Privacy Lecture 1

Digital Footprints and Privacy

Dr Suelette Dreyfus
Department of Computing and Information Systems

I'm teaching you:

- What is privacy? Concepts about digital privacy
  - You are leaving digital footprints
- What is the impact of technology on privacy
  - Difficult to be anonymous or have privacy anymore
  - The State as data-taker
  - Snowden and other revelations
- How to defend end-user privacy - using good security (and how the two are intertwined)
  - Big Five: A hands-on tech sec audit, for those who learn best via kinesthetic learning
  - With some good tools, many of which are free

What is Privacy?

- Cohen: “legal scholarship has conceptualized privacy as a form of protection for the liberal self”
- “Privacy shelters dynamic, emergent subjectivity from the efforts of commercial and government actors to render individuals and communities fixed, transparent, and predictable. “

Julie E. Cohen, ‘What Privacy Is For’, 126 Harv. L. Rev. 1904-1933 (2013).

- What is Privacy? (Cohen cont)
- Invasion of privacy can be “Episodic or systemic”
- “Freedom from Surveillance” needed for “an informed and reflective citizenship”
- Privacy has economic role in innovation: it “shelters the processes of play and experimentation from which innovation emerges.”

- What is Privacy? (Cohen cont)
- Invasion of privacy can be “Episodic or systemic”
- “Freedom from Surveillance” needed for “an informed and reflective citizenship”
- Privacy has economic role in innovation: it “shelters the processes of play and experimentation from which innovation emerges.”

- Important Concepts
  - You're leaving digital footprints
  - It's very difficult to be truly anonymous
  - Anonymity and Privacy are two different but related concepts
    - Anonymity is type of Privacy
  - Privacy and Security are two different things
    - But you need often need security to have privacy.

Privacy

- Anonymity and Privacy need different tools; one is more difficult than the other to get
- Encryption security technologies are good for privacy
- Unless you use strong encryption, you must assume communications are never just between the intended parties.
- End points are the major point of weakness

Who cares about privacy anyway?

- Hands up: how many of you care about privacy?
- What privacy settings do you have on your phone right now?
- To get it, would you spend an extra:
  - 5 min a day? 10 min? 1 hour?
  - Because Privacy, like Security, takes extra effort

THE UNIVERSITY OF MELBOURNE

Who cares about privacy anyway?

Your digital activities are leaving footprints

Your information footprint is not just what you intentionally post online. And it's bigger than you think.

Work habits identify us:

- Curser tracking on websites ("Mouse tracking") without user consent (Mouse movements as proxy for eye tracking)

Metadata identifies you:

- Locational data: happy snaps on your phone?

Your digital activities are leaving footprints

Its not just you or your phone/tablet/device

How many times a week does a friend/family member tag you in photos or mention you in posts that gives away even just some info about you?

Nearby strangers: You could be in the background of someone else's photo – which might be geo-tagged. Then face-recognised by software.

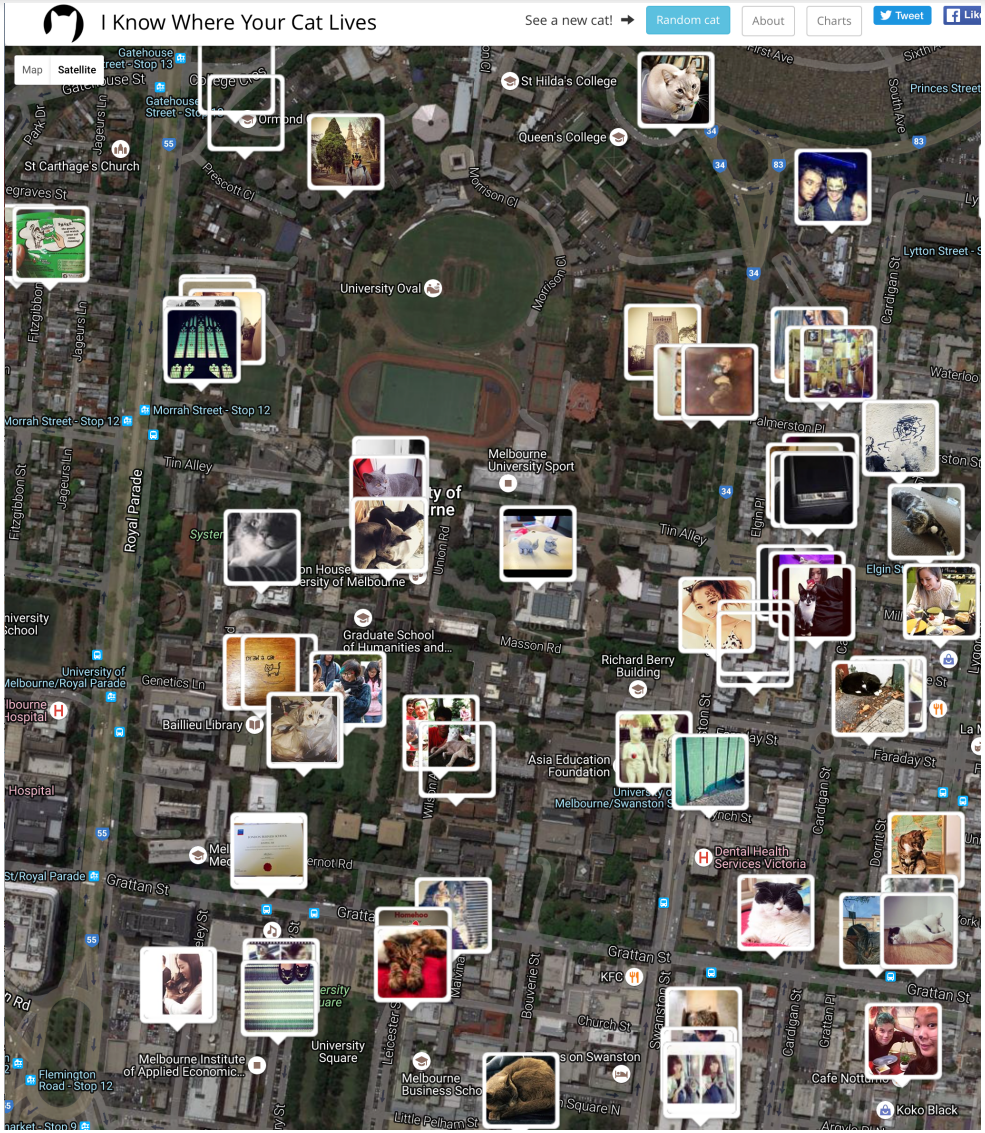
Businesses and services: transactions, how you use their services, - esp credit card

Who here loves cat pics?

Your digital activities are leaving footprints

I know where your cat lives

- a data experiment that visualizes a sample of 1 million public pics of cats on world map,
- locating them by the latitude and longitude coordinates embedded in their *metadata*



Your footprints: Phones

Chatterbox..

Inside TAO: Documents Reveal Top NSA Hacking Unit

By SPIEGEL Staff

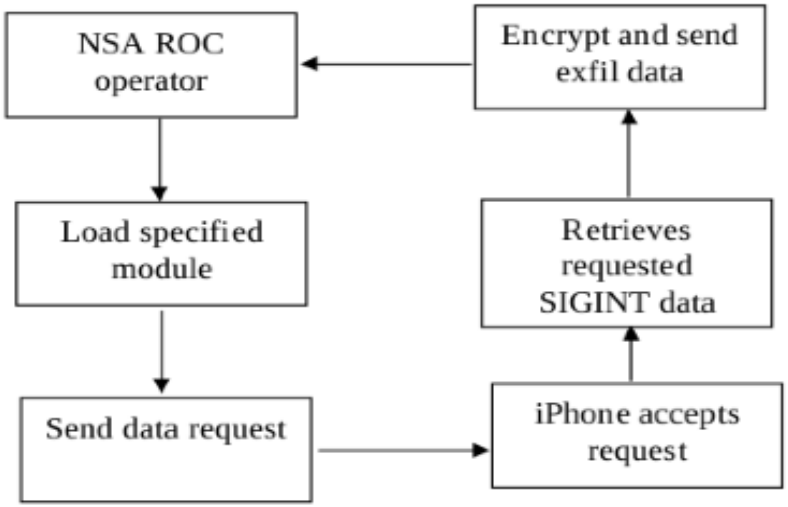
Google Earth

The NSA's TAO hacking unit is considered to be the intelligence agency's top secret weapon. It maintains its own covert network, infiltrates computers around the world and even intercepts shipping deliveries to plant back doors in electronics ordered by those it is targeting.

THE UNIVERSITY OF MELBOURNE

Your footprints: You can just turn off your phone, right?

(TS//SI//REL) DROPOUTJEEP is a STRAITBIZARRE based software implant for the Apple iPhone operating system and uses the CHIMNEYPOOL framework. DROPOUTJEEP is compliant with the FREEFLOW project, therefore it is supported in the TURBULENCE architecture.



(U//FOUO) DROPOUTJEEP – Operational Schematic

(TS//SI//REL) DROPOUTJEEP is a software implant for the Apple iPhone that utilizes modular mission applications to provide specific SIGINT functionality. This functionality includes the ability to remotely push/pull files from the device, SMS retrieval, contact list retrieval, voicemail, geolocation, hot mic, camera capture, cell tower location, etc. Command, control, and data exfiltration can occur over SMS messaging or a GPRS data connection. All communications with the implant will be covert and encrypted.

INCREASING GOVT SURVEILLANCE OF THE MEDIA VIA PHONES

Real Life Case Study: US Govt spied on AP newsroom

"The Justice Department secretly obtained two months of telephone records of reporters and editors for AP in what the news cooperative's top executive called a 'massive and unprecedented intrusion' into how news organizations gather the news."

– AP, 14 May 2013

"More than 100 journalists work in the offices where phone records were targeted, on a wide array of stories about government and other matters."

Your footprints: Phones – Metadata chase

Paul Farrell
The Guardian- AU

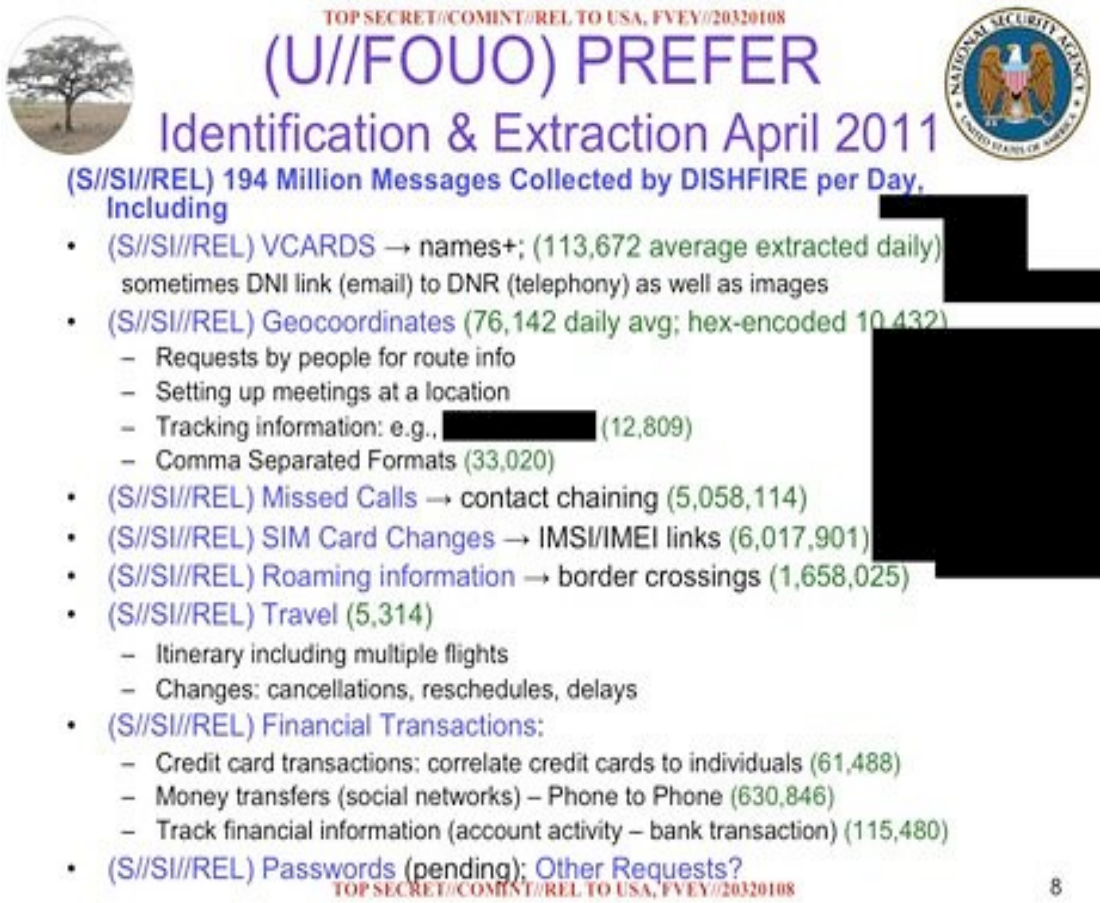
Not just breadth – but DEPTH of spying on journalists

February 2016

200 pages of police files – FOI'ed, heavily redacted ..
The AFP INVESTIGATED HIM TO FIND HIS SOURCE

Your footprints: Phones

DISHFIRE: NSA collected almost 200 million SMS' a day across the globe, to extract data incl location, contact networks & CC details



Practical Ways to Improve Privacy

- Periodically check privacy settings and update them, if possible, to limit unintentional information sharing.
- Particularly on mobile apps, online accounts, other software
- Turn off settings that share information, such as locational data and contacts, that is unnecessary for the service/use

This kind of simple advice is useful in a personal and a business setting. For example, you may not want industry competitors knowing where your sales reps are located if it's a client they are trying to steal away from the competitor.

2. It's very difficult to be truly anonymous

There are technical reasons and state-based (policy) reasons.

