Yui Kee Computing Ltd.

Newsletter

October 2018

Contents

Hong Kong Police Hosts Cyber Security Consortium 2018

<web-link for this article>

Cyber Security Consortium 2018 included a 2-day conference on 23 and 24 October, and a law-enforcement-only session on 25 October. Organised by the Hong Kong Police, the forum was attended by law-enforcement officers from the Mainland, Macau and 17 overseas countries as well as cyber security experts and industry leaders from around the world.

The event provided a platform for participants to share their latest knowledge of cyber security and the best practices to protect critical infrastructure and in incident response.

In his welcoming remarks, Acting Commissioner of Police Lau Yip-shing said that collaboration, strategy, and continuous training and research are crucial in the face of increasing cyber security threats. He added that he hopes participants could gain up-to-date knowledge on cyber security, and strengthen collaboration to cope with the cyber security challenges ahead through the sharing at the consortium.

Under Secretary for Innovation & Technology David Chung said new cyber security threats and technology crimes have emerged quickly with the rapid development of technology. He added, “It is therefore important for all of us to take a holistic and proactive approach to protect our digital economy and assets while maintaining an innovative culture and a vibrant society". He noted the Government has been strengthening collaboration with stakeholders to improve the cyber resilience of Hong Kong.

Speakers brought insights from commercial security companies, including Kaspersky Lab, Symantec and Trend Micro, Government organisations, like the Hong Kong Monetary Authority, Banks, foreign law enforcement, including the FBI, NCA, Dutch National High Tech Crime Unit and INTERPOL, APNIC, HKCERT and others from across the world.

More Information

- Cyber security forum opens
- Hong Kong Police Force Cyber Security Consortium

Privacy: Who Cares? A Quick Look at the BOC Smart Bracelet

<web-link for this article>

Would you give access to all your emails in order to track your fitness? I was recently passed a "BOC Life" branded Smart Bracelet, but I was shocked by the User Agreement of the required App.

The Smart Bracelet was apparently given to BOC Life customers as a sign-up gift, I was given it by a friend who declined to be identified. The Smart Bracelet needs to be paired with a smartphone and an App, called "Veryfit 2.0" must be installed. I downloaded Veryfit 2.0 from the Google Play Store, it is also available for the iPhone, and via a QR code printed on the box.

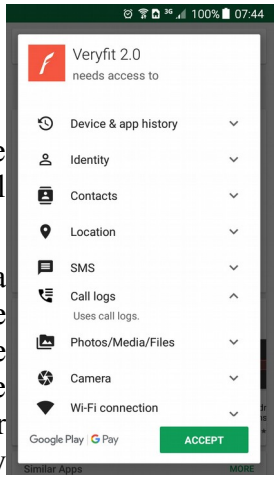
The BOC Life Smart Bracelet in its box

Rear of Smart Bracelet box, listing the device functionality and the App QR code

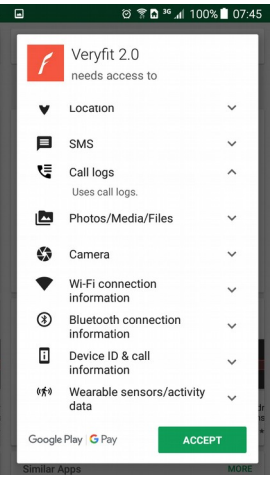
On installation, it asks for a long list of permissions (see screenshots). Some appear necessary for the declared functions of the device (Camera for the remote camera function, location and sensor data for the fitness function), but others are excessive:

- Contacts
- Call logs
- Photos/Media/Files

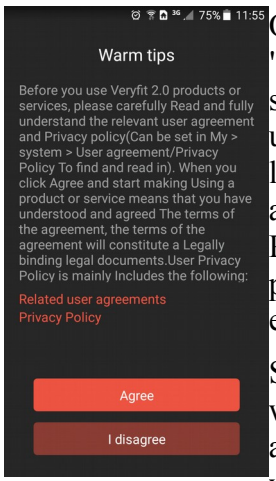
To be clear, the App is asking to access all the details of your friends, when you called them and all of the files that are held on your phone!



Veryfit 2.0 required permissions



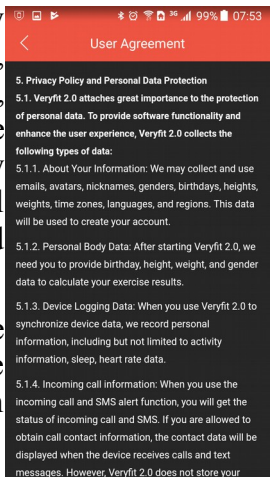
More Veryfit 2.0 required permissions



Veryfit 2.0 "Warn Tips" and user agreement acceptance

On starting the App, there is a "Warm tips" screen (see screenshot) that instructs the user to read and understand the linked "Related user agreements" and "Privacy Policy", but the user can click past without reading them or even scrolling through them.

Section 5.1.1 of the User Agreement is particularly worrying. It states, "We may collect and use emails, avatars, nicknames, genders, birthdays, heights, weights, time zones, languages, and regions." The collection of email messages far exceeds any reasonable requirement for the device functionality. The use of the plural for "genders, birthdays," strongly implies that the data will be collected for multiple people, i.e., the user's contacts as well as the user.



