commissioner and make provision for future technology.

The registration and use of eID could be provided through mobile applications and other Internet platforms. A year after launching the eID system, there will be a review of the Hong Kong Post Certification Authority, including the feasibility of providing all digital certificates by the private sector.

Development of Electronic Transactions in Hong Kong

The Electronic Transactions Ordinance (ETO) was enacted in Hong Kong on 5 January 2000 and came into force in April 2000. Hongkong Post created a public key infrastructure (PKI) and established the first public Certification Authority (CA) in Hong Kong on 31 January 2000. However, few people started using it.

In 2002, after 2 years, the Government launched a review of the ETO, with a public consultation. One of the proposals in the public consultation was to consider whether legal recognition should be extended to cover other forms of electronic signatures, in addition to digital signatures, in order to stimulate e-business development. In the ETO, an electronic signature is any symbols adopted for the purpose of authenticating or approving an electronic record, and a digital signature is a subset of electronic signature that uses an asymmetric cryptosystem and a hash function. The proposal was criticised as being a step backwards because digital signatures offer a high level of integrity, authentication and non-repudiation that other current technologies cannot match. It was predicted that recognition of other types of electronic signature would merely reduce the security and fragment the market, with a negative effect on e-business development.

Nevertheless, in 2003 the Government amended the ETO to allow a 6-digit password to be used as an electronic signature for submitting tax returns.

Using e-Cert

Early adopters always encounter difficulties. A minor difficulty was that, initially, the Hongkong Post Certificate Authority was not recognised as a trusted root CA by major

browsers, including Internet Explorer. This was gradually improved, but is was not until 2010 that Mozilla included Hongkong Post's root certificate in the Firefox browser.

Another issue was that applications did not use the certificate in the same way. The process for signing a tax return was entirely different to the process for signing the application to have a library card added to a Smart ID card. The explanation was that the two applications have different security requirements, but this misses the needs of the user: a familiar process that they can understand. It is not necessary to learn a new method of handwriting one's signature when using the paper-based equivalents.

More serious were the compatibility problems. At one point, the Hongkong Post e-Cert management application required a different version of the Java Runtime Environment (JRE) to the Inland Revenue's e-Tax application. The applications only supported specific browser versions, and they were often not the most recent ones.

The Government's applications failed to keep up with evolving internet standards. Although Java looked like a good cross-platform choice in 2000, in 2015 Google and Mozilla announced their plans to remove support for NPAPI plugins that are required to run JAVA Applets in the web browser. Microsoft introduced their new browser, Edge, without JAVA support. However, at the time of writing, the GovHK software requirements for services requiring a digital certificate still include JRE, restricting browser choice to Safari and the obsolete Internet Explorer.

eID Strengths and Weaknesses

To be successful, eID has to build on the strengths of e-Cert, while avoiding its problems. The discussion paper has some positive indications:

- Based on Digital Signatures. The paper does not explicitly state this, the closest is in paragraph 7, "eID will support digital signing with legal backing under the Electronic Transactions Ordinance (Cap. 553)". Hopefully, "digital signing" means securing with a digital signature, because digital signatures have important advantages not shared by other forms of electronic signature.
- Free. Although the e-Cert annual fee is only HK$50 per annum, it is a disincentive when the expected usage is an annual tax return.
- API. Providing a well-documented API is important for getting third-party applications using the eID.
- Active Promotion. The intention to encourage usage is positive.

On the negative side:

- Compatibility. It needs to 'just work'. e-Cert has shown that even enthusiastic early-adopters become discouraged when there are recurring compatibility problems. The system must use open standards so that users are not excluded by their choice of computing environment, and must look forwards to technology developments (like the announced abandonment of browser JAVA support).
- Entrenched solutions. Active promotion may no longer be enough to bring major online services onboard. Banks, shops and payment services have all developed their own, fragmented, authentication solutions and they have little reason to adopt eID in addition. Perhaps the HKMA can make accepting eID mandatory for all HK banks.
- Poorly thought-through security implications. The proposal includes the suggestion, "the registration and use of eID could be provided through mobile applications and other Internet platforms". While using eID in a mobile app will be essential, registration is another matter. Registration is the point at which the identity of the user is verified and bound to the digital certificate, so how is the user's identity going to be established with any degree of certainty by a mobile app? This concern is also linked

to another suggestion, that there will be a, "review of the services and operating arrangements of the Hongkong Post Certification Authority, including the feasibility of providing all digital certificates by the private sector". The use of Post Offices for issuing e-Certs was one of the strengths of the system. The registration was conducted face-to-face by trusted public servants that were already vetted and trained in verifying people's identity for other purposes, and the process could take place at offices in every district. The private sector can provide the benefit of the free market when the participants bear the costs of failures, but the cost of a failure in registration is paid by the third parties who are identity theft victims or that rely on the falsely-issued certificate.