Technical:

- Your IP address is transmitted *
- Your browser's transmitted information about the browsers config to the website server:
  - http://useragentstring.com
- Browser history (Cookies anyone?)
- Cloud services, drop boxes may have data users think are long gone; simply out of site
- Case study of Paula Broadwell and Gen Petraeus

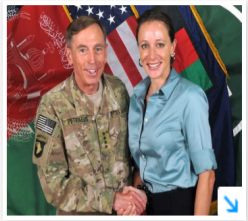
Case Study:

Gen David Petraeus and Paula Broadwell communications are discovered by capture of Broadwell's IP address

Petraeus and Broadwell used commo

Donna Leinwand Leger and Yamiche Alcindor USA TODAY 9:40 p.m. EST November 13, 2012

The FBI is wise to many of the tricks used by terrorists and others to hide email trails



(Photo: Handout Getty Images)

STORY HIGHLIGHTS

- Some messages were composed using a "drop box"
- Thousands of pages of e-mails are under investigation

Paula Broadwell, ex-mistress of former CIA chief David Petraeus, could have used several methods to hide her identity if she sent anonymous, threatening e-mails to Tampa socialite Jill Kelley, experts say.

But the FBI has many techniques available to trace such communications, said Shawn Henry, who retired in March as the FBI's executive assistant director in charge of all civil and criminal cyber investigation.

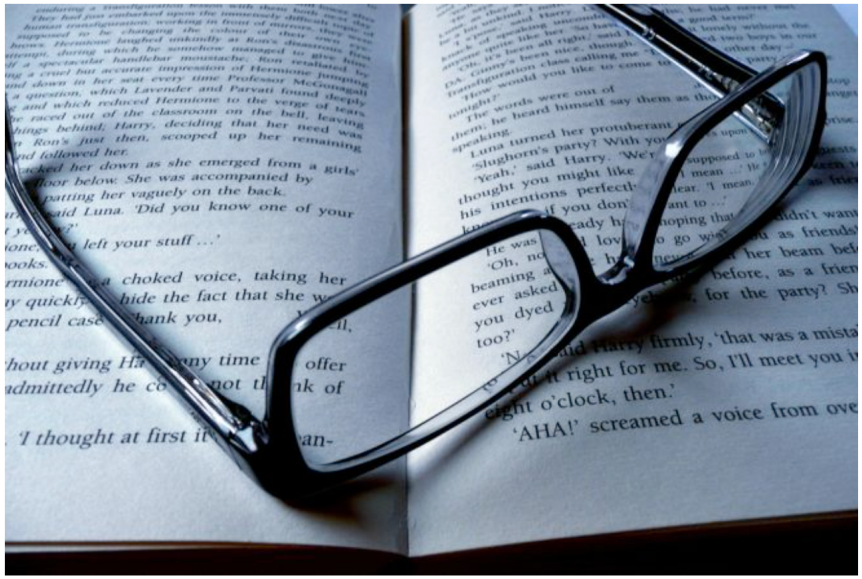
"Somewhere along the way, her IP address was captured," Henry said. An IP address, or internet protocol address, is a string of numbers unique to a particular computer or device on the internet. With it, authorities can usually track the identity of the person who sent an e-mail or visited a website.

Source: Leger, DL, & Alcindor, Y 2012. 'Petraeus and Broadwell used common email trick', *USA Today*, 13 Nov. See: http://www.usatoday.com/story/tech/2012/11/13/petraeus-broadwell-email/1702057/

It's difficult to be truly anonymous

Technical (Cont)

- Data Mining, and inference techniques (facial recognition, activity modeling, speaker identification)



BY PHOTOSTEVE101, VIA FLICKR

ONLY HUMAN *A Blog by Virginia Hughes*

How Forensic Linguistics Outed J.K. Rowling (Not to Mention James Madison, Barack Obama, and the Rest of Us)

Source: Hughes, Virginia 2013. *National Geographic*, 19 Jul. See: http://phenomena.nationalgeographic.com/2013/07/19/how-forensic-linguistics-outed-j-k-rowling-not-to-mention-james-madison-barack-obama-and-the-rest-of-us/

It's very difficult to be truly anonymous (Cont)

The State may have designed deliberate policy enforcement mechanisms to remove your anonymity. Example:

- Mobile Phones
- No anonymous phone calls
- No anonymous text messages

Not true in every country. But some countries are considering going further – case study: Thailand.

Thailand: "Foreigners ..Required to Use tracking SIM Cards"

"Telecom .. approved in principle a requirement that foreign visitors to Thailand use special SIM cards in their phones that can be tracked by the authorities.."
"..the National Broadcasting and Telecommunications Commission (NBTC), said the resolution was in the interests of national security.."
"Mobile operators can preset some technical features in SIM cards to ensure that they can always locate users, who will be unable to turn off the function"

Sources*: The Bangkok Post*, 9 Aug 2016. See:
http://www.bangkokpost.com/news/security/1057061/foreigners-to-be-required-to-use-tracking-sim-cards
The Bangkok Post, 10 Aug 2016. See:
http://www.bangkokpost.com/news/general/1057913

Practices to Deal with Anonymity Issues

1. Assume you have less anonymity, and therefore less privacy, when you're doing something electronically than you would if you were doing it non-electronically

2. Only give out as much personal information as you have to. Ask yourself what they need it for. Either:

- Don't give them the information;
- Give them made-up information;* or
- Choose some other way of getting that service.
- *But stay within legal bounds

3. **Use Tools that reduce Websites ability to track you**

Big Five – Security Audit

1. Patch!
   - All your OS' and Applications must be up to date, fully patched.
2. Use strong, unique passwords:
   - Use a password manager. These are a few: 1Password, LastPass, Keepass (open source password manager), Dashlane
   - Or otherwise find a way to have strong, unique passwords for EACH account
3. Encrypt data at rest:
   - Bitlocker; File Vault 2, Luks
4. Encrypt data in transit (i.e. avoid POTS, SMS; prefer encrypted IM like Signal, WhatsApp, Viber)
5. Enable mfa (multi-factor authentication); preferably using OTP-generating smartphone

Running a Big Five – Security Audit

1. Is your buddy's OS on phone and laptop running the latest greatest software? (fully patched)
    1. Check it now on laptop. Write down what they are running.
    2. Now check – can it be updated?
    3. Now check their phone. Not updated? Write it down.
        - running anything less than Android 7 or iOS 10.3.2, get it updated
    4. Now check their most common App – say, Office on laptops
    5. Now check the settings for updates on their phone and laptop.
    6. Who has updates to do? Make a LIST
    7. Red stickits – Green stickits exercise in class

Use strong, unique passwords:

- How many of you have a unique password for each account?
- How many have a password of more than 4 digits for your phone?
- How many of you use a password Manager?
- Some of many possibilities:
  - Last Pass, 1Password, KeePass

Passwords

The Hacker News™
Security in a serious way

Facebook CEO Zuckerberg's Twitter, Pinterest accounts Hacked! And the Password was...

Sunday, June 05, 2016 Mohit Kumar

G+1 124 Like 10K 19.1K 2218 203 21.7K

The man who runs the biggest social network and continuously implements new security measures to boost its billion users security, himself failed to follow basics of Internet security for his own online accounts.

Yes, I'm talking about Facebook CEO Mark Zuckerberg, who had his Twitter and Pinterest accounts compromised on Sunday.

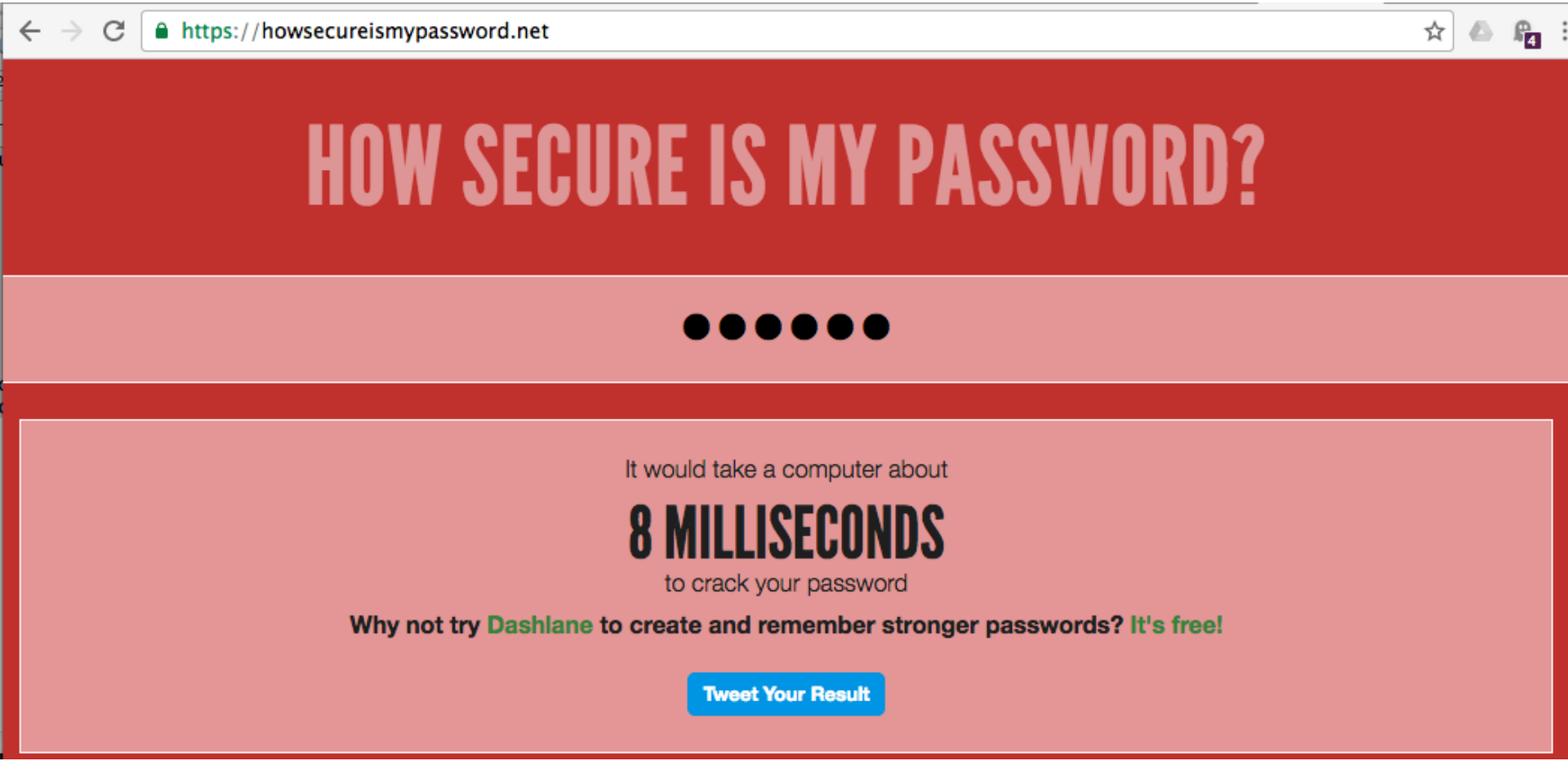
The hacker group from Saudi Arabia, dubbed **OurMine**, claimed responsibility for the hack and guess how the group did it?

June 2016: Hackers used the account credentials from the Linked In data breach. Zuckerberg had re-used his password. They penetrated his Twitter and Pinterest accounts.

- Don't reuse passwords
- Choose secure passwords (not 'dadada'!)
- Consider a password manager

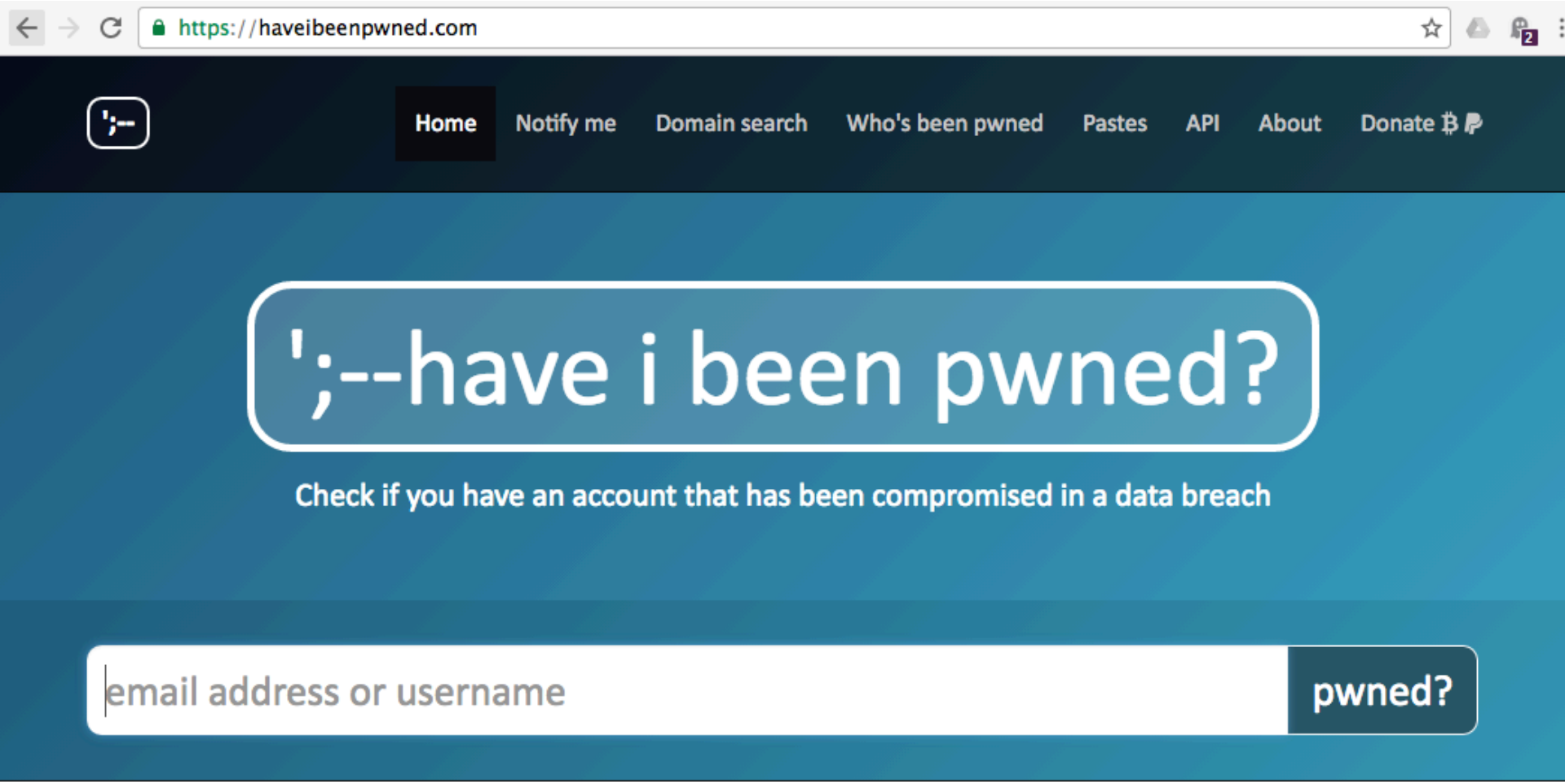
Are you serious about password security?