Section 5, Privacy Policy of Veryfit 2.0 User Agreement

It may be that the User Agreement is poorly worded, but the facts are that the app requires excessive data access when it is installed, and the agreement requires permission to use excessive data access. This is in violation of DPP1:

DPP1 - Data Collection Principle

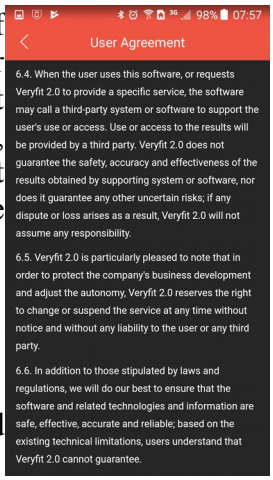
Personal data must be collected in a lawful and fair way, for a purpose directly related to a function /activity of the data user.

Data subjects must be notified of the purpose and the classes of persons to whom the data may be transferred.

Data collected should be necessary but not excessive.

It seemed unwise to accept the user agreement and therefore it was impossible to evaluate what the Smart Bracelet actually does.

Who is responsible for this egregious user agreement? The developer of the App is only identified by the App name, "Veryfit 2.0", in the user agreement. Maybe there are more contact details within the App, but they cannot be accessed without accepting the agreement. However, BOC Life made the decision to put their brand on the device and offer it to their customers, so they should take some responsibility for the software necessary to use the device.



Section 6.5 of the Veryfit 2.0 User Agreement is very strange

BOC Life has been contacted and asked to:

1. Immediately cease distribution of the device and app.
2. Contact all their customers who received the device to recall it.
3. Consider whether to issue an updated version of the device and app that addresses the privacy concerns
4. Update their procedures to properly vet future promotional gifts for privacy concerns.
5. Make a full, public report to the Privacy Commissioner for Personal Data (PCPD).

The PCPD has also been contacted with the same details. I await developments.

Allan Dyer

The Abysmal State of Personal Data Protection

<web-link for this article>

What do Cathay Pacific, Experian and LinkedIn have in common? All three companies have suffered a data breach that exposed their users' personal data. The data breach at Cathay Pacific is the most recent, and, ironically, Cathay Pacific chose to help their affected passengers by offering ID monitoring services provided by Experian.

Experian is a consumer credit reporting agency. Experian collects and aggregates information on over one billion people and businesses and also sells decision analytic and marketing assistance to businesses. Its consumer services include online access to credit history and products meant to protect from fraud and identity theft. Their data breach occurred between 2013 and 2015, affecting up to 15 million people who used the company’s services. However, the they are still trusted used by the UK government, for the Verify ID system, and USPS for their Address Validation. Presumably their security has improved since 2015.

I found out that my data had been compromised when I received an email from infosecurity@cathaypacific.com which specified which items of my personal data had been compromised, and invited be to use the Experian ID monitoring service by visiting a website: http://www.globalidworks.com/identity1 and entering a personalized activation code. I was immediately suspicious of the message: it was an unexpected message that invited me to visit an unrecognised website. The message also gave the address of their dedicated website, infosecurity.cathaypacific.com, which is in the well-known Cathay Pacific domain.

Fortunately, only my Name and Address had been compromised. Many people were not so lucky, other data accessed included passenger name; nationality; date of birth; phone number;

email; address; passport number; identity card number; frequent flyer programme membership number; customer service remarks and historical travel information; and a small quantity of credit card numbers, without the CVV code.

One other item of information was compromised: the implied information that I'm a Cathay customer, which could be used to send a phishing email telling me about the data breach and inviting me to give personal data to an "ID monitoring service". It would be a good idea to check the correct link for the Experian service from multiple sources, and not just rely on an unverified email.

I decided to try the Experian service with limited information. To use the service, it is necessary to agree to Experian's privacy policy, which includes the clause:

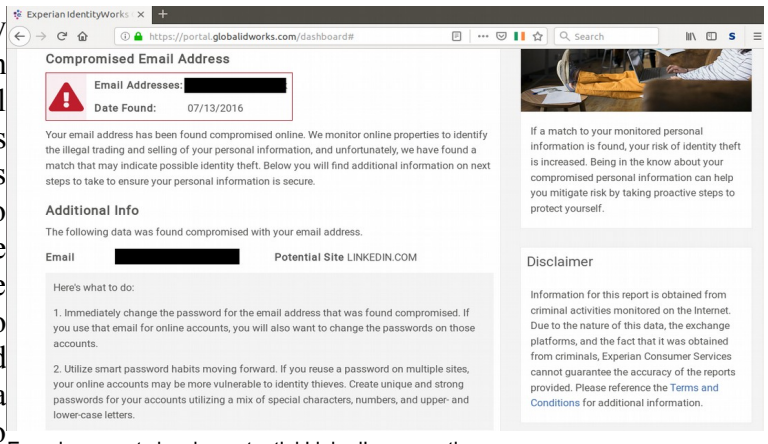
> 5.2 In order for us to provide you with our Services and for the prevention and detection of fraud, we will share your personal information with third parties who perform services on our behalf, including IT companies who perform services on our behalf. This includes the provision of IT services such as data storage and the provision of emails alerts sent to you to provide notification any of your suspected compromised information once you have enrolled to access our Services. These companies are required only to use your personal information as necessary to provide their services to us and only on our instructions. They are not permitted to process your personal information for their own purposes.

