Infosec 101

Protect Your Data, Protect Your Sources

26 February 2015
Foreign Correspondents’ Club
Hong Kong

Presented by

Fabian Lischka • Larry Salibra • Leonhard Weese

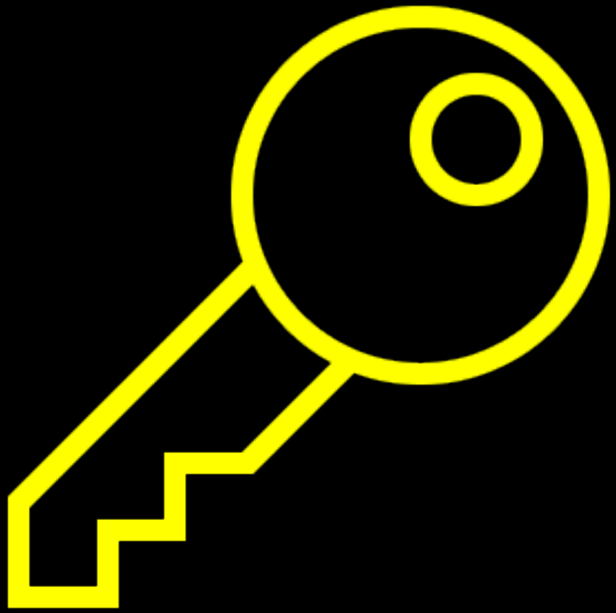
HITACHI
PHILIPS
SAMSUNG

Agenda

- Encryption Works
- Protect Your Device
- Protect Your Account
- Protect Your Communication

Encryption Works

Algorithm creates mathematically linked lock and key.
(usually called public and private key)



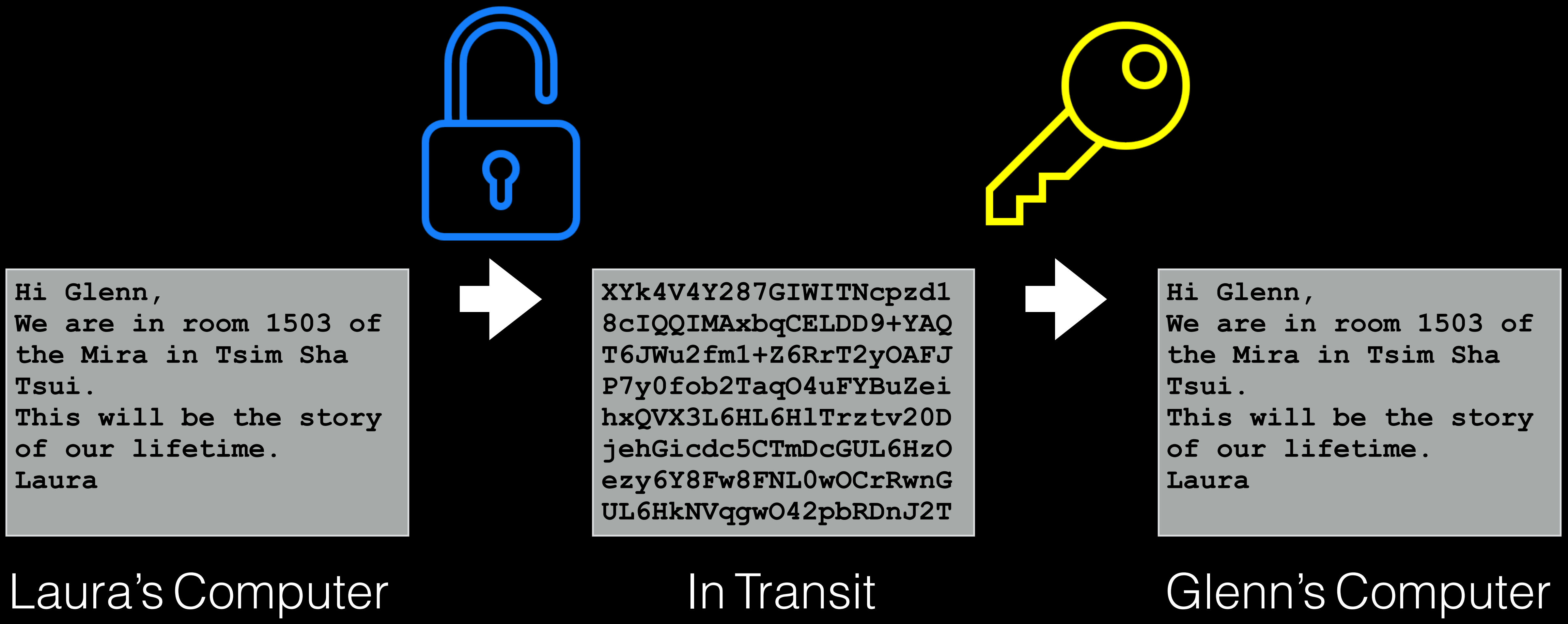
Private key
Never leaves the
computer

Public lock
Uploaded and
given to anybody

Encryption Works

Anybody can encrypt any data using the public lock.