A 2013 survey by Deloitte found that 90% of user-generated passwords should be considered vulnerable to hacking.



Passwords: Ever used LinkedIn?

Well, you might have been pwned. Test it.

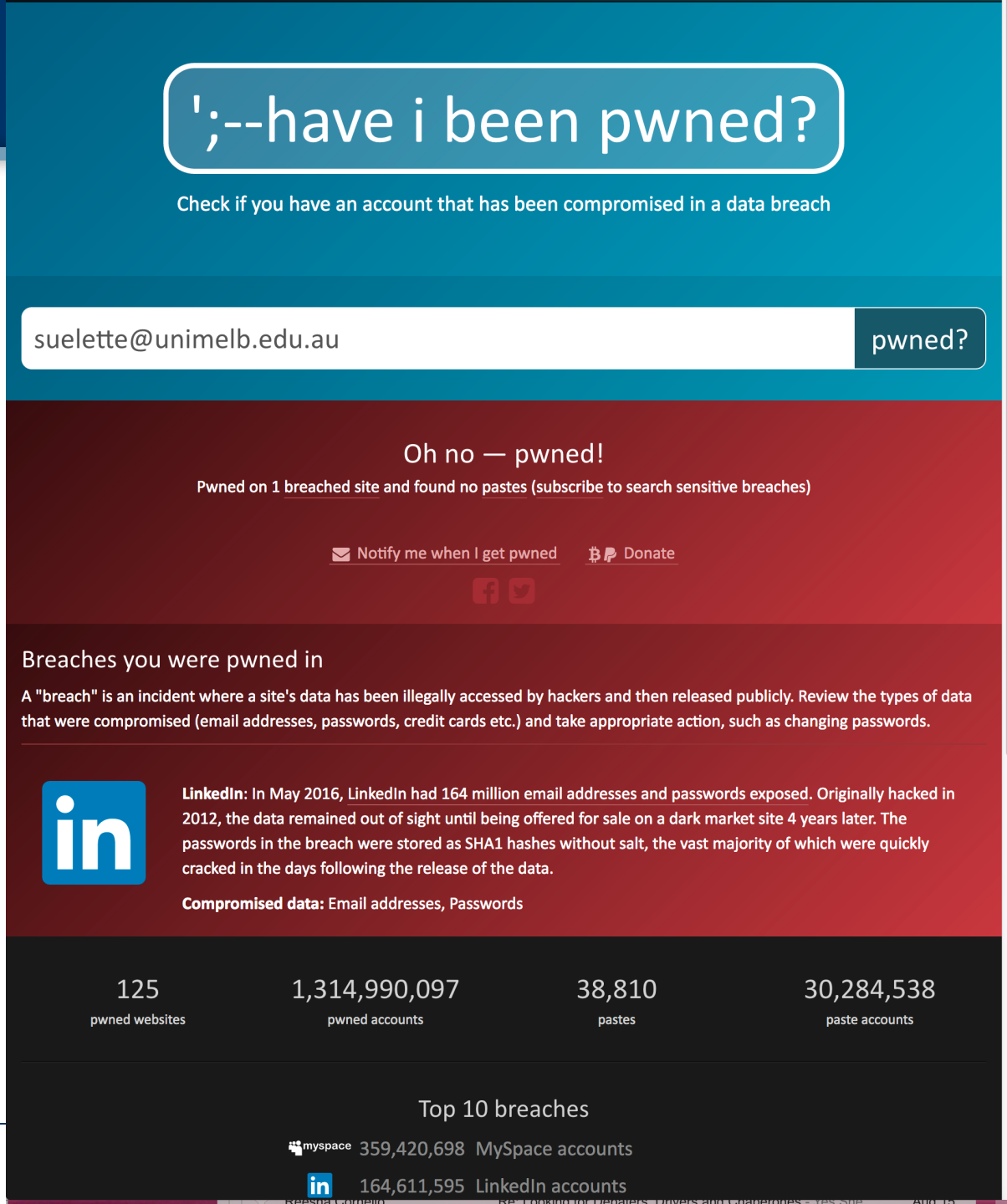


THE UNIVERSITY OF MELBOURNE

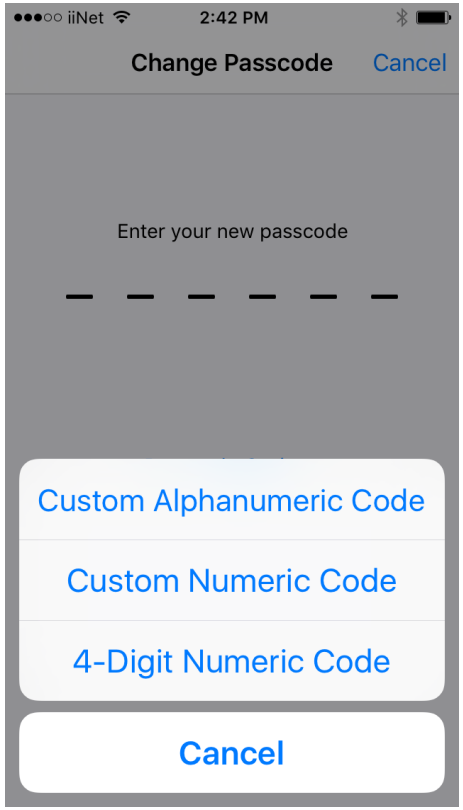
Think you are too smart?

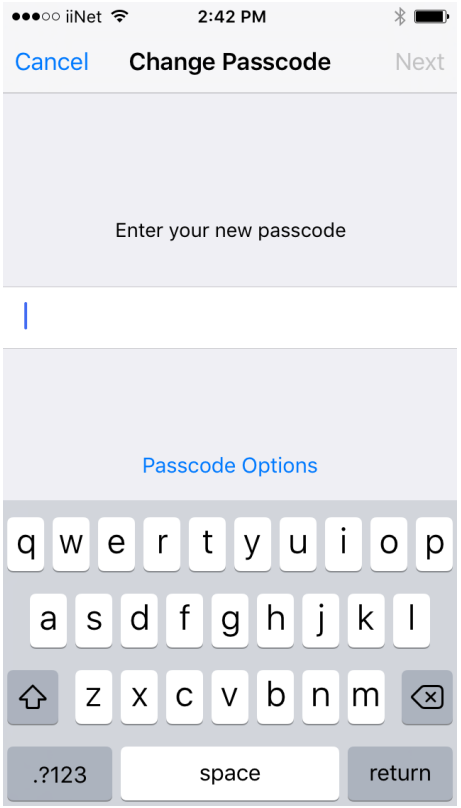
Can't get owned?

Think again.



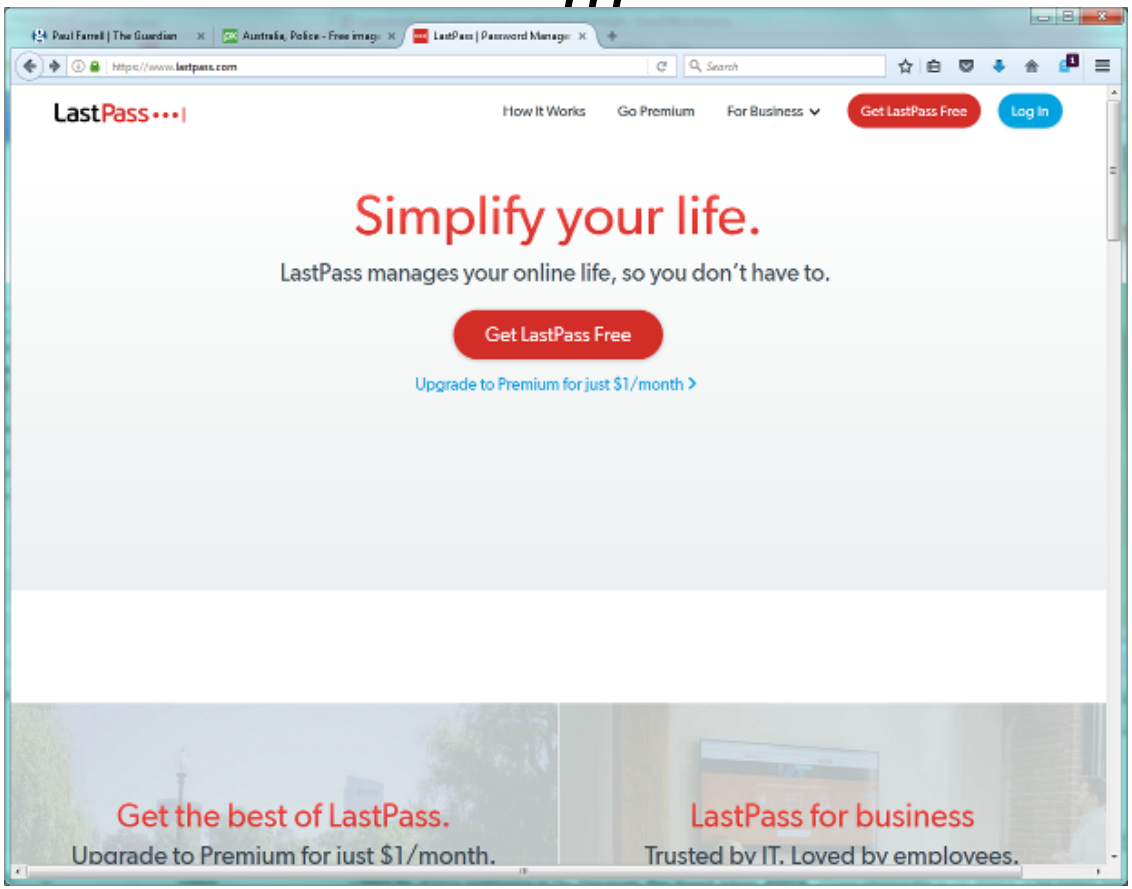
Password protect iPhone: use alphanumeric





