Yui Kee Computing Ltd.

Newsletter

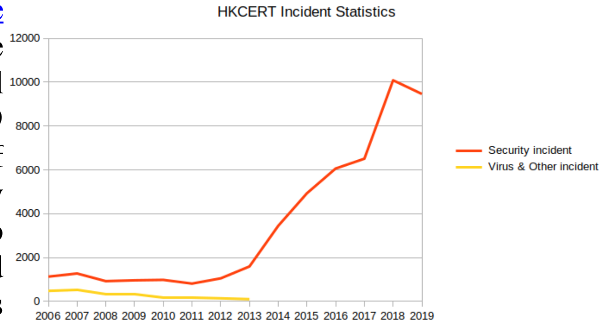
March 2020

Contents

Is Cybercrime Falling in Hong Kong?

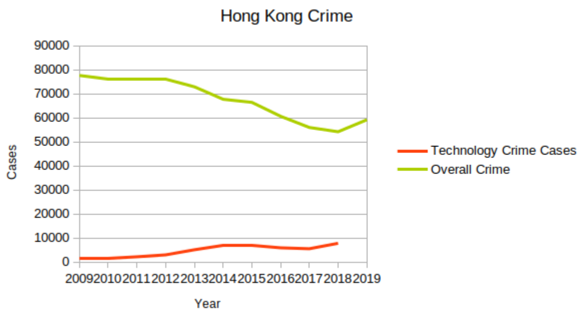
<web-link for this article>

The Hong Kong Police's summary of crime statistics for 2019 shows a dramatic change from previous years, which noted an overall fall in crime, but a rise in cybercrime. 2019 has a rise of 9.2%, and no mention of cybercrime. The police statistics do not show a technology crime category. However, two categories that are frequently implemented online nowadays decreased: blackmail cases fell from 635 to 415 (-34.6%) and deception cases fell from 8372 to 8216 (-1.9%).



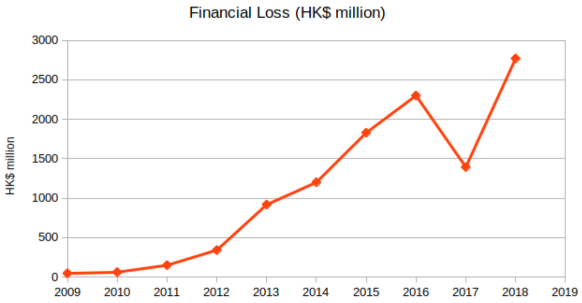
HKCERT Incident Report

The statistics also do not show what has happened to Personal Data Privacy crimes. The Privacy Commissioner stated that 430 cases had been referred to the Police for investigation between 2019-06-14 and 2019-07-26 but they are not evident in the Police statistics. It is possible that some of those cases could be classified as Criminal Intimidation, but that figure dropped by 22% (from 1512 in 2018 to 1180 in 2019).



HK Cybercrime Statistics

Statistics from the Government InfoSec website are currently only available to 2018,

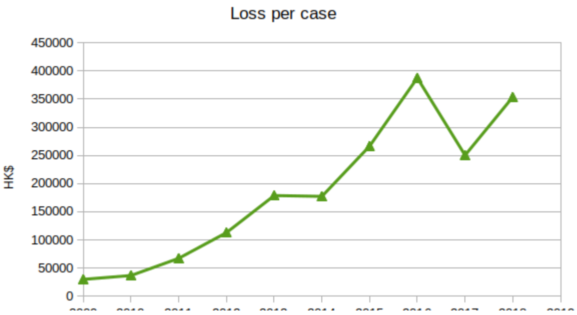


Cyber Crime Financial Loss Statistics

and they show a rise in both the number of cases and the financial loss per case from 2017 to 2018.

Hong Kong CERT statistics show a 6.2% decrease in reported security incidents from 2018 to 2019.

The rise in the crime statistics is directly relatable to the recent civic disturbances, and the Police link the rise in robbery, burglary, snatching and theft from vehicle to criminals taking advantage of the thinning out of crime prevention work and resources of Police, but this does not explain why those crimes increased when blackmail, deception, criminal intimidation and information security incidents fell. Possible explanations include an increase in public awareness of cybersecurity due to the publicity around fake news, prevention of surveillance, and promotion of encrypted messaging apps, or under-reporting of crimes due to high levels of distrust in the Police.