Only the owner of the private key
can decrypt the data and open the file.



```
Hi Glenn,
We are in room 1503 of
the Mira in Tsim Sha
Tsui.
This will be the story
of our lifetime.
Laura
```

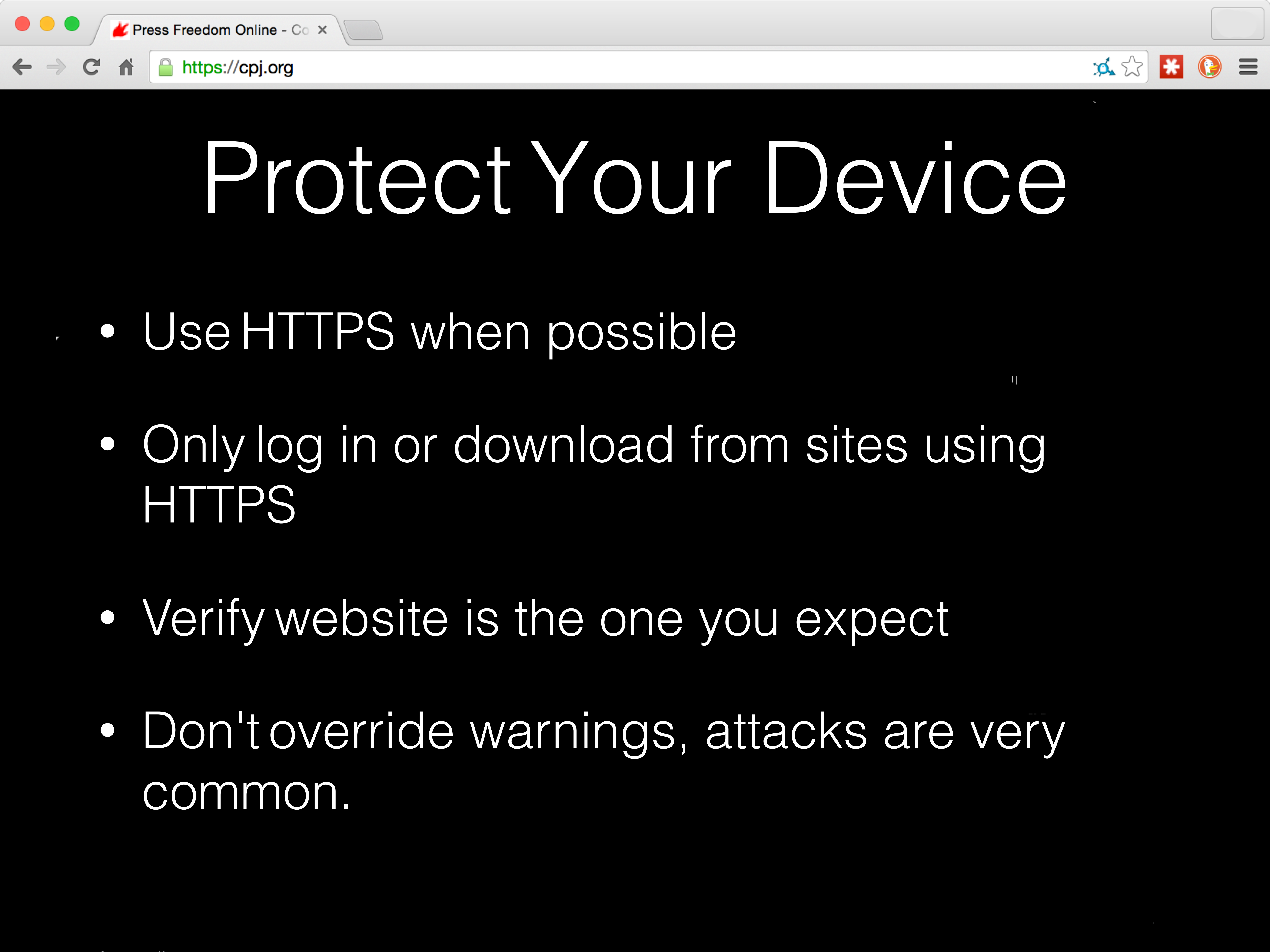
Laura’s Computer

```
XYk4V4Y287GIWITNcpzd1
8cIQQIMAxbqCELDD9+YAQ
T6JWu2fm1+Z6RrT2yOAFJ
P7y0fob2TaqO4uFYBuZei
hxQVX3L6HL6HlTrztv20D
jehGicdc5CTmDcGUL6HzO
ezy6Y8Fw8FNL0wOCrRwnG
UL6HkNVqgwO42pbRDnJ2T
```