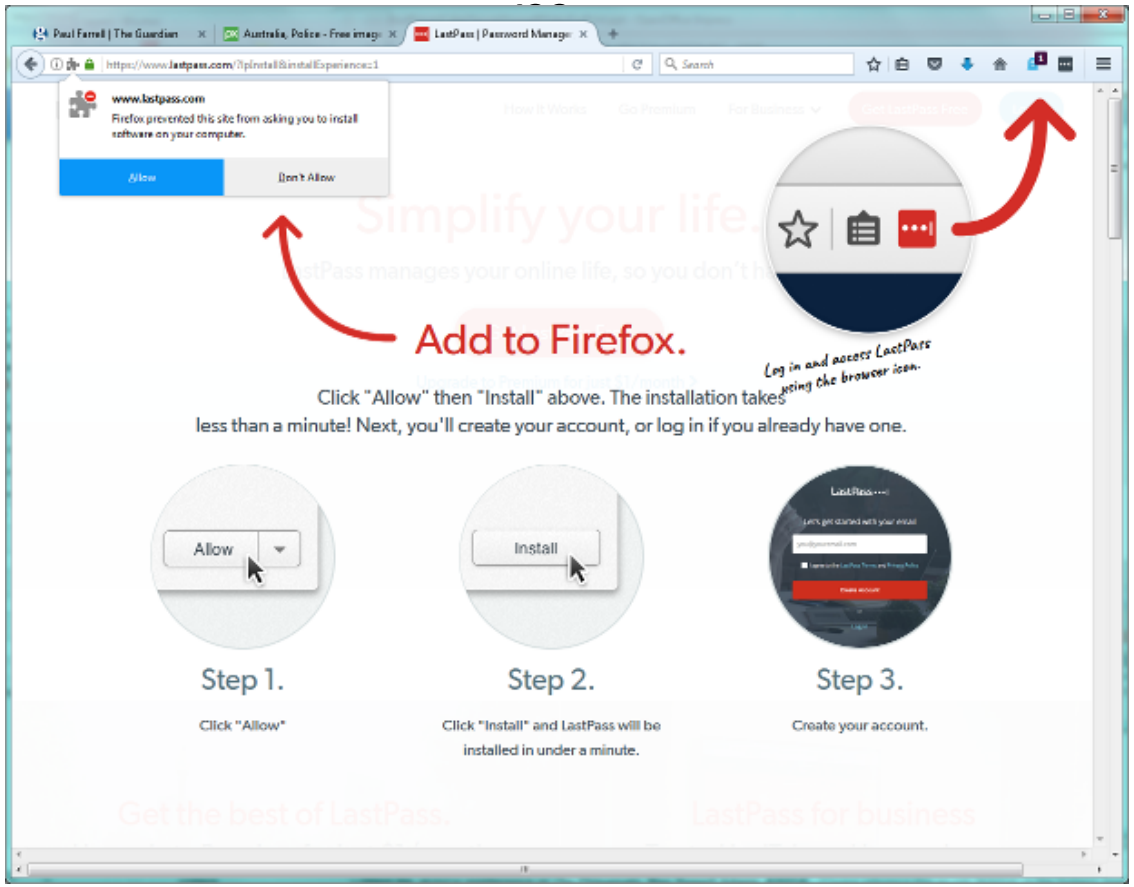
Managing Passwords in LastPass

www.lastpass.com



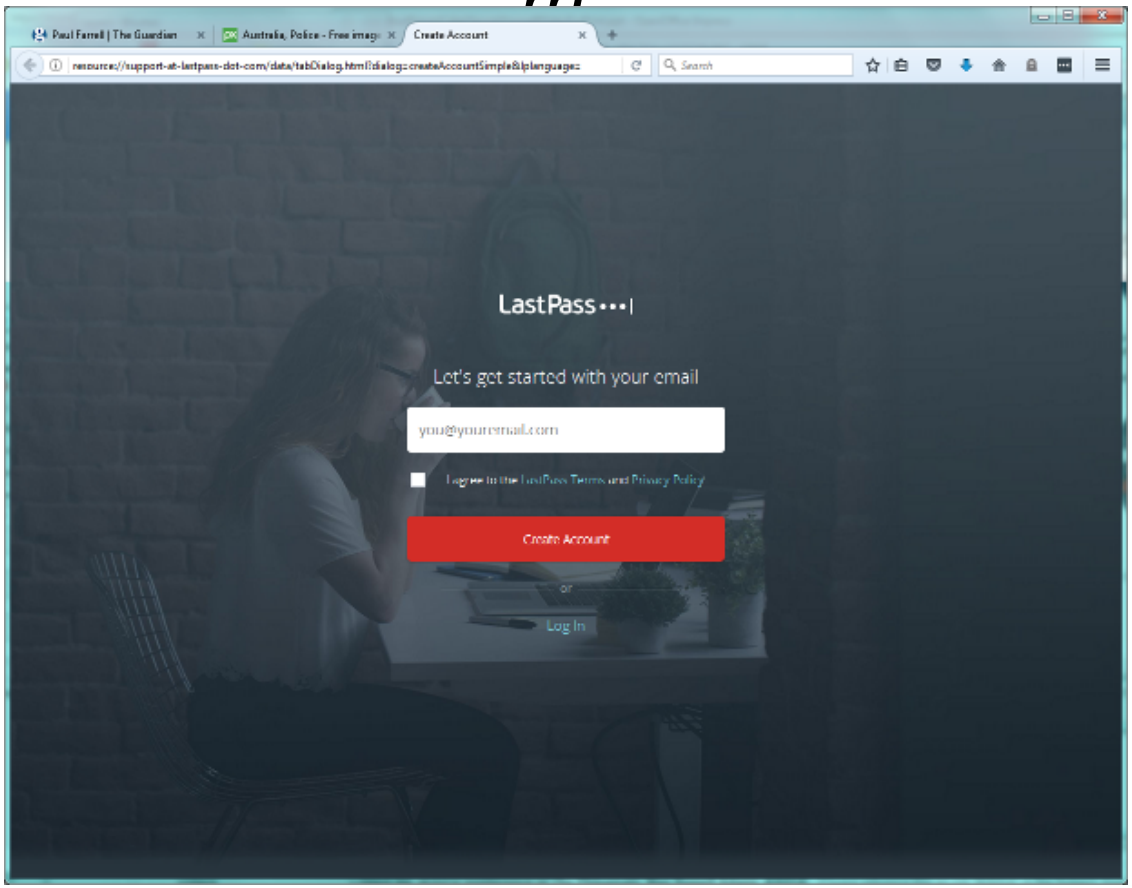
Managing Passwords in LastPass

www.lastpass.co



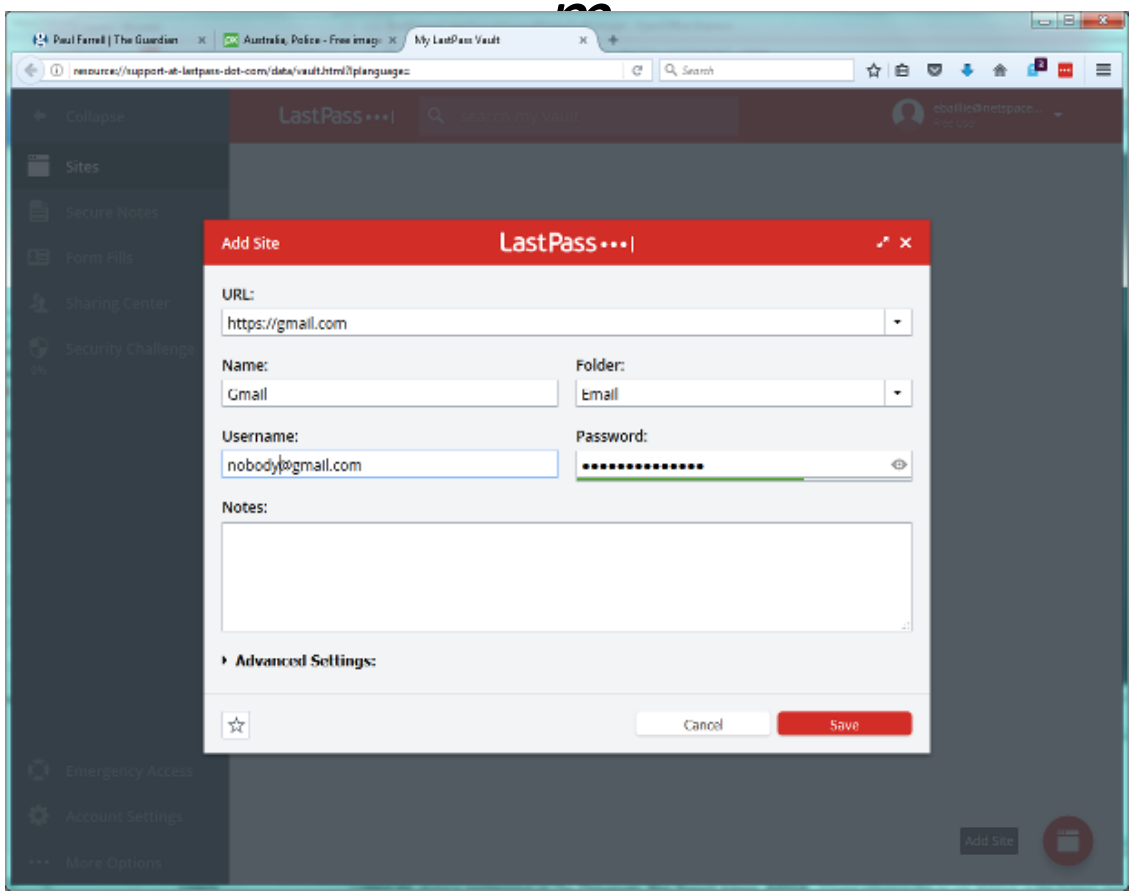
Managing Passwords in LastPass

www.lastpass.com



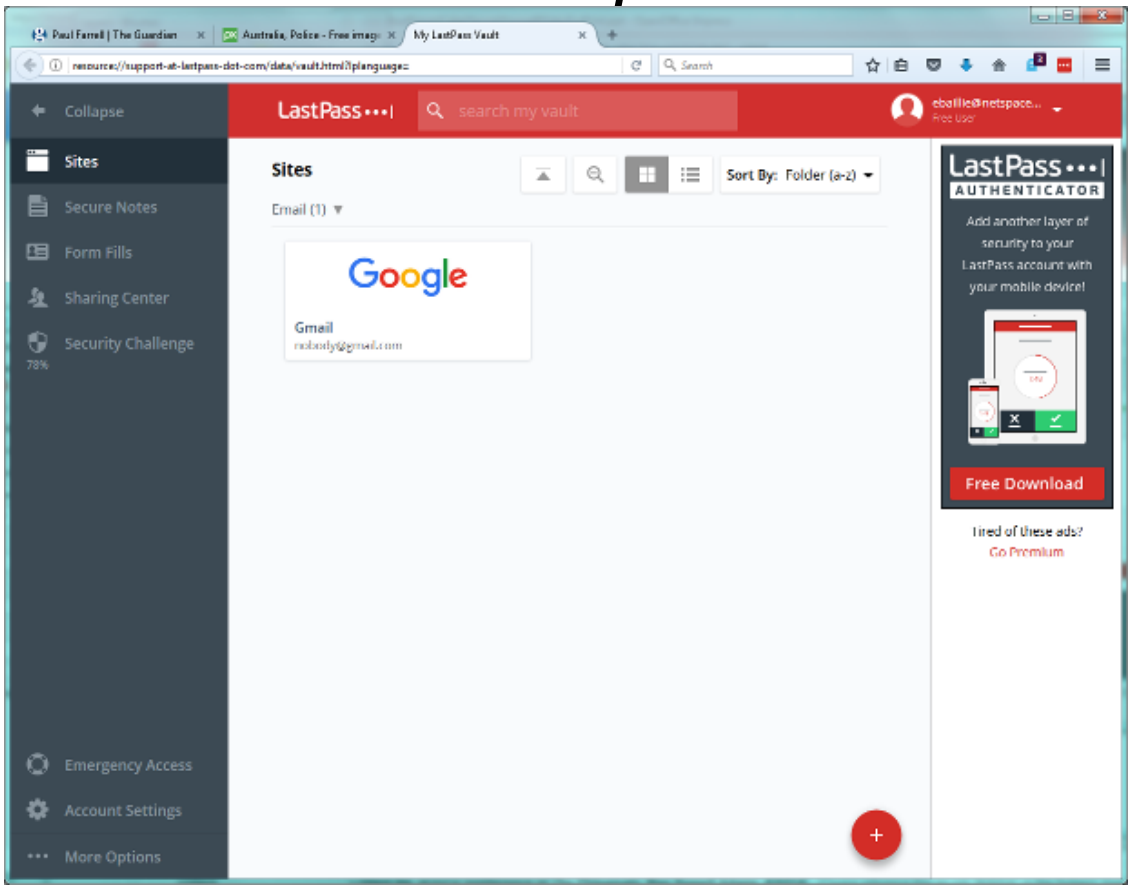
Managing Passwords in LastPass

www.lastpass.com

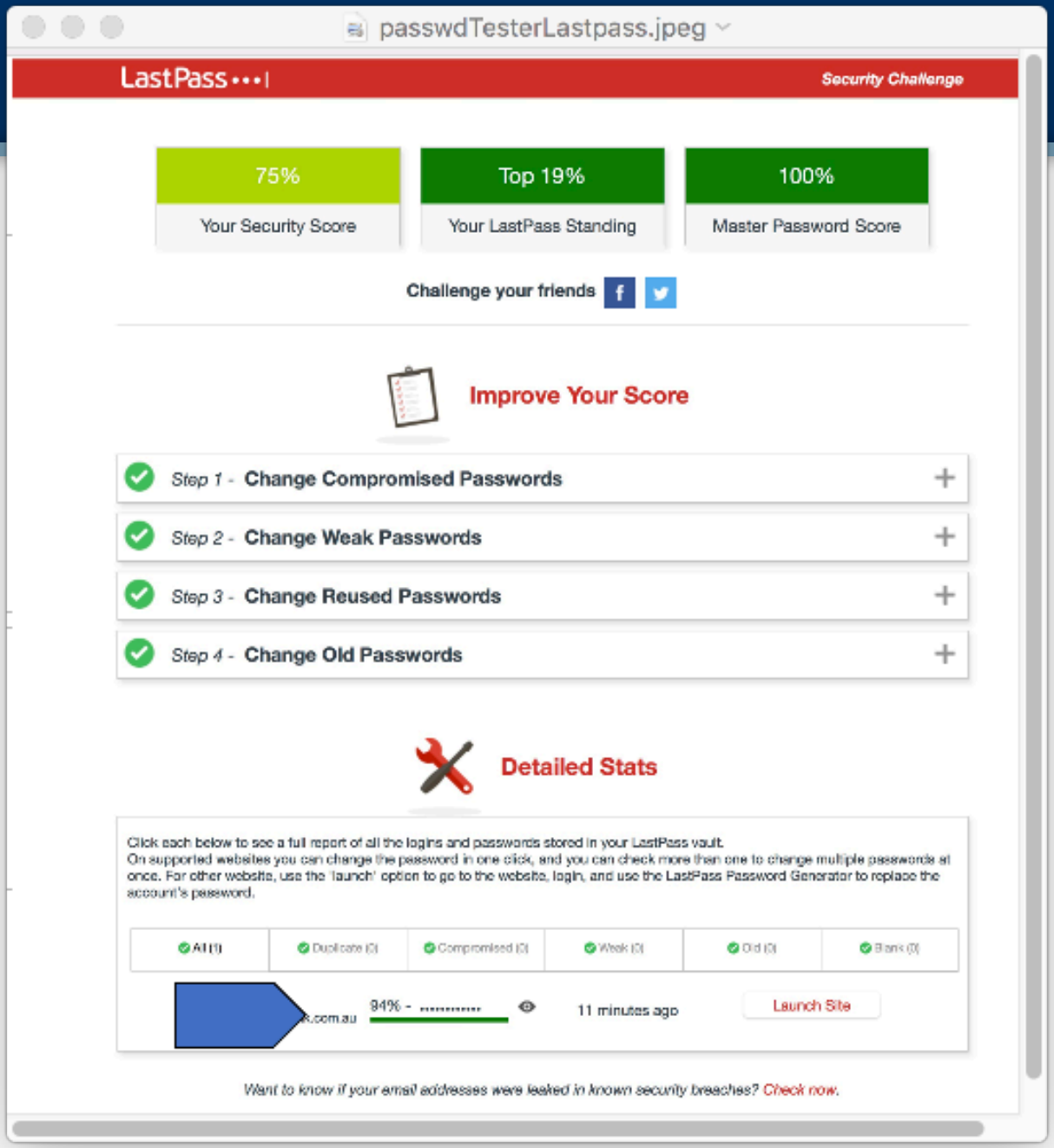


Managing Passwords in LastPass

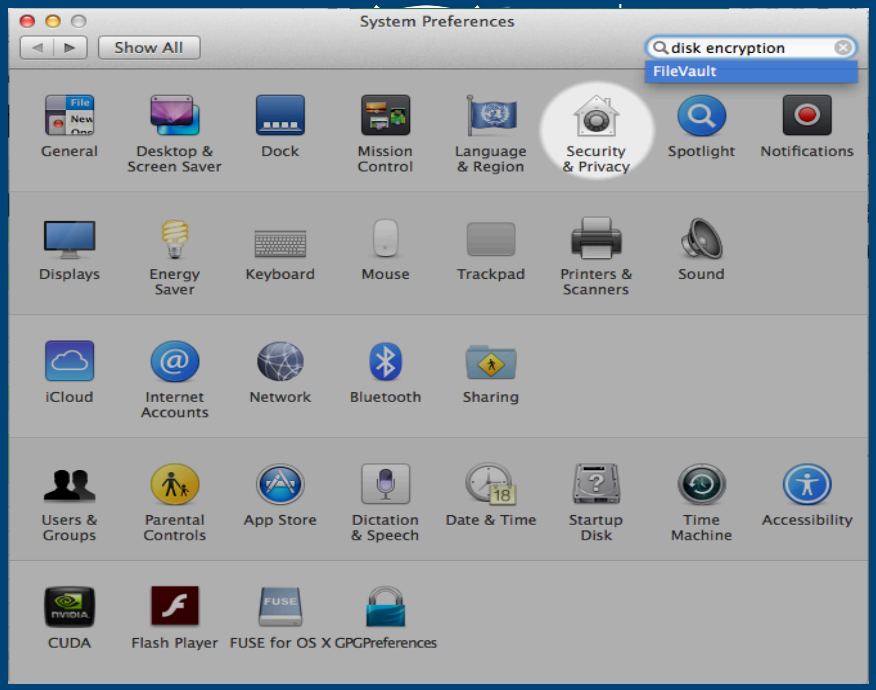
www.lastpass.com

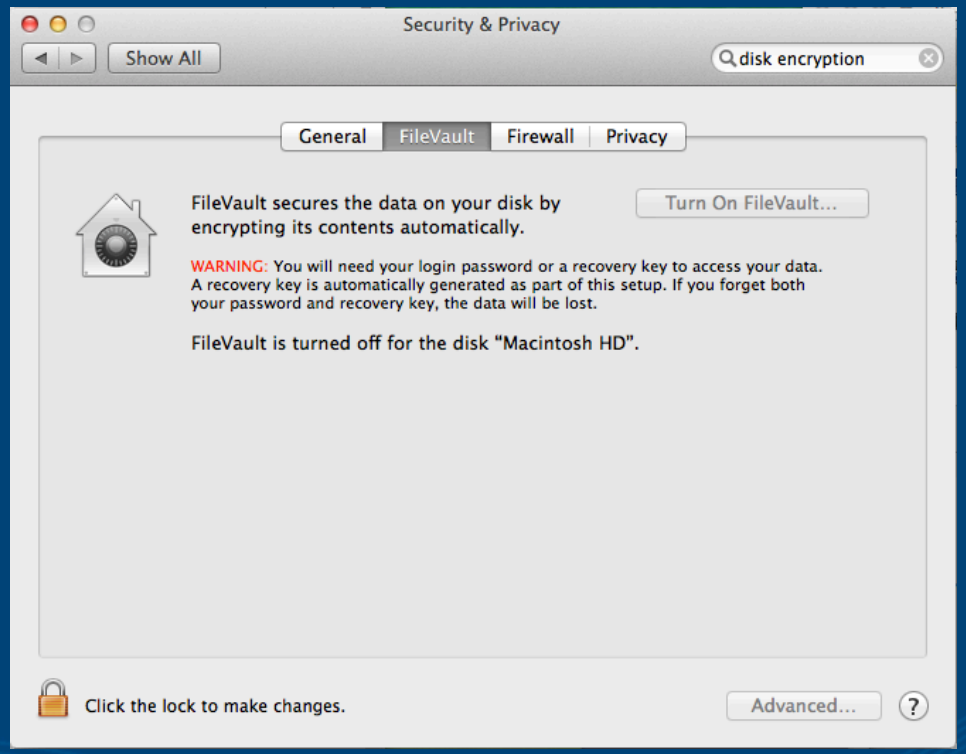


LastPass Password Strength Tester



Encrypt data at rest





Bitlocker; FileVault.
You need Win 10 Pro to get Bitlocker included.

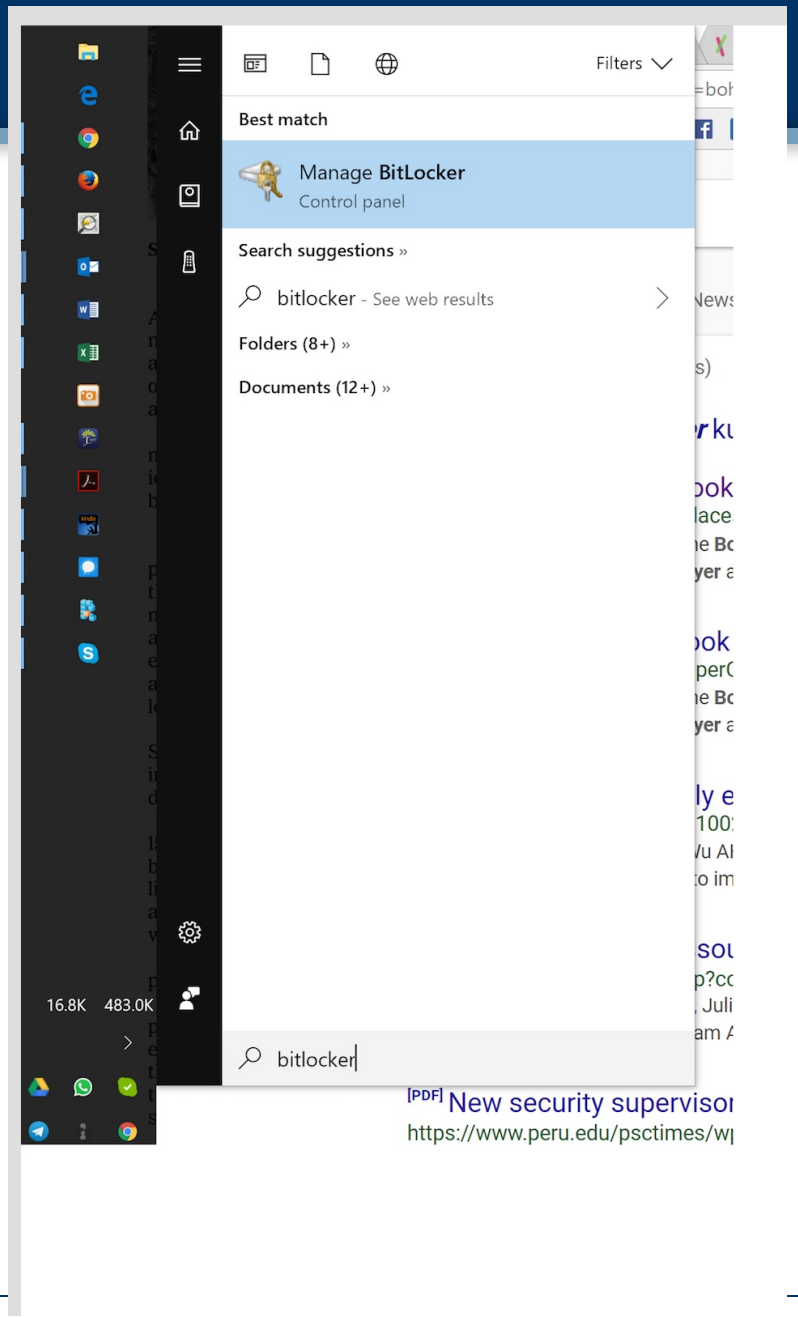
Win 10BitLocker

Step by Step

1) hit the "window" key
2) type: bitlocker
3) when "manage bitlocker" resolves to the control panel (the picture of a hard drive overload with keys on a keyring), then hit Enter

   if you don't have Pro, then in step 3, what you typed won't resolve to a control panel at all; i.e. you'll just be missing that control panel, in toto

4) you'll see the "old-style windows control panel" with pictures of all your hard drives. select your operating-system hard drive and click "enable protection," and off you go.