Cyber Crime Financial Loss per Case Statistics

More Information

- Crime rises in 2019
- Personal Privacy and the Free Flow of Information
- Hong Kong Cybercrime Continues to Rise
- Computer Related Crime
- HK CERT Statistics
- Criminal Investigation Procedures Commenced on 430 Cases of Online Disclosure of Personal Data in Accordance with the Law
- Personal Privacy and the Free Flow of Information

Is DKIM a Waste of Resources?

<web-link for this article>

If all goes well, the March 2020 Yui Kee Newsletter will be the first to be distributed in a DKIM-signed email, but why has it taken so long, and what are the advantages of DKIM?

DomainKeys Identified Mail (DKIM) is an internet standard defined by RFC 6376, published in 2011. It is intended as an email authentication method, allowing a sender to sign their message headers and body using a key published on their DNS server. Recipients can verify the signature to check whether the sender is authorised to send email from that domain, and whether the message body has been modified.

Usage of DKIM has been increasing. Some online email testing services, such as mail-tester, use DKIM in calculating their "Spammyness" score, Google replaces the sender's profile image with a question mark if the sender cannot be authenticated and the UK Government provides guidance on using DKIM, SPF and DMARC. Wait, so what are SPF and DMARC?

SPF

Sender Policy Framework (SPF) is a different method of email authentication, defined by RFC 7208 published in 2014, but earlier versions date from around 2002. Senders can publish a list of hosts that are permitted to send email for their domain on their DNS. If a recipient receives email from an unlisted host, they can reject it or mark it as spam. SPF is easy to implement for organisations that know where their sending email servers are. It can be more difficult for large organisations or email service providers. Yui Kee has been using SPF for many years.

DMARC

Domain-based Message Authentication, Reporting and Conformance (DMARC) depends on DKIM and SPF and is defined by RFC 7489. DMARC allows the domain owner to publish a policy in their DNS records to specify how they are using DKIM and SPF, how the receiver should handle failures and a reporting mechanism. The reporting mechanism could be an important way for domain owners to get feedback on the state of their email. However, a full discussion of DMARC will have to wait for another article, it is sufficient to note here that it communicates a policy about DKIM and SPF from the domain owner to the world.

Comparison

So DKIM and SPF both provide some assurance that a message which purports to be from a particular domain actually was authorised by the domain owner in some manner. SPF tests the MAIL FROM (envelope) address, which is not necessarily the same as the address presented to the end user in the email client. DKIM signs the From header field, which is normally presented to the end user in the email client.

In addition, DKIM prevents modification of the header fields and the body (but not necessarily all of them). This might prevent a malicious intermediary modifying a message, or prevent repudiation of a genuine message. Modification of email in transit is not thought to be a common problem, and depending on the configuration, DKIM might not protect the important parts of the headers or message. In any case, server-to-server encryption of the message (by TLS) would be a more reliable way to prevent modification in transit.

It would be risky to rely on the prevention of repudiation provided by DKIM; as there is no published policy for replacing keys, the domain owner could replace the signing key in the DNS at any time, preventing the verification of the signatures on historically-received messages. S/MIME is a more suitable technology for providing end-to-end integrity and non-repudiation of email content.

Mailing Lists

Mailing lists present a challenge for any sender authentication system: A sends a message to list M, and M re-sends the message to X, Y and Z. Does the authentication verify A, M or both? Depending on the circumstances, the message distributed to the recipients might fail either or both DKIM and SPF tests.

With SPF, the solution is to use the mailing list's address in the envelope when re-sending. For example, this Yui Kee Newsletter uses newsletter-bounces@yuikee.com.hk as the MAIL FROM address. The receiver can verify that the message is coming from an authorised mail server for the mailing list's domain, and the reader can understand that the message was distributed to many recipients via the list.

For DKIM, the situation is more complex. Apart from the From header address not necessarily matching the domain of the mailing list, mailing list software often modifies the Subject (adding the name of the list) and the body (maybe adding unsubscribe instructions). Both of these can invalidate a DKIM signature added by the original sender's mail server. One possible solution is for the mailing list server to simply add another DKIM signature, after the modifications. RFC 6376 was written with the possibility of multiple invalid signatures, and a valid signature in mind, and this is the solution that the Yui Kee Newsletter is using. An alternative method is for the mailing list to wrap the incoming message in an outer message with the From: header containing the list's posting address. The outer message can be signed with a new DKIM signature, verifying that it was sent by the list, and the inner message still has a valid DKIM signature, verifying it was sent by the original author. This method might be more suitable for discussion-type mailing lists.