In Transit

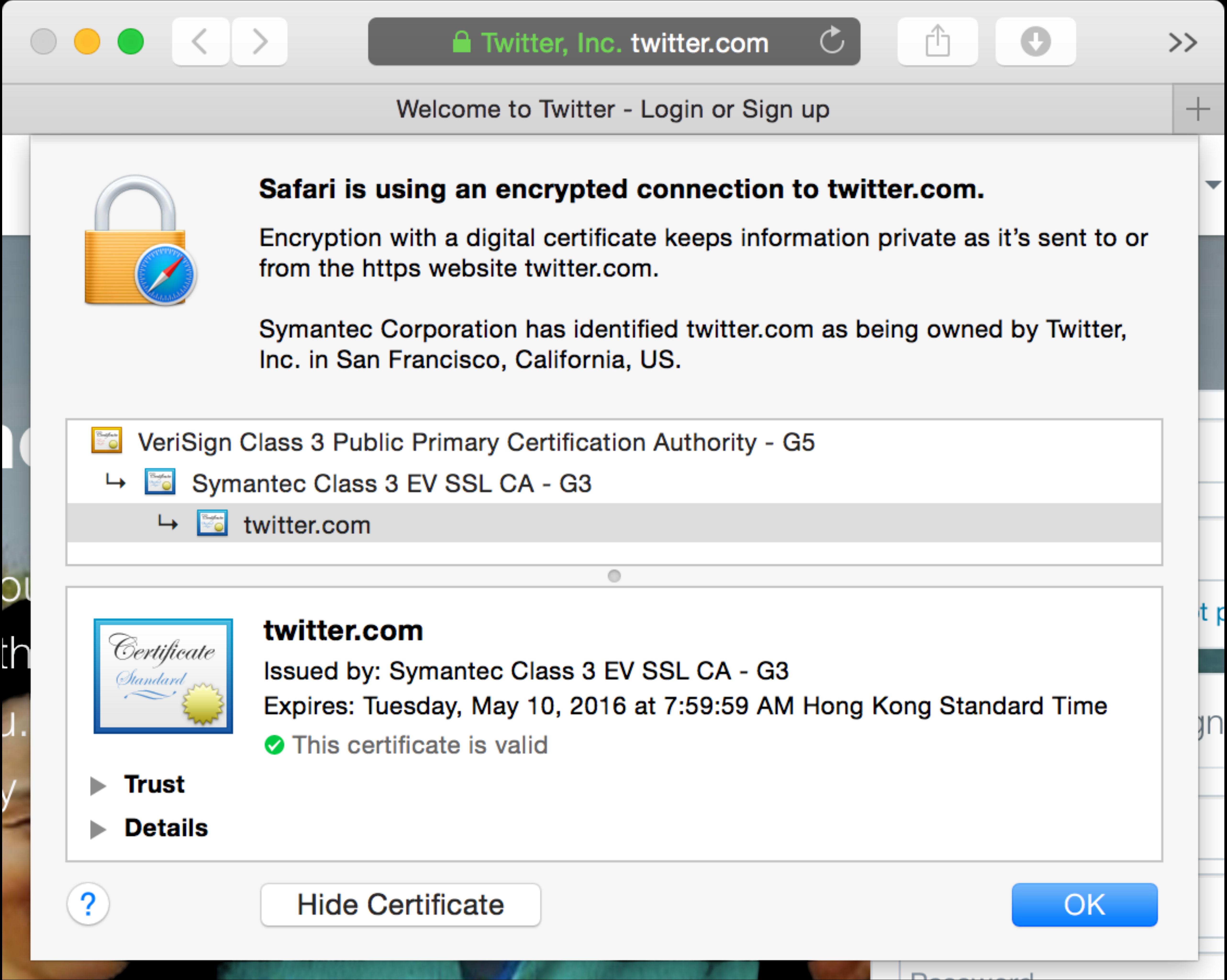
```
Hi Glenn,
We are in room 1503 of
the Mira in Tsim Sha
Tsui.
This will be the story
of our lifetime.
Laura
```

Glenn’s Computer



Protect Your Device

- Use HTTPS when possible
- Only log in or download from sites using HTTPS
- Verify website is the one you expect
- Don't override warnings, attacks are very common.