5) if your OS says "oh, wait, sorry; I can't do that for you--your PC lacks TPM", check on Google search how to solve this.



Handle the Cloud with care

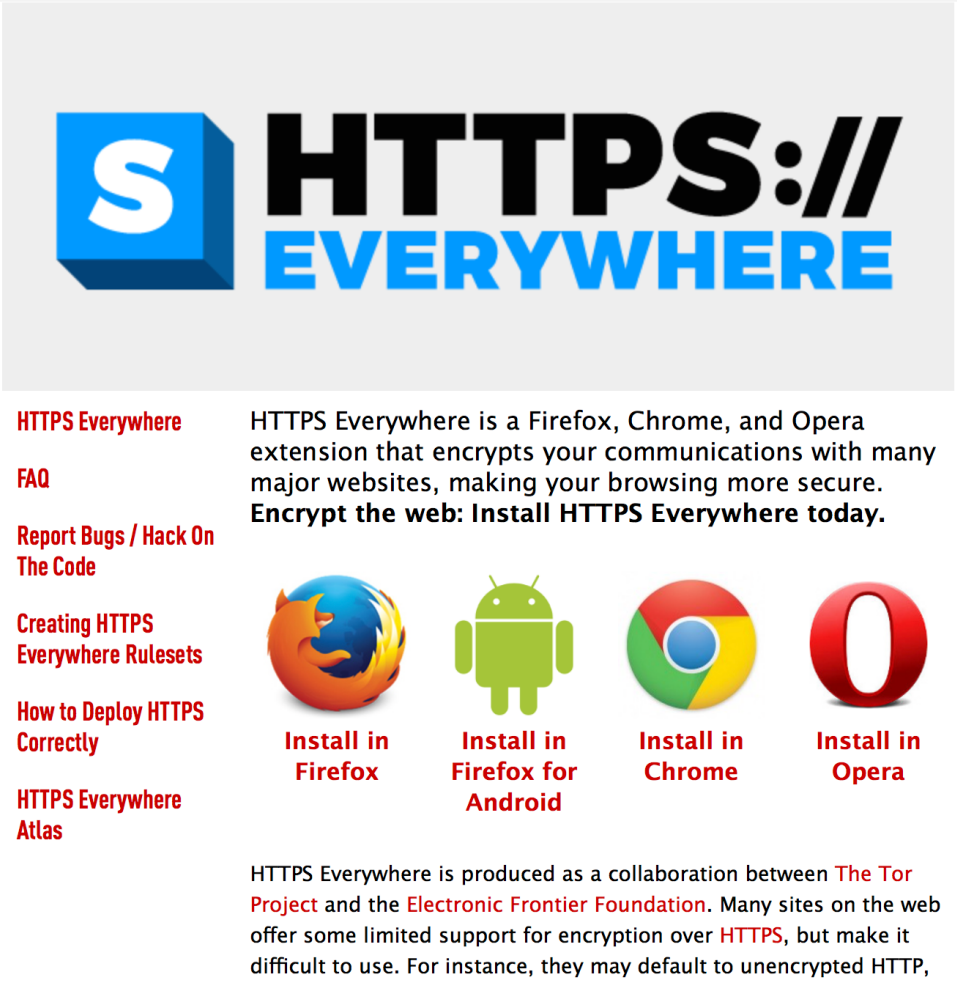
- Encrypt in your cloud storage
- Encryption should occur on YOUR Devices (not in the cloud – or else what's the point?)
- Useful for being 'clean' crossing borders
- An option: SpiderOak's 'ONE' product $5USD p/m
-

SpiderOak

Encrypt data in Transit

HTPPS Everywhere

- An extension for Firefox, Chrome, Opera that encrypts comms with many major websites
- Overcomes problems of a site using default of plaintext



https://www.eff.org/https-everywhere

Encrypt data in Transit: what Encrypted message system?

End-to-end encrypted, audited

Signal,FB Messenger,WhatsApp,Wickr,Ricochet

E2E,but not audited

Viber, Telegram, Line, Allo, Wire

User-to-server encrypted

Skype, Google Hangouts

U2S, dodgy owner

WeChat

Vulnerable

SMS
POTS

More Secure Phones: Signal

Secure messaging and voice calls.

Free and Open Source Software, anyone can audit the code for correctness or help contribute improvements.

End to End Encrypted, can send txt, pics, video msgs, and talk voice over it. But not documents. Yet.

It uses data connection not phone. Both people need to have internet access on phone. (But no SMS or MMS Fees!)

