Yui Kee Computing Ltd.

# Newsletter

June 2017

## Contents



## Hong Kong Privacy Commissioner Takes Maximum Action on REO Data Breach

*<web-link for this article>*

Stephen Kai-yi WONG, Hong Kong's Privacy Commissioner for Personal Data (PCPD), has issued his investigation report into the loss of notebook computers containing personal information of Hong Kong electors by the Registration and Electoral Office (REO). The Constitutional and Mainland Affairs Bureau (CMAB) has also issued the report of its Task Force charged with reviewing the reasons leading to the same incident.

The PCPD concluded that Data Protection Principle (DPP) 4 was breached and has issued an Enforcement Notice instructing the REO to remedy and prevent any recurrence of the contravention. DPP4 is the Data Security Principle, which requires, "practicable steps to safeguard personal data from unauthorised or accidental access, processing , erasure, loss or use". Issuing an Enforcement Notice is the maximum limit of the PCPD's powers under the Personal Data (Privacy) Ordinance. Failing to comply with an Enforcement Notice is an offence punishable by a maximum fine of HK$50,000 and imprisonment for 2 years. In other words, the PCPD has told the REO, "don't do it again", and the PCPD does not have the power to do anything more.

In the Hong Kong Government structure, the REO comes under the CMAB, so the report issued by the CMAB is, essentially, the Government's internal investigation into the incident. The report recommended improvements in the handling of Personal Data, following the IT Security requirements more strictly, improvements in the general security of election venues, and changes to the REO so that staff responsibilities are clearly understood and experience is retained between elections.

### Security Design

According to the PCPD's report, the REO was asked to demonstrate the security measures on a similar system, and "Considering the risk that would be brought about by the disclosure of the security technology (e.g. brand of the encryption software, composition of passwords, data access procedures, etc.), PCPD only invited experts from the OGCIO to attend the demonstration, and requested them to raise questions to the REO and offer professional advice on site." This suggests that the PCPD does not know Kerckhoffs's principle:

> *A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.*

or Shannon's maxim:

> *One ought to design systems under the assumption that the enemy will immediately gain full familiarity with them.*

Obviously, the possessor of the stolen notebook can identify the encryption software used and the workings of the system by inspection, so by restricting the information the REO is only preventing useful feedback on how to improve the system for future use.

The decision by the PCPD to obscure details of the security technology looks even more questionable when the CMAB report is examined. The CMAB report contains details of the two data systems installed on the two stolen netbooks, namely the Polling and Counting Access Control System (PCACS) and the Electors Information Enquiry System (EES). The PCACS (which the PCPD concluded was not a problem under the Privacy law) operated through handheld devices that connected to the stolen notebook through an encrypted WiFi network, and the database on the notebook was protected by an 8 character password. On the other notebook, the EES was protected by three layers of login: to Windows, to the encryption software protecting the EES and its database, and to the EES itself. The disc drive containing the database and EES were encrypted with AES 256. The Hong Kong Identity Numbers (HKID) were encrypted with AES 256 (presumably in an encrypted database column), and the whole database was encrypted with AES 128. The report claims, "The decryption would need to be done through the EES programme", but does not explain how that restriction was enforced, if it could be.

The report also states, "The key to decrypt the database was unrelated to the three passwords mentioned above. In other words, even if a person holds the three passwords, he/she would still not be able to decrypt the entire database using the passwords.", which presumably implies that the decryption key for the entire database was, somehow, embedded in the EES programme. Therefore, suitable reverse engineering of the EES programme could recover the decryption key.

Is it possible to guess what software was used for the disc drive encryption? What encryption software that supports AES 256 is commonly used on Windows to encrypt whole drives? Microsoft has actually provided BitLocker with Windows since Windows Vista, so the disc encryption is probably BitLocker. This is good news, if the notebook computer has a Trusted Platform Module (TPM), because BitLocker will store the key in the TPM, and the TPM will prevent brute-force password guessing. Enterprise-grade notebooks often have a TPM.

If these assumptions are correct, then the continued security of the Hong Kong Voters' database depends on:

1. Does the stolen notebook computer have a TPM?
2. Can the thief reverse-engineer the EES and recover the other encryption keys?