Twitter, Inc. twitter.com
Welcome to Twitter - Login or Sign up

Safari is using an encrypted connection to twitter.com.

Encryption with a digital certificate keeps information private as it's sent to or from the https website twitter.com.

Symantec Corporation has identified twitter.com as being owned by Twitter, Inc. in San Francisco, California, US.

VeriSign Class 3 Public Primary Certification Authority - G5
↳ Symantec Class 3 EV SSL CA - G3
↳ twitter.com

twitter.com

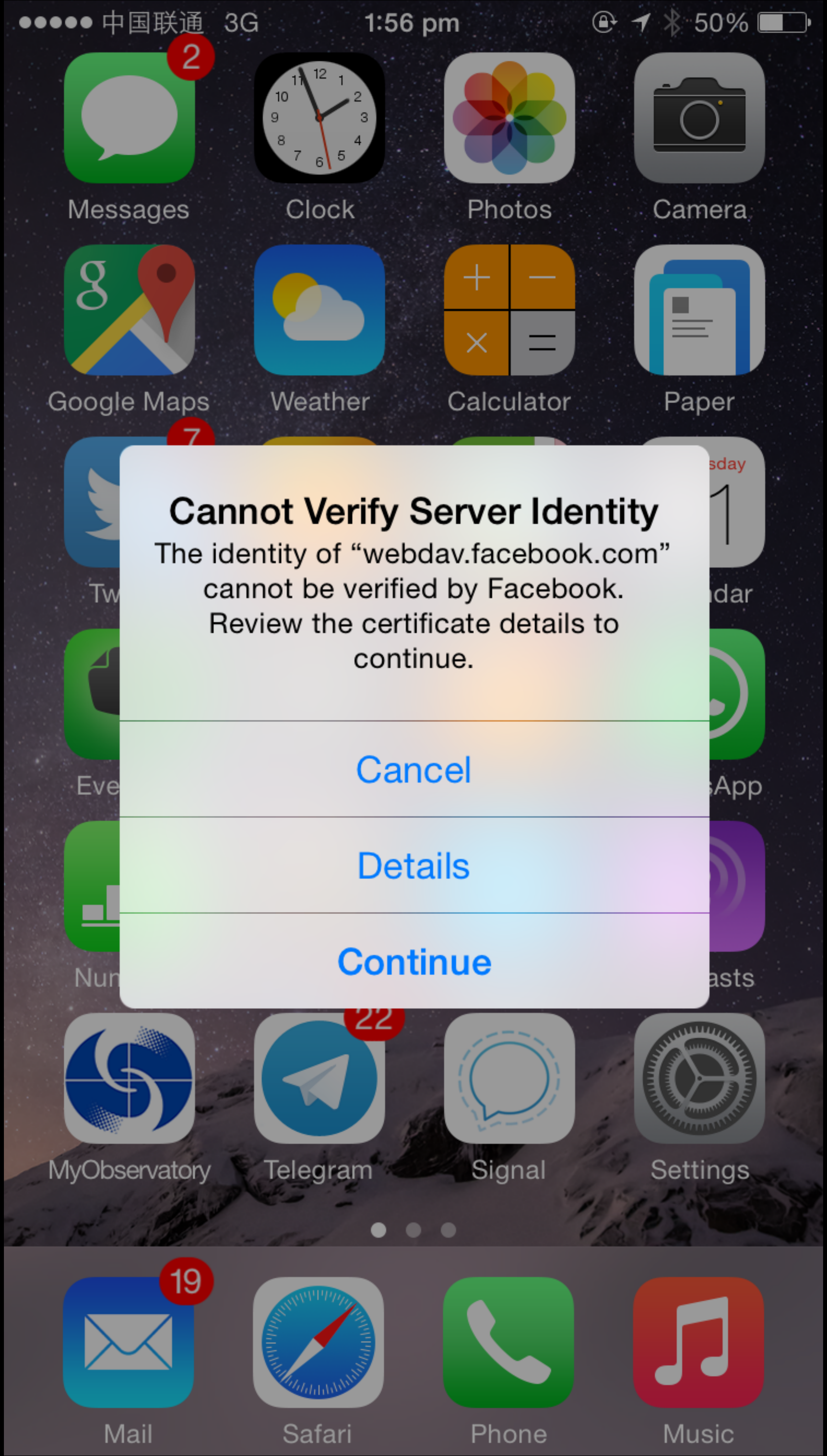
Issued by: Symantec Class 3 EV SSL CA - G3