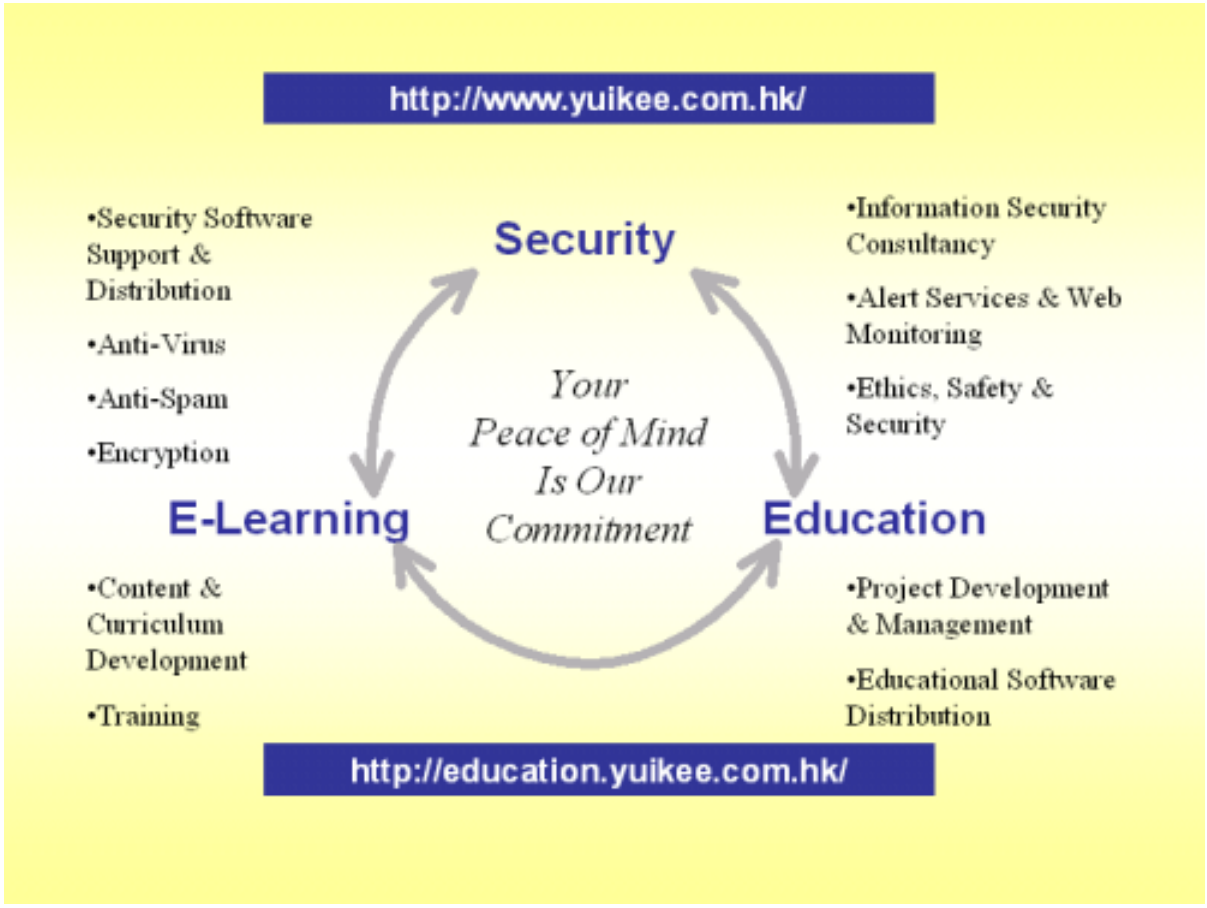
Hopefully, the eID project will correct the mistakes of the last 18 years.

More Information

- Legislative Council Panel on Information Technology and Broadcasting Key Infrastructure Projects f or Smart City Development
- LCQ14: Provision of an electronic identity for Hong Kong residents
- Electronic Authentication & Digital Certificates
- HK eID to support private services
- The Smart City Blueprint for Hong Kong
- 10 questions about Hong Kong's new smart identity card answered
- UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001
- System Requirements for GovHK Online Services
- Smart city plan unveiled
- Hongkong Post and HP Collaborate to Drive Adoption of Free e-Cert on Smart ID Card
- Hongkong Post Certification Authority's root certificate included in Mozilla Firefox web browser
- Accessing Hong Kong Government Services using a Hongkong Post eCert from Firefox on Ubuntu Linux
- e-Cert File USB
- The Hongkong Post eCert and the State of Digital Signatures in Hong Kong
- Hongkong Post e-Cert Subscribers Told Certificates Expired
- Review of the Electronic Transactions Ordinance
- Authentication Pitfalls

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/