**More Information**

- Hong Kong privacy watchdog blasts electoral office for massive data breach
- Privacy Commissioner Publishes Investigation Report on the Loss of Registration and Electoral Office's Notebook Computers containing Personal Data of Election Committee Members and Electors
- Investigation Report (Translation) : Registration and Electoral Office Loss of Notebook Computers containing Personal Data of Election Committee Members and Electors
- Report of the Task Force on the Computer Theft Incident of the Registration and Electoral Office

# Beware of Fake Security Advice

***<web-link for this article>***

*Allan Dyer*

I was recently asked to share a privacy guide for journalists, unfortunately, on inspecting the guide, I found very serious flaws, and evidence of deliberately misleading advice. Therefore, I am sharing my anti-recommendation of "Online Privacy Guide for Journalists 2017", which is at https://www.vpnmentor.com/blog/online-privacy-journalists/ . Here is why:

The article starts with a brief description of the confidentiality problems faced by investigative journalists. Then, under the heading, "Communicating with your source and safeguarding the sensitive data", the advice begins. The advice starts with a warning about backdoors and a recommendation to encrypt everything; there is a link to a Bruce Schneier article, so it looks reasonable. Then there's the sentence, "But if you want bullet-proof security, you will need more than the AES encryption method.", but no explanation of what "more" is. This woolly sentence seems to throw doubt on the security of AES, but 256 bit AES is required by the NSA for Top Secret information and it is generally regarded as, currently, the best available algorithm. Perhaps the sentence is supposed to imply that encryption is just one part of your operational security, and the other aspects must not be neglected, but it does not make that clear. Let's say this is poor writing and continue.

My attention was grabbed by point 8, "Protecting Data on your computer" that discusses password and passphrase strength. The discussion uses screenshots from "Gibson Research Corporation’s password strength calculator" to compare the strength of "F53r2GZlYT97uWB0DDQGZn3j2e" and "i wandered lonely as a cloud" and concludes, 'The phrase: “I wandered lonely as a cloud”, he points out, is so much easier to remember and is also more secure, taking the same software 1.24 hundred trillion centuries to exhaust all possibilities. Well, passphrase it will be.' My bovine excrement alarm deafened me.

Passphrases are good, a definite improvement on a password, but the title of a famous poem is not a good passphrase. Compared to a good passphrase, it is like using 'password' instead of a good password. We advise not choosing a word that can be found in a dictionary as a password, and using a famous quote as a passphrase is just as bad. "I wandered lonely as a cloud" is item 36 on this list of 48 Of The Most Beautiful Lines Of Poetry.

Secondly, the discussion implies that the entropy of "i wandered lonely as a cloud" is equivalent to the entropy of "F53r2GZlYT97uWB0DDQGZn3j2e". By restricting the passphrase to dictionary words in a meaningful order, the number of possibilities has been vastly reduced. The well-known XKCD cartoon on passphrase strength attributes 11 bits of entropy to each common random word. Assuming a vocabulary of about 2000 common words, that is reasonable because $2^{11} = 2048$. Using the same estimate of entropy, 6 random common words would give 66 bits of entropy, but point 8 claims the 6 non-random words of “I wandered lonely as a cloud” represent a search space of $62^{26}$ possibilities, which is about 154 bits of entropy. The strength of XKCD's "correct horse battery staple" example depends on randomly choosing the words *without any consideration of meaning*, and retrospectively constructing a meaning as a memory aid. For the removal of any doubt, "correct horse battery staple" became a terrible choice for a passphrase the moment XKCD published that cartoon, concentrate on the method.

Having had my attention grabbed, I looked closer at point 8 and found something far more disturbing: this was not just bad advice, it was maliciously constructed bad advice. The evidence is:

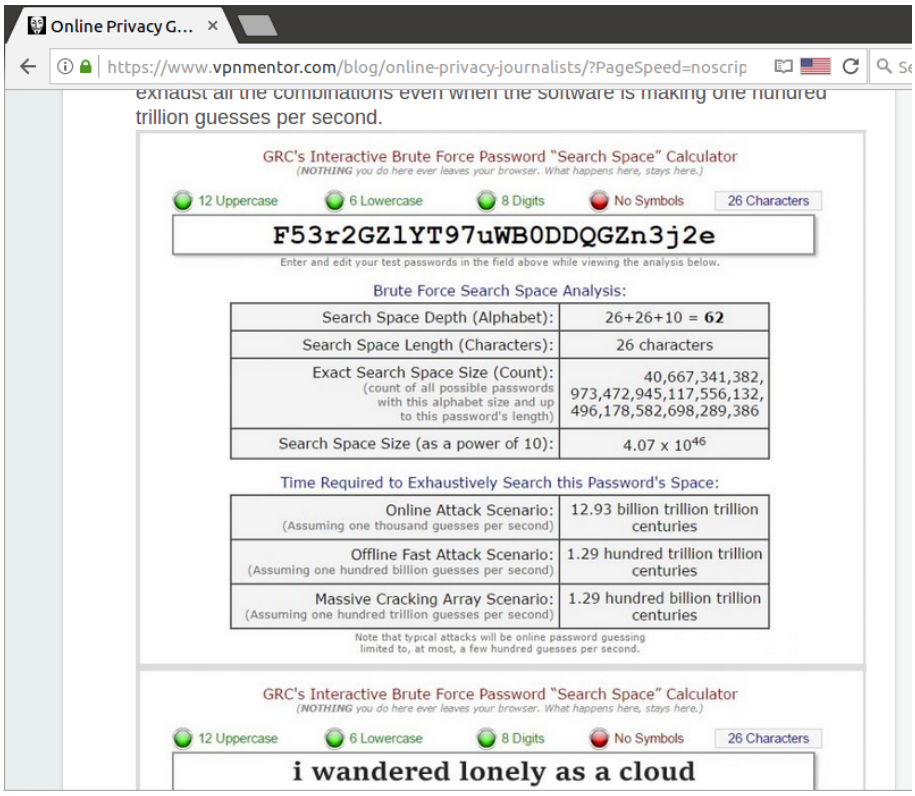
1. It misrepresents GRC's | Password Haystacks: How Well Hidden is Your Needle? as "Gibson Research Corporation’s password strength calculator". In fact, the page

specifically warns, "IMPORTANT!!! What this calculator is NOT . . . It is NOT a “Password Strength Meter.”" I am not sure that I agree with the idea of "Password Padding" that Gibson presents on his page, it seems highly dependant on the attacker not using a search strategy that considers password padding, but the "Online Privacy Guide for Journalists 2017" (OPG) is misleading about Gibson's message.

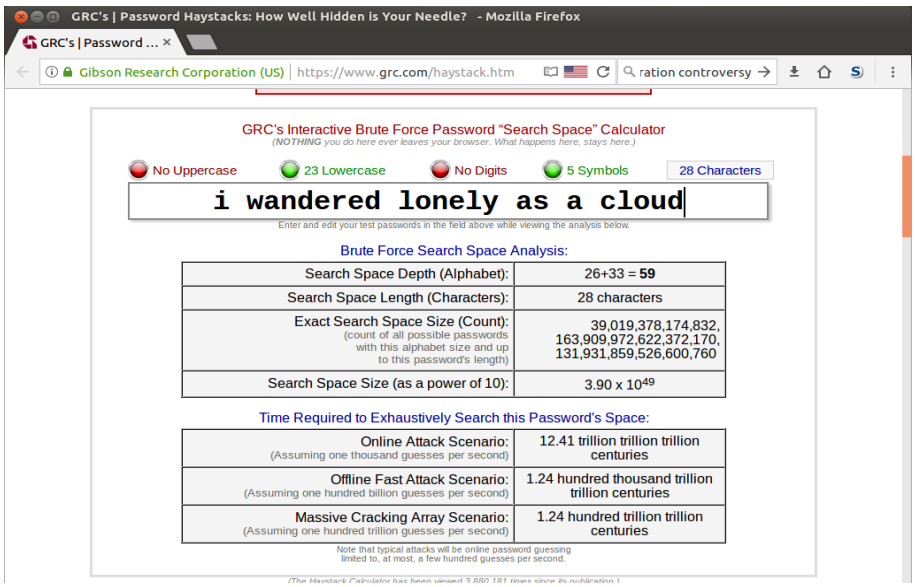
2. It falsifies the results from GRC's Password Haystacks page. Compare this screenshot of the Online Privacy Guide (OPG) with my screenshot of GRC's Password Haystacks page. Note:

    1. The OPG screenshot shows "i wandered lonely as a cloud" contains 12 Uppercase, 6 Lowercase, 8 Digits and No Symbols. My count is No Uppercase, 23 Lowercase, No Digits and 5 Symbols.
    2. There is a difference in the character count: 26 characters versus 28 characters
    3. The font for the phrase is different, the OPG has a serif font and my screenshot shows the GRC page uses a sans serif font. Look closely at the tail of the y and the tops of the w, for example.