Expires: Tuesday, May 10, 2016 at 7:59:59 AM Hong Kong Standard Time

✓ This certificate is valid

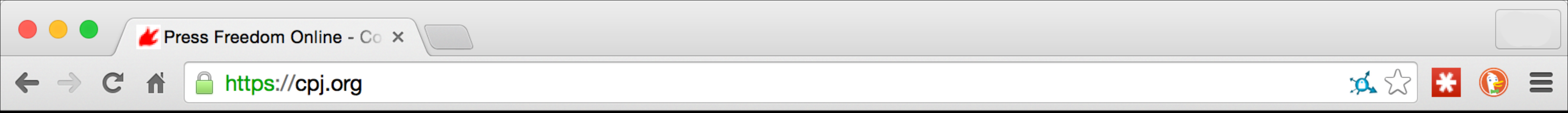
▶ **Trust**

▶ **Details**



Cannot Verify Server Identity

The identity of “webdav.facebook.com” cannot be verified by Facebook. Review the certificate details to continue.

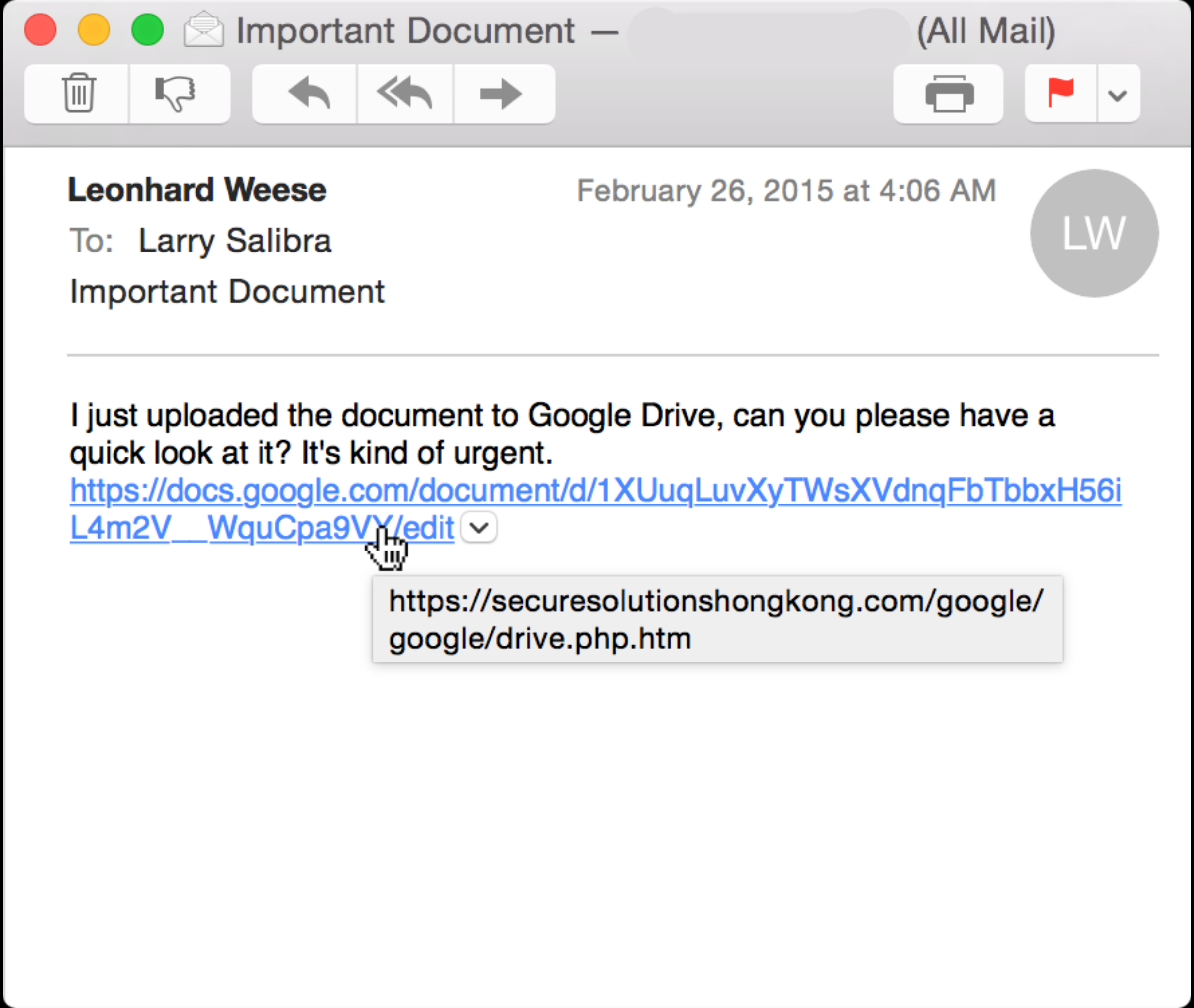


Protect Your Device

Be careful with all links!