Incoming Email Statistics

What does DKIM and SPF give us in practical terms? Email services such as GMail indicate when a sender has not been authenticated by replacing the profile image with a question mark, as mentioned above. Is this something the average user notices and acts on when deciding whether to trust a message? It is difficult to measure such an effect.

We can measure how SPF and DKIM affect messages at an email gateway. The statistics presented here are based on about 10 days of incoming messages received at Yui Kee by our Sophos Puremessage gateway. They do not include connections from blocked IP addresses, in those cases the connection was dropped before message transmission. Sophos Puremessage tests both SPF and DKIM. In Yui Kee's configuration, an SPF result of FAIL results in an immediate rejection of the message, this is not the default configuration, but it honours the published policy of the sender: that the message should be rejected if it does not arrive from a listed IP address.

Sophos Puremessage has 25 rules that test some aspect of DKIM, but only two of them (CS_DKIM_SIG and CS_DKIM_SIG2) have any effect on the "spamminess" score (increasing the weight by 6.5 and 1, respectively). These are describe as "DKIM-Signature header has content common in snowshoe spam", in other words, the spamminess score is increased because the DKIM signature looks suspicious.

A total of 8027 messages were received, 29% (2291) were kept and the rest were quarantined or rejected:

Keep	2291	28.54%
Quarantine	3233	40.28%
Reject	572	7.13%
SPF_FAIL	1578	19.66%
Block List	254	3.16%
aborted	99	1.23%

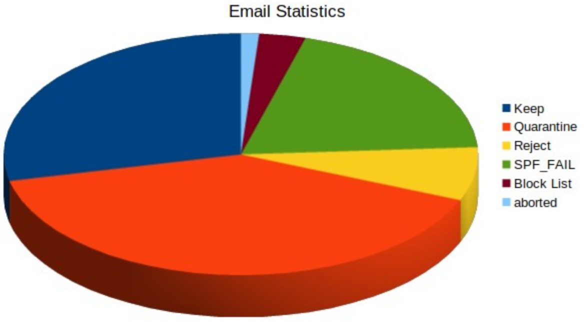


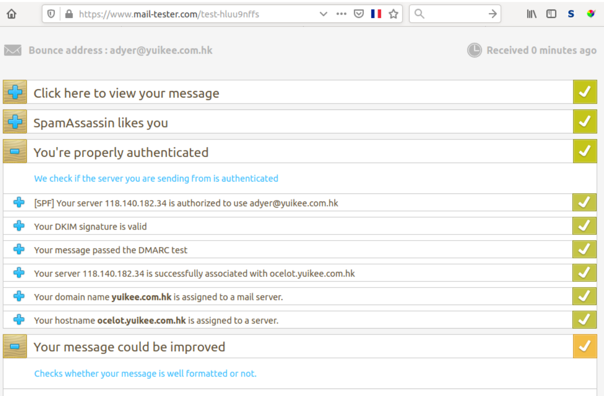
Illustration 1: Email Statistics for 10 days

24% (1920) messages had a DKIM signature, and 58% (4618) had a usable SPF record for the domain. 20% (1578) messages were rejected for failing the SPF test. Of the 1920 messages with a DKIM signature, none matched the CS_DKIM_SIG rule, and 1.8% (141) matched the CS_DKIM_SIG2 rule. All of those 141 messages had a spam probability of over 80%, they were all quarantined under the policy and the weight of 1 for the CS_DKIM_SIG2 rule did not change that classification.

Conclusion

We did not hurry to implement DKIM because of the uncertain benefits and limited adoption. Not all internet "standards" gain wide acceptance, other proposed email authentication standards include ADSP and Sender ID, both never gained wide acceptance and are now considered historic.

SPF was simple to implement for outgoing email (just add a DNS TXT record) but DKIM required careful consideration of the signing policy and effects on mailing lists. The



Bounce address : adyer@yuikee.com.hk

Received 0 minutes ago

Click here to view your message ✓

SpamAssassin likes you ✓

You're properly authenticated ✓

We check if the server you are sending from is authenticated

[SPF] Your server 118.140.182.34 is authorized to use adyer@yuikee.com.hk ✓

Your DKIM signature is valid ✓

Your message passed the DMARC test ✓

Your server 118.140.182.34 is successfully associated with ocelot.yuikee.com.hk ✓

Your domain name **yuikee.com.hk** is assigned to a mail server. ✓

Your hostname **ocelot.yuikee.com.hk** is assigned to a server. ✓

Your message could be improved ✓

Checks whether your message is well formatted or not.