    In short, the OPG faked the screenshot for the "strength" of "i wandered lonely as a cloud" by taking the screenshot for the "strength" of "F53r2GZlYT97uWB0DDQGZn3j2e" and pasting in the phrase "i wandered lonely as a cloud".




Screenshot of Online Privacy Guide




Screenshot of GRC Password Haystacks page

I think that is enough to establish the bad intention of the author of this "Online Privacy Guide for Journalists 2017". I strongly recommend looking for more reliable sources of security advice, and, most importantly, understand their arguments and use your own critical thinking.

**Updated: 20th June 2017**

vpnMentor has responded to the criticism in this article:

A letter to Allan and his readers.

Hi there, my name is Ariel and I'm one of the founders of vpnMentor. I wanted to address a post that Allan wrote, and explain to you guys what happened.

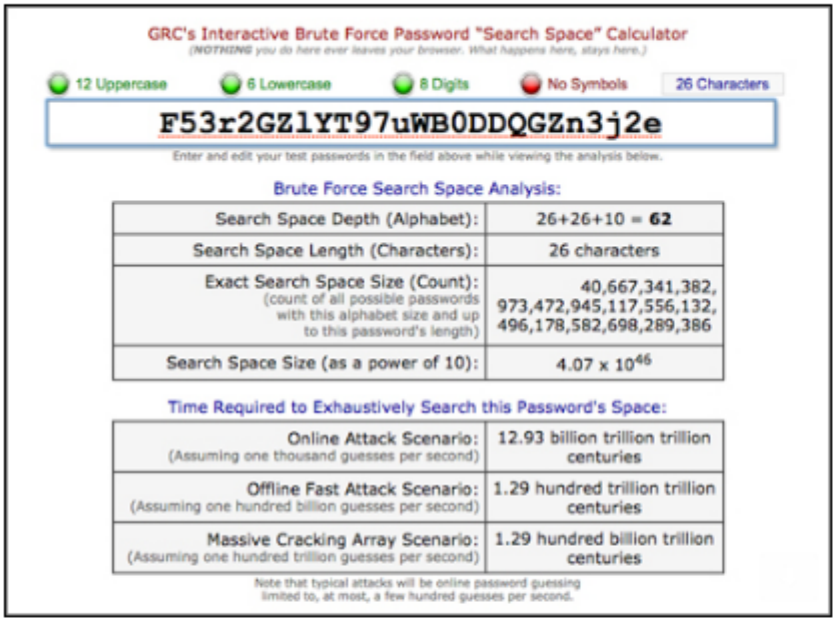
Basically, in his posts, Allan has three doubts:

1. The OPG screenshot shows "i wandered lonely as a cloud" contains 12 Uppercase, 6 Lowercase, 8 Digits and No Symbols. My count is No Uppercase, 23 Lowercase, No Digits and 5 Symbols.
2. There is a difference in the character count: 26 characters versus 28 characters
3. The font for the phrase is different, the OPG has a serif font and my screenshot shows the GRC page uses a sans serif font. Look closely at the tail of the y and the tops of the w, for example.

It actually easy to explain. Mike, who wrote the privacy guide, received assistance from many people in writing it. One of them was in charge of the graphics and he was asked to send a screenshot, he just didn't use the same password the text uses, but rather the one he was instructed to replicate during the early writing process. This is why the screenshot doesn't match the password we used in the text. We didn't think this is of such importance. But, every so often, one comes across someone serious as Allan who checks the text, and verifies for his users that what he shares, doesn't just look nice, but is also serious and accurate.

Below is the screenshot from Mike's email to the graphic designer:

3. Here, please insert this password: F53r2GZlYT97uWB0DDQGZn3j2e and then just activate the calcula




4. A picture of Thinkpad X60 or X61. much like this one:
http://www.laptopoutlet.com/ibm-thinkpad-x60-used-laptops.html#.WMUdjzvys2w

5. A screenshot of duckduckgo home page.
https://duckduckgo.com/

Could we have them back in two to three hours :-), because it's a bit urgent?

I'm around for every question.

All the best,

Mike

Anyhow, we want to first thanks Allan for being cautious. Just imagine if the Democratic Party in the U.S. was as cautious as him when they got a Russian email asking them to click here and restore password…

I hope that we helped explain the issue, and urge you to protect your privacy online, which is under threat more and more each day.

Best,
Ariel Hochstadt

I would like to thank Ariel Hochstadt and the team at vpnMentor for their openness and willingness to respond to criticism. Allan.