- Don't trust emails & text messages: anybody can spoof them

- Verify all links before you click



Important Document — [redacted] (All Mail)

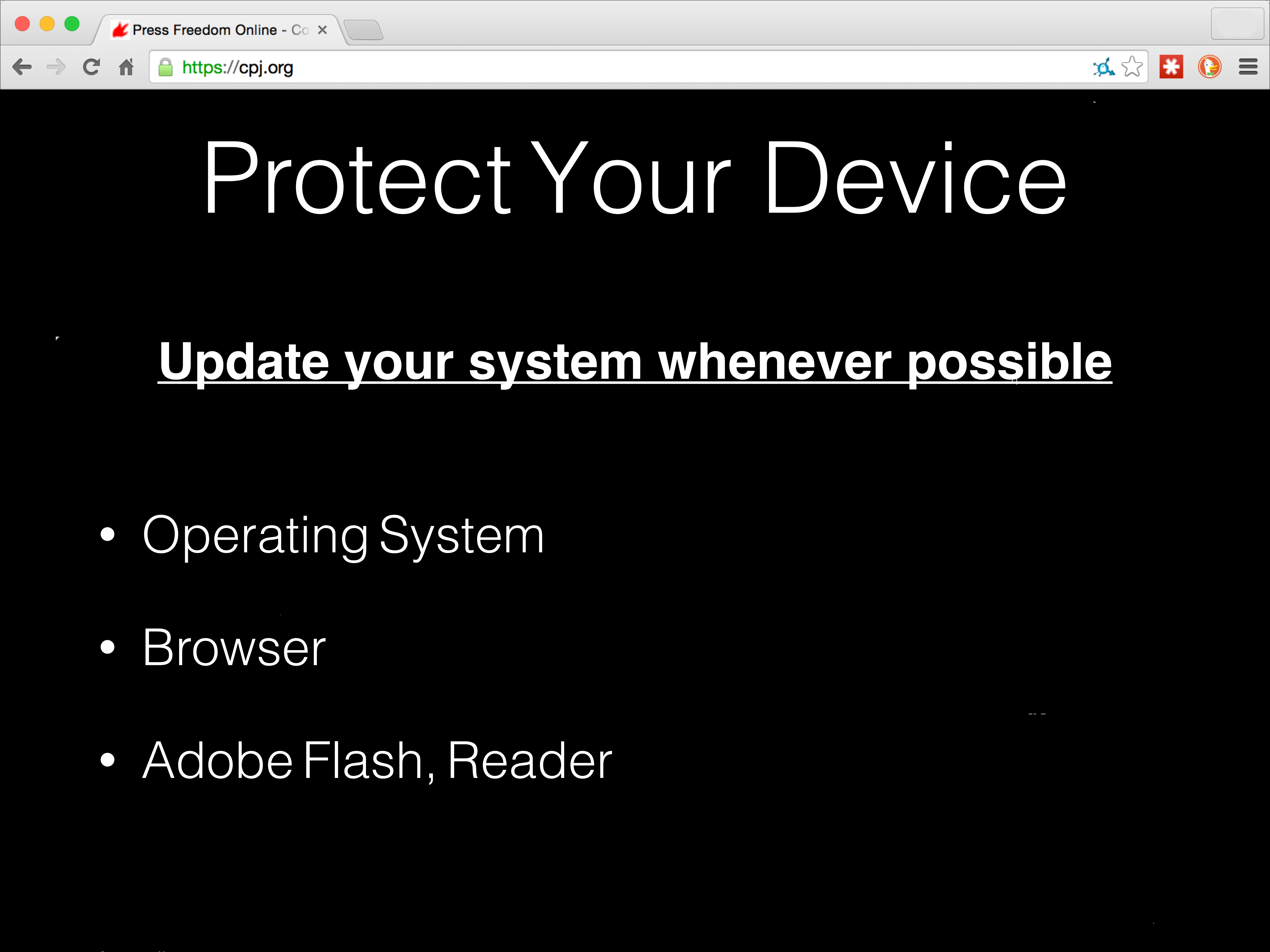
Leonhard Weese February 26, 2015 at 4:06 AM

To: Larry Salibra

Important Document

I just uploaded the document to Google Drive, can you please have a quick look at it? It's kind of urgent.
https://docs.google.com/document/d/1XUuqLuvXyTWsXVdnqFbTbbxH56iL4m2V__WquCpa9VY/edit

https://securesolutionshongkong.com/google/google/drive.php.htm



Protect Your Device

Update your system whenever possible

- Operating System
- Browser
- Adobe Flash, Reader

Protect Your Account

Use a Password Manager

Lastpass

1Password

Protect Your Account

Benefits of a Password Manager

- Only need to remember 1 password: the one for your password manager
- All other passwords are:
    - Stored by your password manager
    - Random & strong like *LE~onD5cY!JD);S$&6*