It offers privacy (encryption) but NOT anonymity.

signal

Steps:

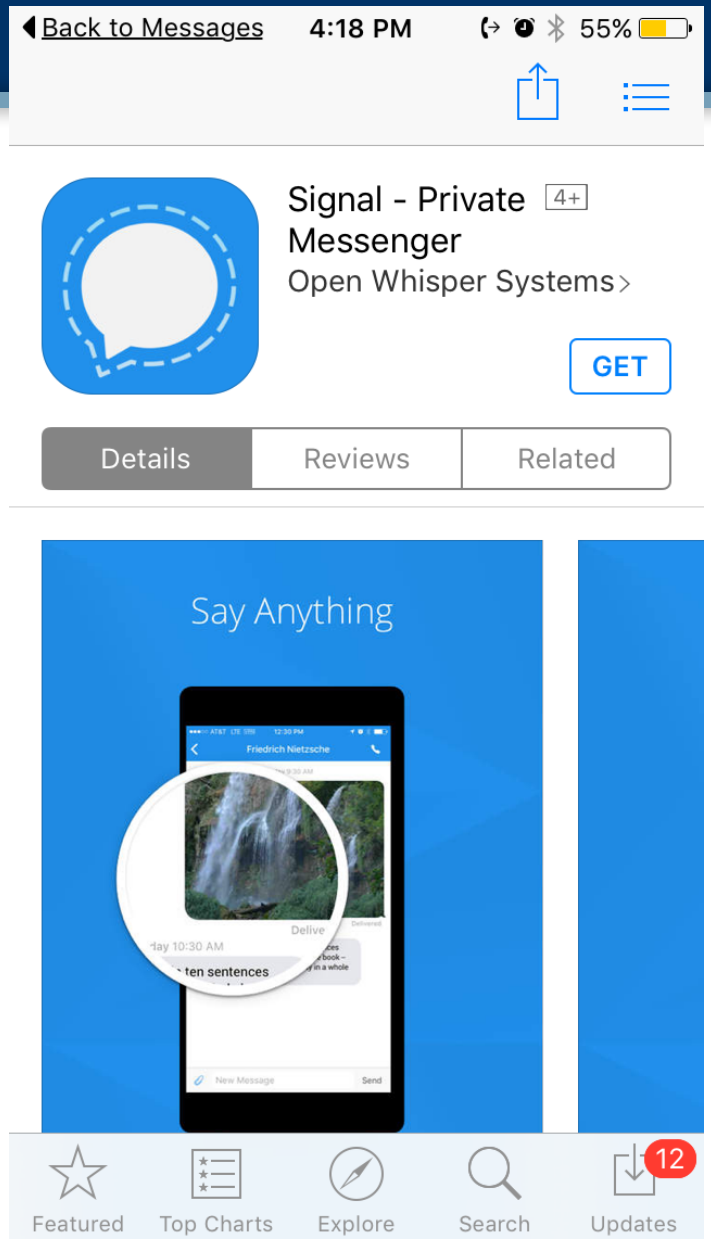
Find a buddy: share phone numbers

Open your App store in your smartphone

Search: Signal Private Messenger (by Whisper Open Systems)

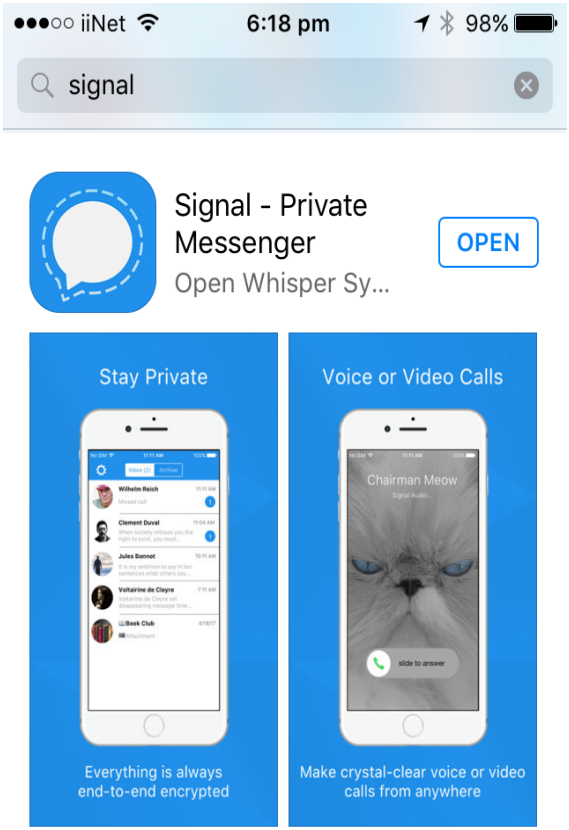
Be sure you get the right App!