**More Information**

- XKCD Password Strength
- GRC's | Password Haystacks: How Well Hidden is Your Needle?
- list of 48 Of The Most Beautiful Lines Of Poetry

# Hong Kong Police Launch Cybersecurity 2017 Campaign

*<web-link for this article>*

The Cyber Security and Technology Crime Bureau (CSTCB) of the Hong Kong Police and supporting organisations have launched a Cybersecurity 2017 Campaign with the slogan "Build Botnet-Free City".

The website focusses on simple advice, conveyed through a YouTube video:

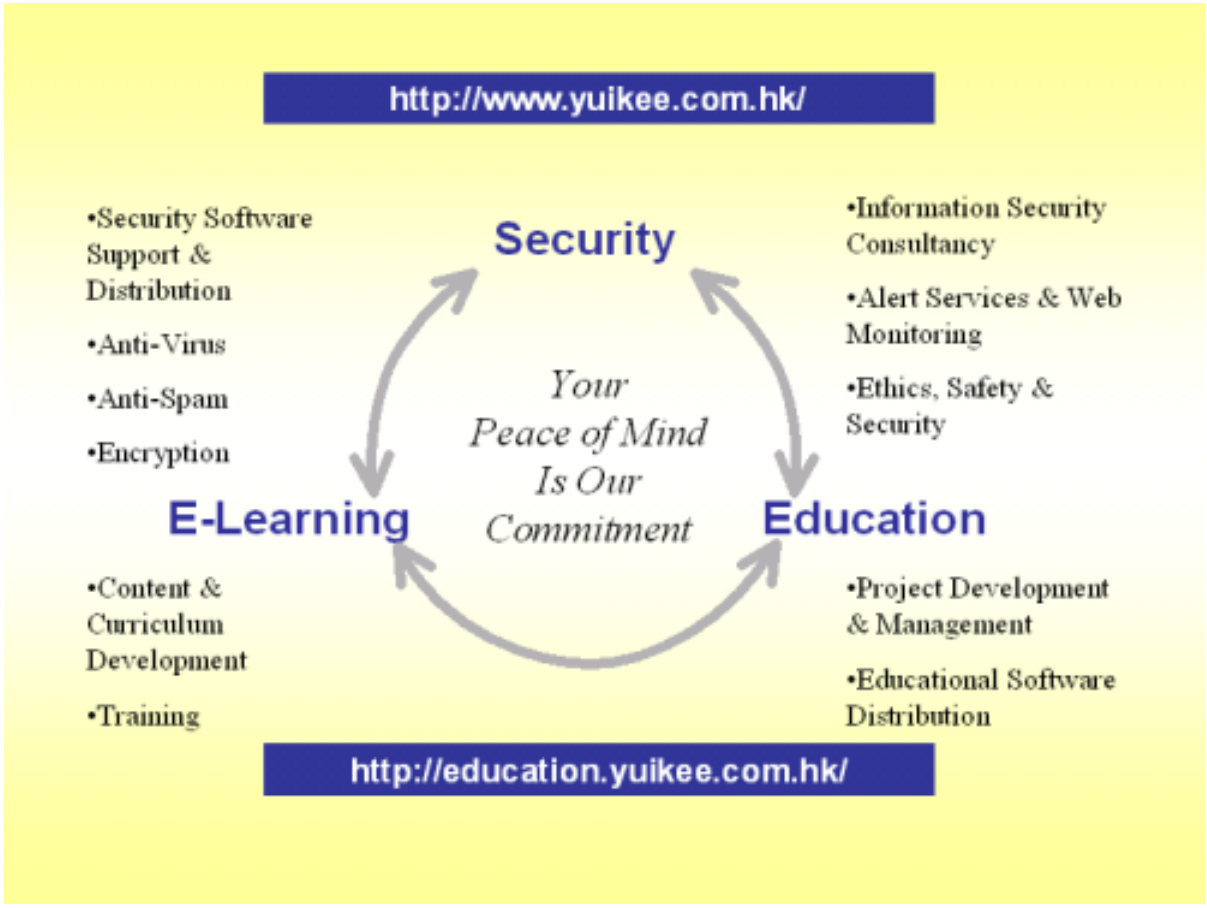
- Firewall On
- Install Anti-Virus Software
- Do not click on suspicious email

The campaign has attracted attention on Twitter.

**More Information**

- Cybersecurity Campaign 2017
- Leo Weese comments on Twitter


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/