Protect Your Account

Enable Two-Factor Authentication

- Each time you log in from a new device or a suspicious location you are sent an extra one-time passcode via SMS.
- Offered by Google, Dropbox, Facebook, Apple and many others

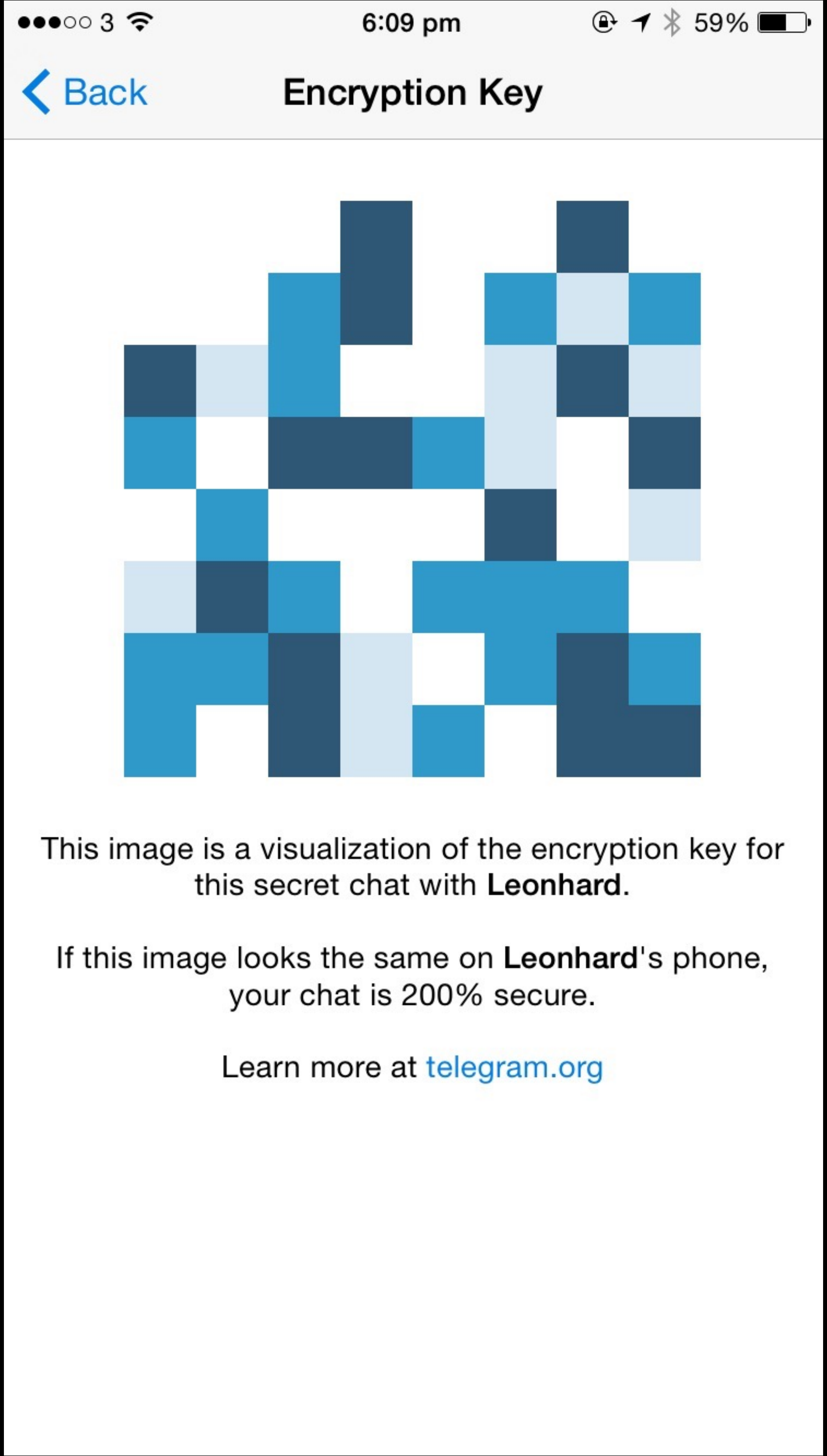
Telegram Privacy Warriors 3 members Media Edit

Protect Your Communications

Protect Your Chats

Telegram

- End-to-end encrypted chats
  (Only between individuals - not groups!)
- Open source
- Verification of keys



Encryption Key

This image is a visualization of the encryption key for this secret chat with **Leonhard**.