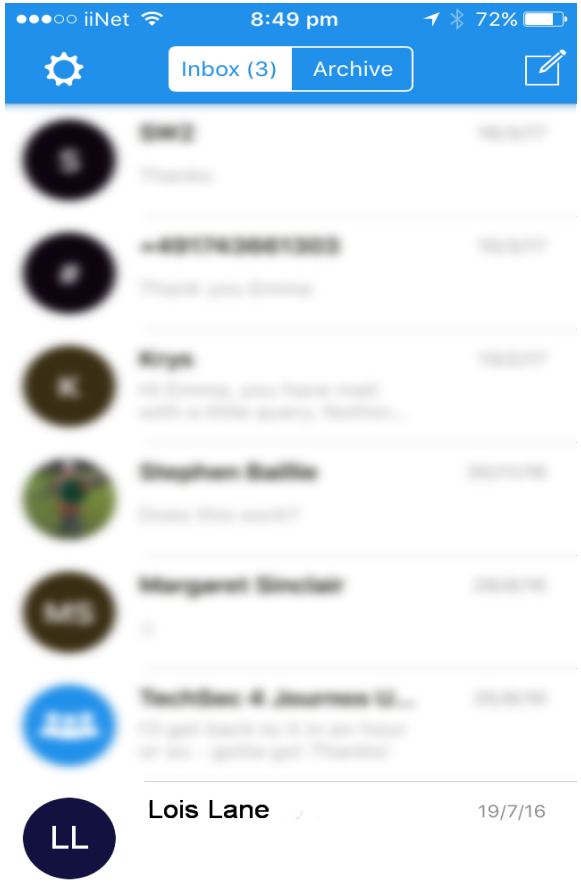
Download
Open



THE UNIVERSITY OF MELBOURNE

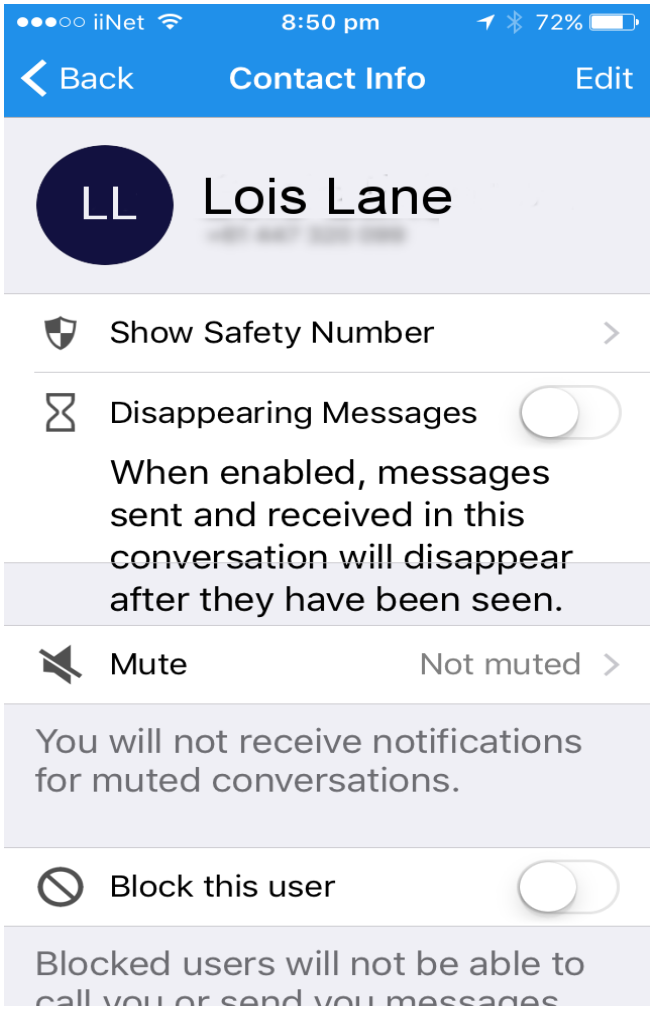
Signal



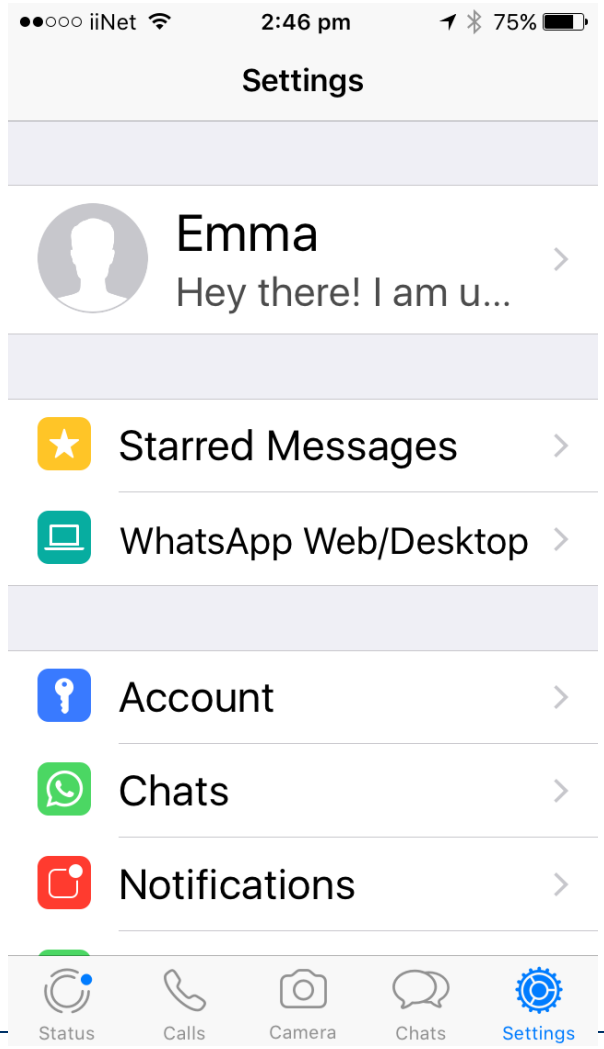


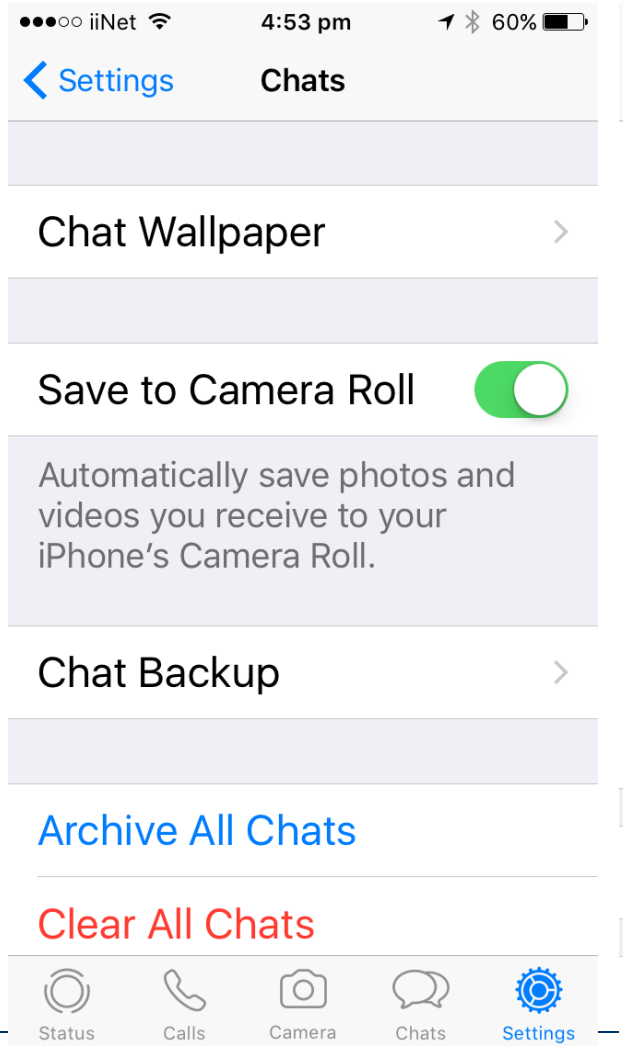
THE UNIVERSITY OF MELBOURNE

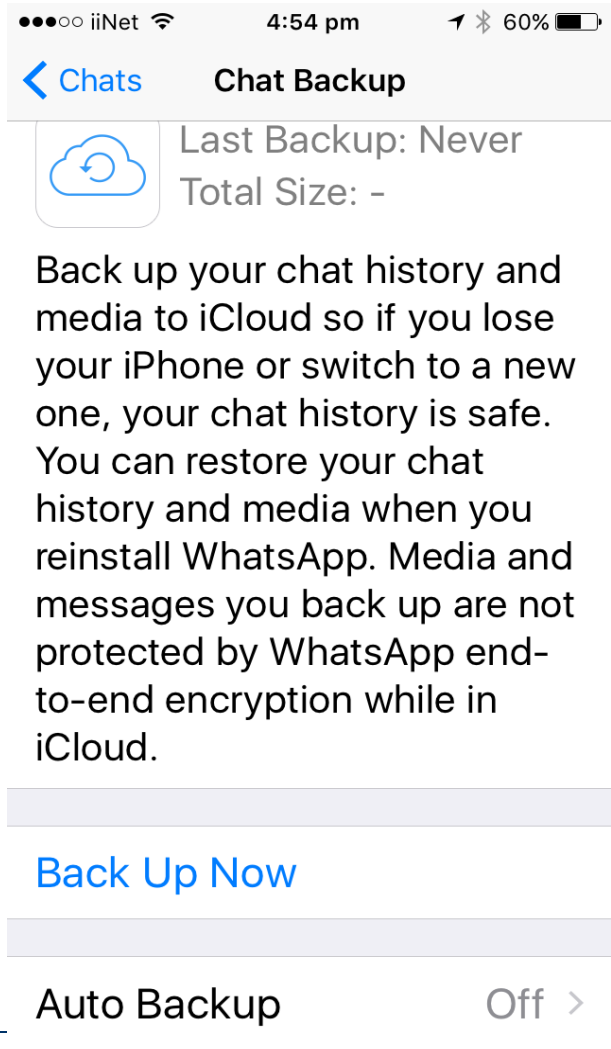
Signal



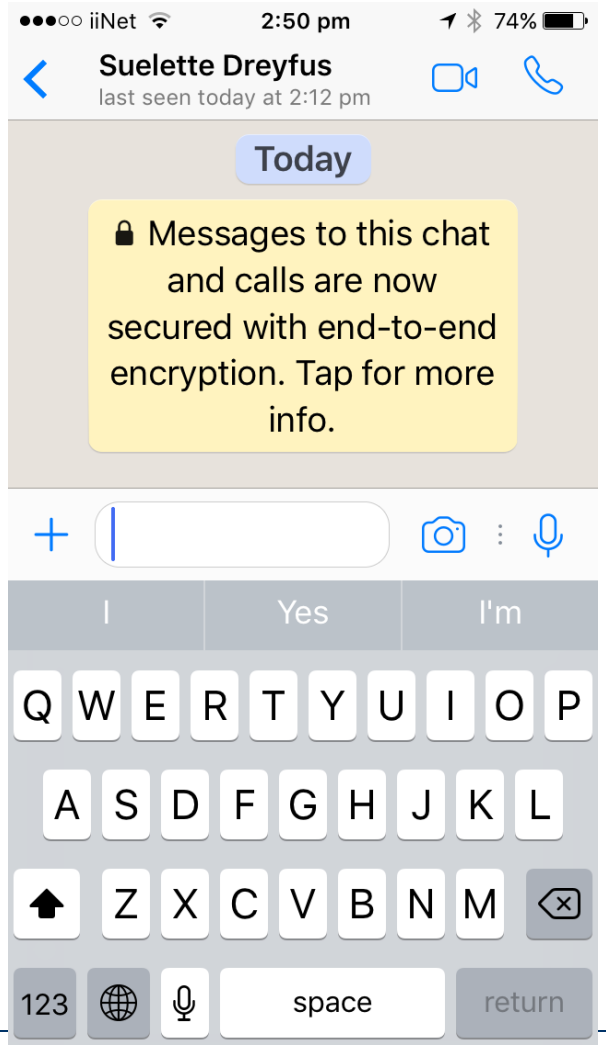
Whatsapp – removing cloud backup

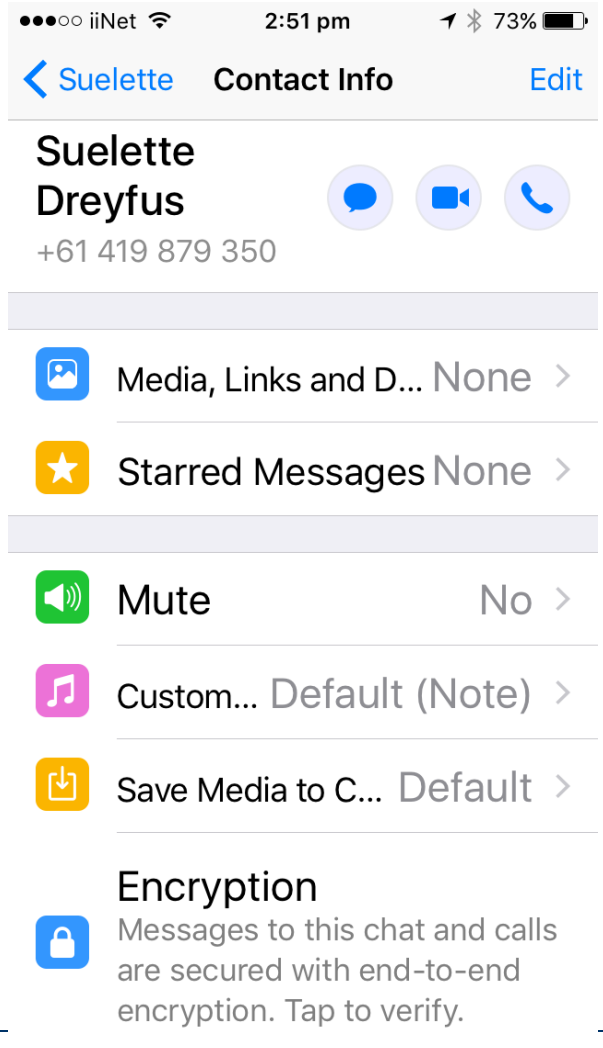


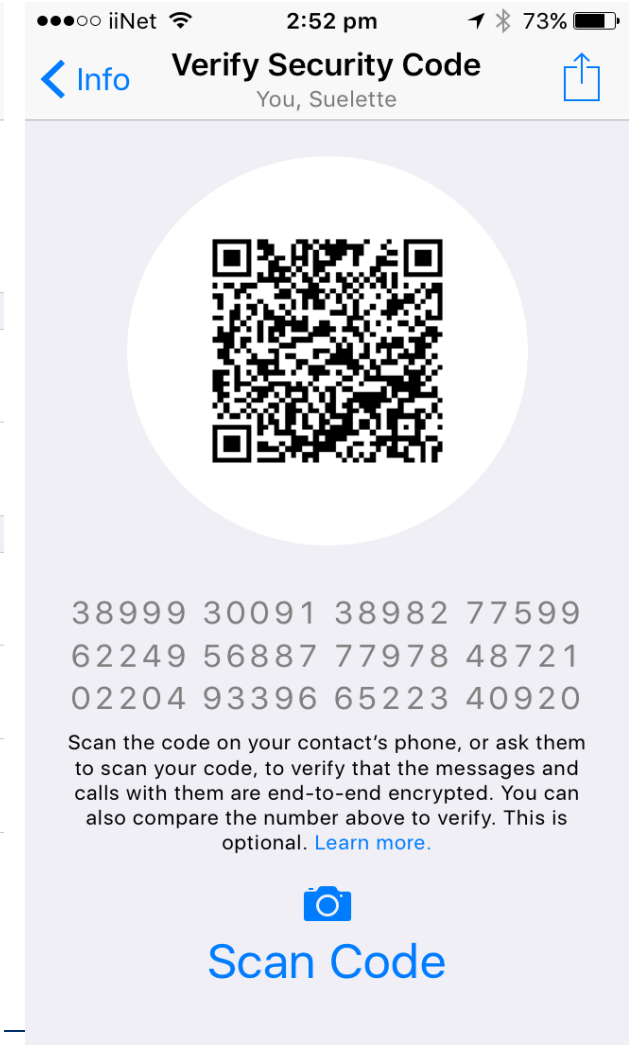




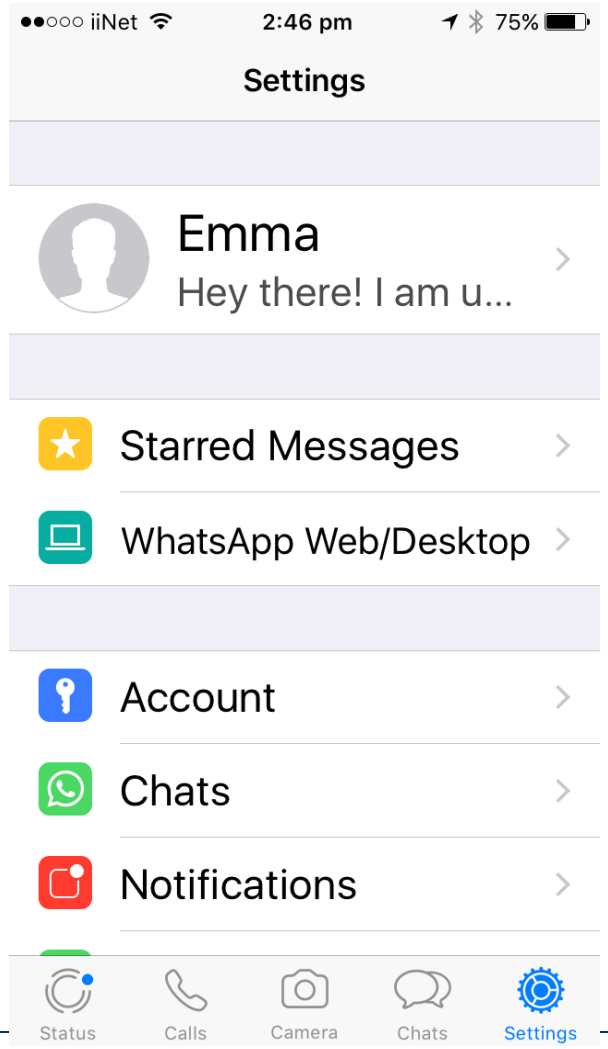
Whatsapp – checking chat security

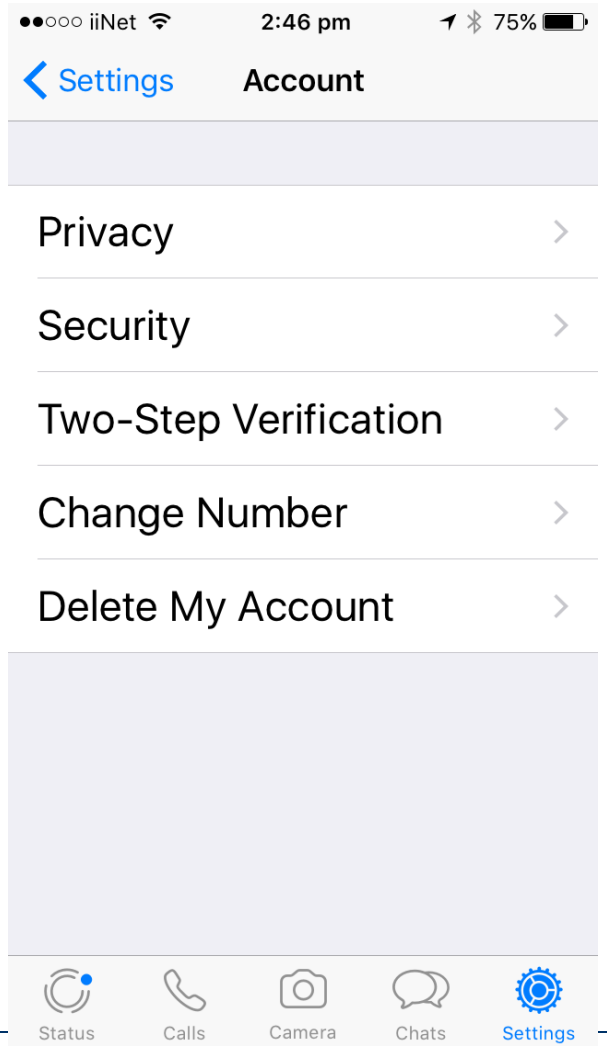


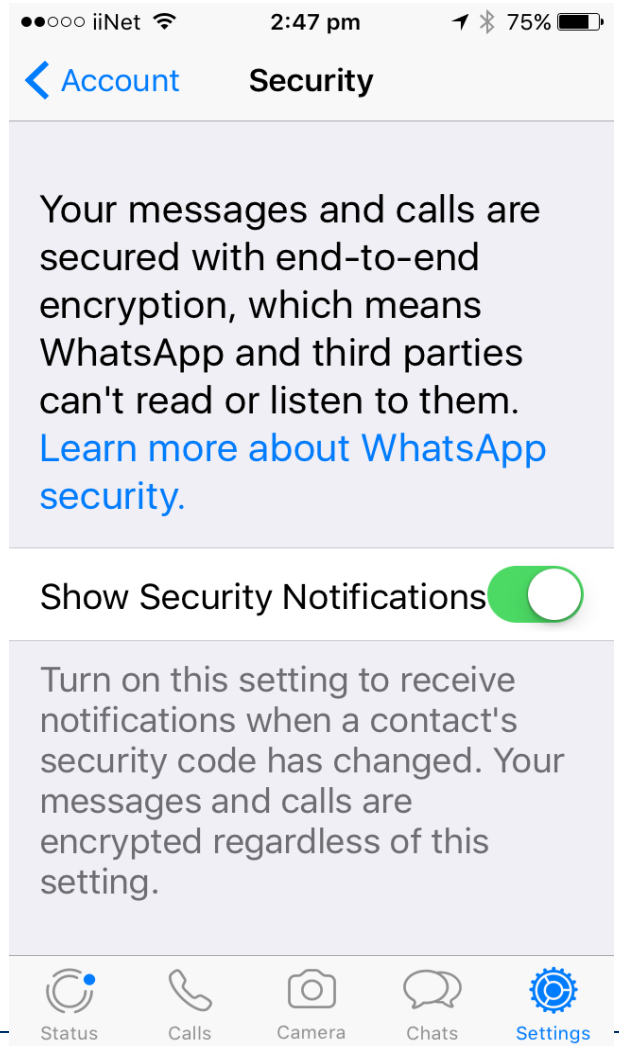




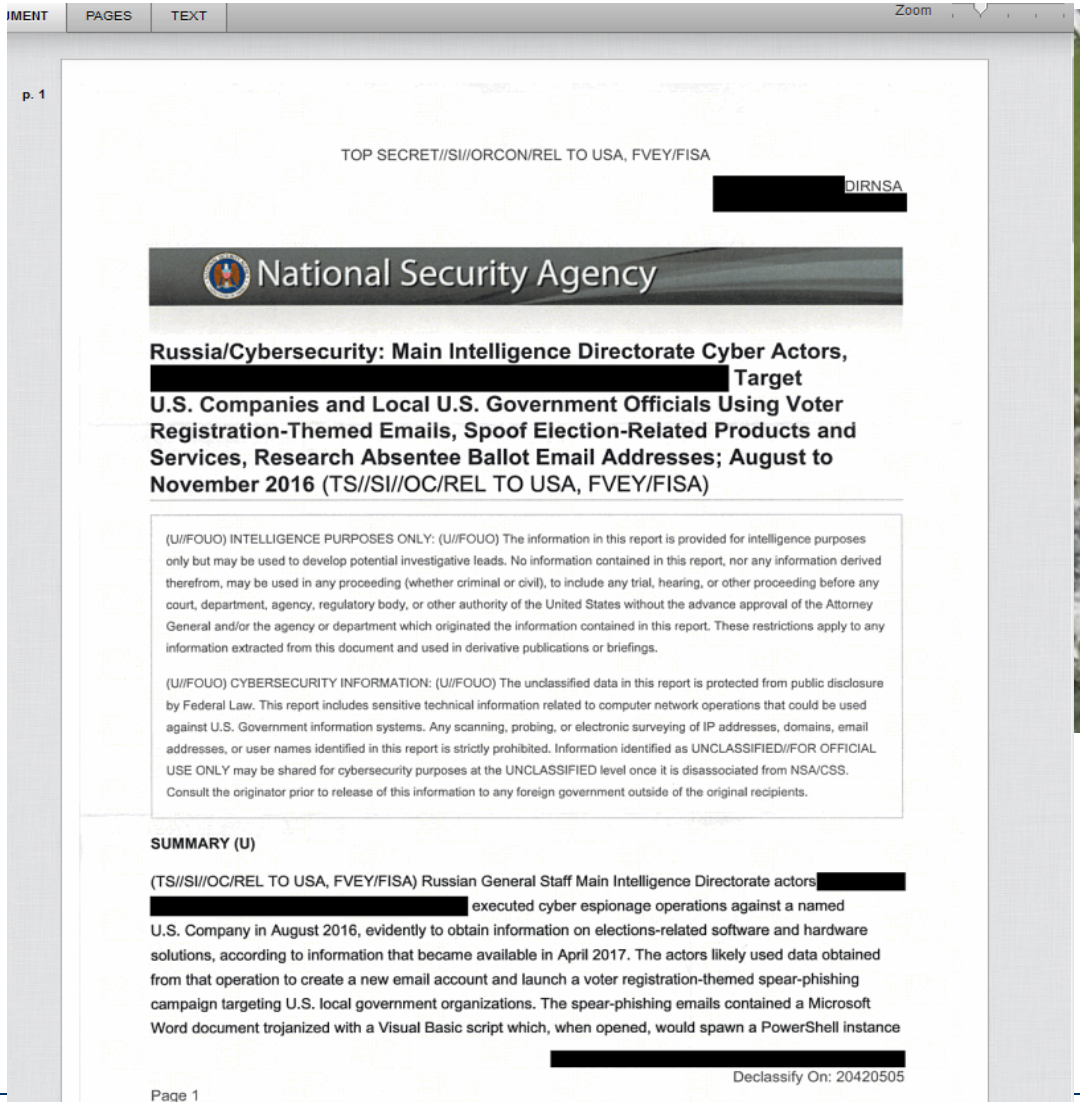
Whatsapp – security notifications







Printer dots and anonymity



IMENT PAGES TEXT Zoom

p. 1

TOP SECRET//SI//ORCON/REL TO USA, FVEY/FISA

[redacted] DIRNSA

National Security Agency

Russia/Cybersecurity: Main Intelligence Directorate Cyber Actors, [redacted] Target U.S. Companies and Local U.S. Government Officials Using Voter Registration-Themed Emails, Spoof Election-Related Products and Services, Research Absentee Ballot Email Addresses; August to November 2016 (TS//SI//OC/REL TO USA, FVEY/FISA)