This contradicts the statement that information provided would be used solely for identity monitoring and not be shared with any other entity, made by Experian chief marketing officer Sisca Margaretta and reported by the South China Morning Post.

After agreeing to the privacy policy, the user can create an account with a user id and password. The password must be 8 to 15 characters, including at least one upper case, one lower case, one digit and one other character. However, the user is not warned of these restrictions in advance.

It is then necessary to select a "Security Question" and enter an answer. I have discussed previously the problems of security questions.

After complting the account registration, I provided two email addresses: the one dedicated to my Cathay Pacific account, and my general-purpose address.

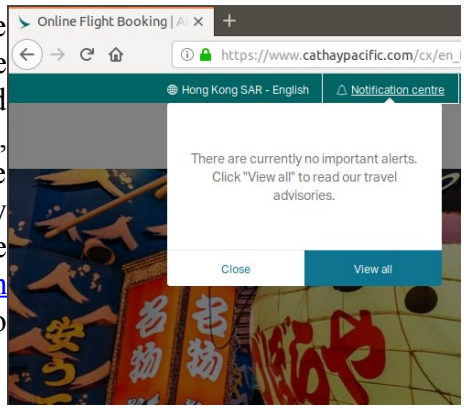


Experian report showing potential LinkedIn connection

I got an immediate report that my general purpose address had been found in July 2016, "Potential Site: LINKEDIN.COM". This was confusing, that email address is linked to my LinkedIn account, so were Experian simply telling me about that account? If that was the case, then why advise me to change the password immediately? Then I made a connection that brings us back to the commonality between Cathay Pacific, Experian and LinkedIn: there was a data breach at LinkedIn in 2012, and data from that breach became available online in May 2016, maybe Experian collected that information two months later? The information included email addresses and encrypted passwords for 117 million LinkedIn accounts, so that would be a very good reason to change my LinkedIn

password. Fortunately, I had already changed that password in 2012, in response to the original breach announcement. I had also not used the password on any other site.

Suggestions



Cathay Pacific website Notification centre on 2018-10-30

- Instead of using a link to an unknown site in the notification email, Cathay Pacific could have directed their passengers to a site they would already know, https://www.cathaypacific.com/, and use a prominent notice there to link to the Experian site. At the time of writing, Cathay Pacific do not have a prominent warning about the data breach on their main site, their Notification centre even says, "There are currently no important alerts."
- Experian should permit long passwords.
- Experian could improve their report wording:
    - Make it clear whether the email address and encrypted password were found online. An email address alone is not a significant threat, but an encrypted password can be cracked.
    - The advice is unclear about whether it is discussing the password used to access the email account, or one or more passwords for online accounts where the email address is used as a unique identifier. It makes a difference to which passwords need changing.
- Users should follow good security practice:
    - Minimise the personal data at risk: Only provide the minimum personal information that is required for providing the service.
    - Never re-use passwords.
    - Use strong passwords.

Protecting personal data after a breach is like a tar-pit. In order to sign up for an ID monitoring service, it is necessary to submit to more flawed security and distribute your personal data to more entities to enable the monitoring. Each effort to escape the tar enlarges its grip and drags you down.

Allan Dyer

More Information

- Experian's privacy policy
- Hong Kong government weighs in on Cathay Pacific data breach, urging airline to cooperate with privacy watchdog in investigation
- Hong Kong police visit Cathay Pacific HQ to investigate major data breach that hit 9.4 million customers
- No law to force firms to reveal data leaks, says Hong Kong privacy chief amid Cathay scandal
- Cathay Pacific hit by data leak affecting 9.4m passengers
- OPINION: Is the Cathay Pacific breach Hong Kong's worst-ever?
- Cathay Pacific urged to extend free ID monitoring service in wake of massive data breach affecting 9.4 million passengers
- After Cathay Pacific's debacle, companies must get proactive with cybersecurity and get customers involved
- Cathay Pacific passengers 'don't feel secure' after massive data leak hits Hong Kong-based airline
- Cathay Pacific likely to avoid harsh punishment despite taking months to notify passengers about massive data breach

- LinkedIn Revelations Highlight the Need for Stronger Network Security
- Another Day, Another Hack: 117 Million LinkedIn Emails And Passwords
- As Scope of 2012 Breach Expands, LinkedIn to Again Reset Passwords for Some Users
- Experian 2015 data breach
- Questioning Password Resets
- Personal data of 9.4 million passengers of Cathay Pacific and subsidiary leaked, airlines say
- Cathay Pacific data leak: airline warns customers to guard against phishing attempts
- Hong Kong's Cathay Pacific faces first collective legal action over massive data breach, with 200 customers poised to make claims

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/