If this image looks the same on **Leonhard**'s phone, your chat is 200% secure.

Learn more at telegram.org

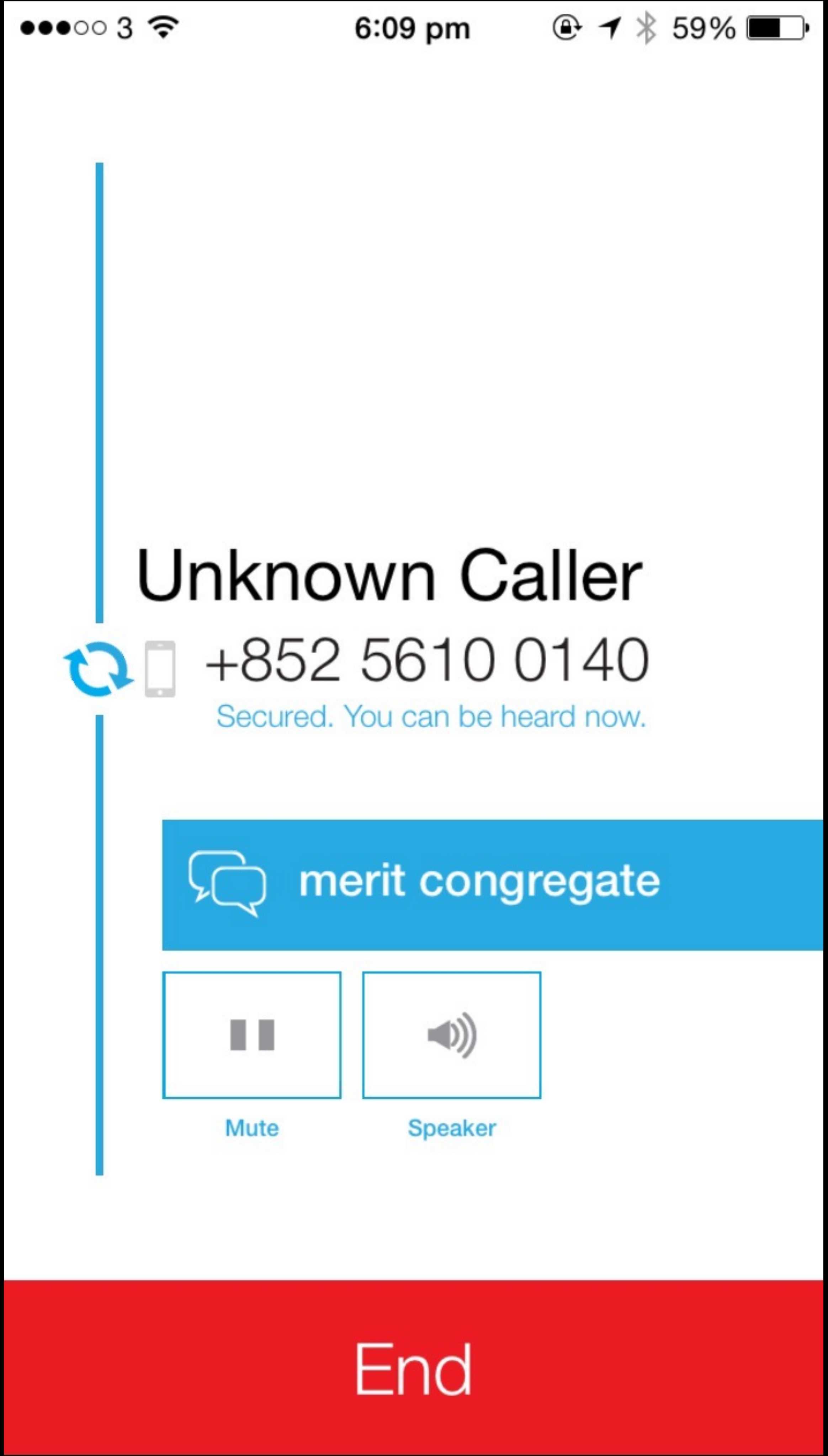
Protect Your Communications

Protect Your Calls

Redphone (Android)

Signal (iPhone)

Open source apps for free encrypted calls



Unknown Caller

+852 5610 0140

Secured. You can be heard now.

“Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it.”

–Edward Snowden

Questions?

+fab

Fabian Lischka

fabian.lischka@me.com

+larry

Larry Salibra

larry@salibra.net

@larrysalibra

+liongrass

Leonhard Weese

leonhard@weese.de

@LeoAW

More info:

https://fabianlischka.github.io/InfoSec101/