SPF, DKIM and DMARC EMail Authentication Testing at mail-tester growing adoption by major email service providers and support by governments eventually prompted our adoption. The possibility that a recipient might regard our email as suspect because it lacks a DKIM signature is enough reason to use it.

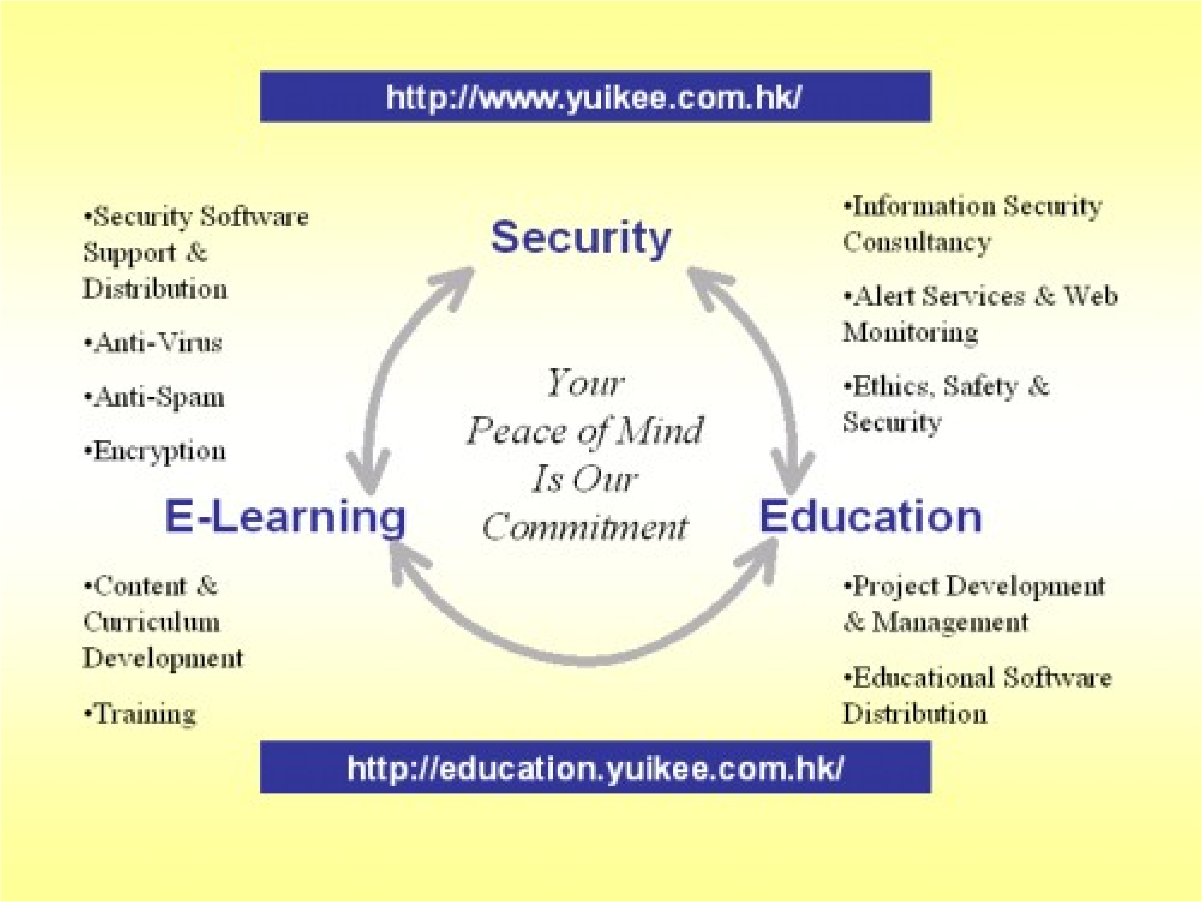
However, for incoming email, the statistics above show that the DKIM tests had no effect on which messages were kept, quarantined or rejected. We could regard the resources used in those tests to be wasted.

More Information

- DomainKeys Identified Mail
- RFC 6376 DomainKeys Identified Mail (DKIM) Signatures
- mail-tester
- Making email safer for you
- Using Domain-based Message Authentication, Reporting and Conformance (DMARC) in your organisation
- Sender Policy Framework
- RFC 7208 Sender Policy Framework (SPF) for Authorizing Use of Domains in Email
- DMARC
- RFC 7489 Domain-based Message Authentication, Reporting, and Conformance
- Author Domain Signing Practices (ADSP)
- Sender ID

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 Software Support & Distribution

•Anti-Virus

•Anti-Spam

•Encryption

Security

•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/