(U//FOUO) INTELLIGENCE PURPOSES ONLY: (U//FOUO) The information in this report is provided for intelligence purposes only but may be used to develop potential investigative leads. No information contained in this report, nor any information derived therefrom, may be used in any proceeding (whether criminal or civil), to include any trial, hearing, or other proceeding before any court, department, agency, regulatory body, or other authority of the United States without the advance approval of the Attorney General and/or the agency or department which originated the information contained in this report. These restrictions apply to any information extracted from this document and used in derivative publications or briefings.

(U//FOUO) CYBERSECURITY INFORMATION: (U//FOUO) The unclassified data in this report is protected from public disclosure by Federal Law. This report includes sensitive technical information related to computer network operations that could be used against U.S. Government information systems. Any scanning, probing, or electronic surveying of IP addresses, domains, email addresses, or user names identified in this report is strictly prohibited. Information identified as UNCLASSIFIED//FOR OFFICIAL USE ONLY may be shared for cybersecurity purposes at the UNCLASSIFIED level once it is disassociated from NSA/CSS. Consult the originator prior to release of this information to any foreign government outside of the original recipients.

SUMMARY (U)

(TS//SI//OC/REL TO USA, FVEY/FISA) Russian General Staff Main Intelligence Directorate actors [redacted] executed cyber espionage operations against a named U.S. Company in August 2016, evidently to obtain information on elections-related software and hardware solutions, according to information that became available in April 2017. The actors likely used data obtained from that operation to create a new email account and launch a voter registration-themed spear-phishing campaign targeting U.S. local government organizations. The spear-phishing emails contained a Microsoft Word document trojanized with a Visual Basic script which, when opened, would spawn a PowerShell instance [redacted]

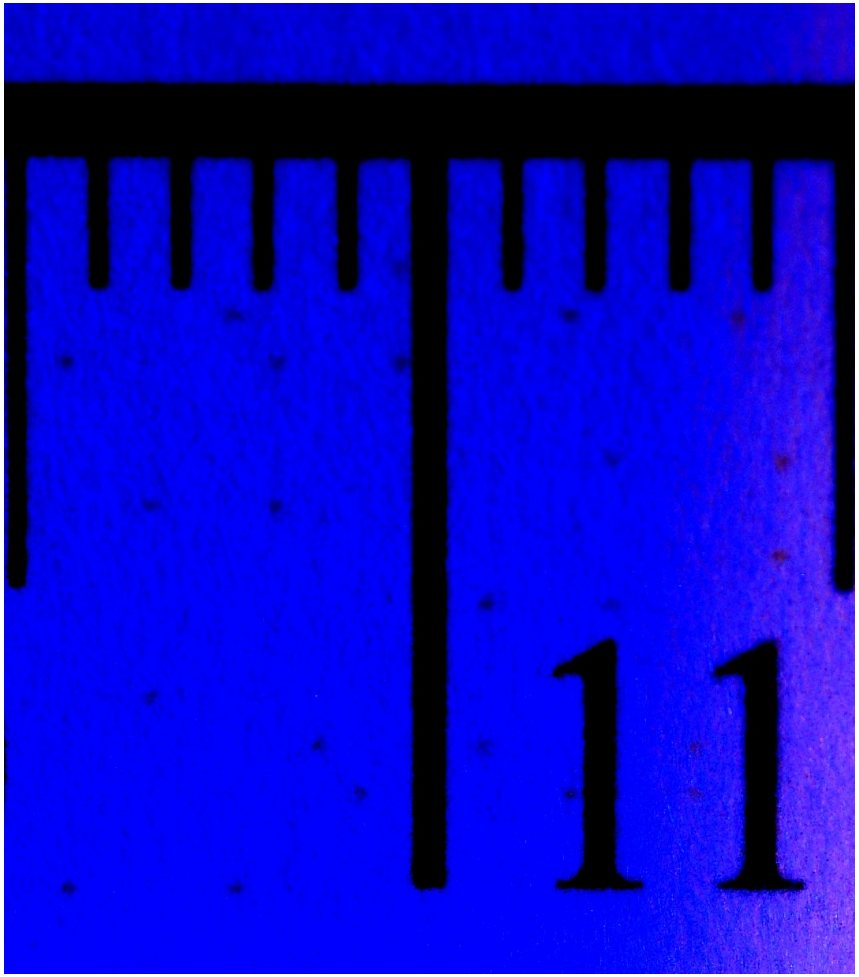
Declassify On: 20420505

Page 1

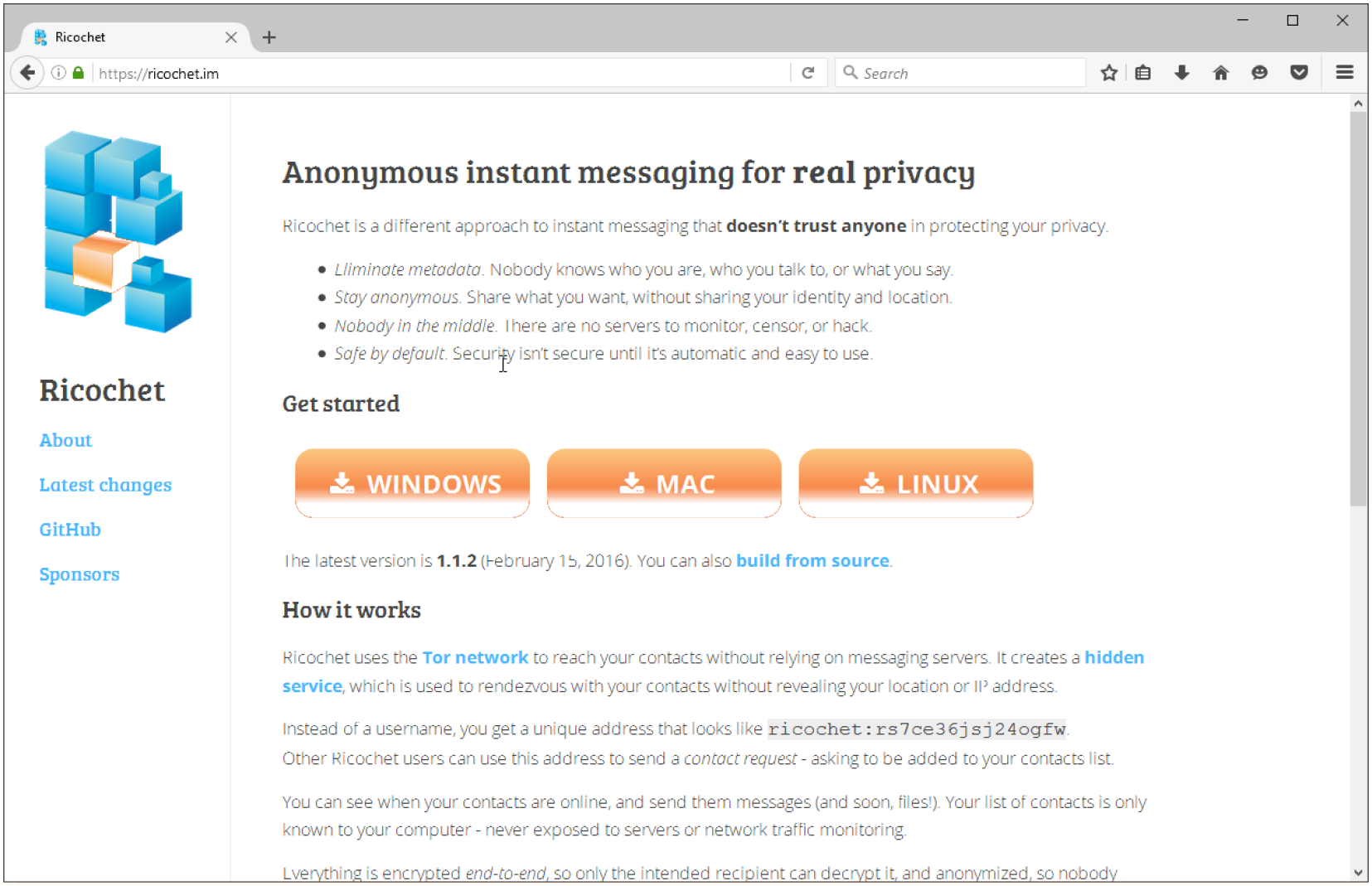
Reality Winner, NSA-Contractor and alleged whistleblower to *The Intercept*

Printer dots and anonymity

- Secret information – yellow dots which can be seen under blue light or with digital manipulation - encoded in the documents when they were printed may have allowed her identity to be quickly exposed.

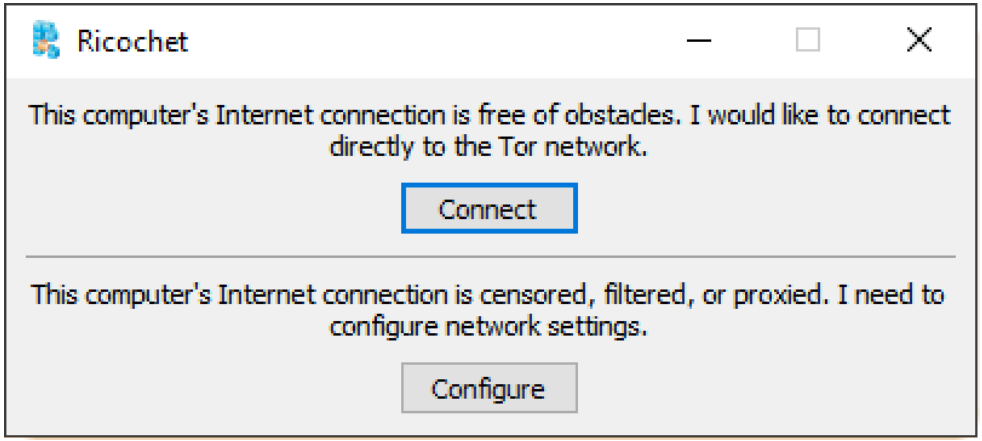


Ricochet

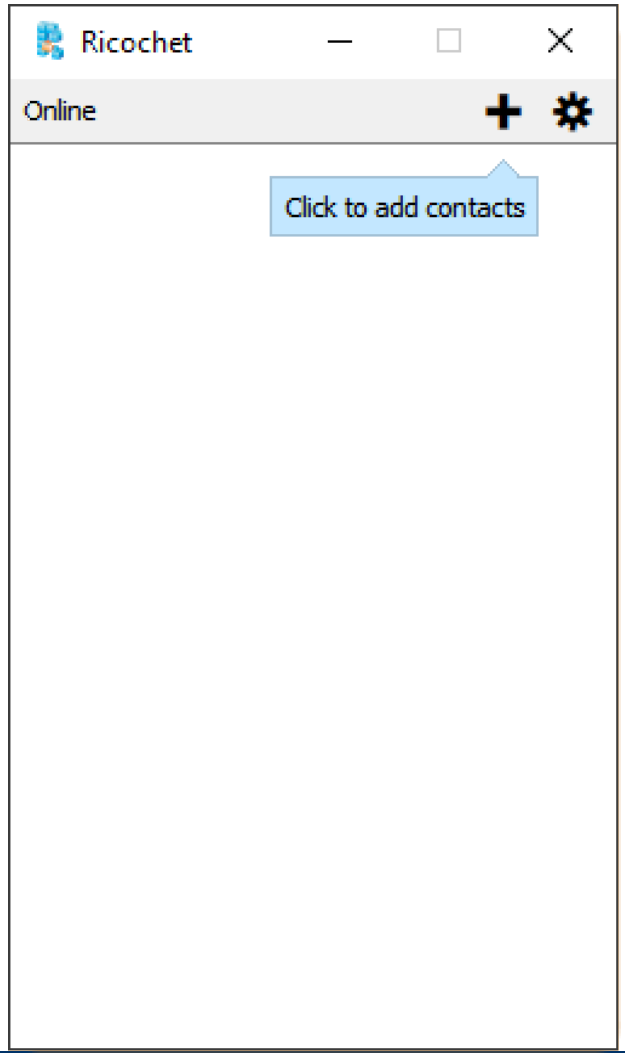

Ricochet
https://ricochet.im
Search
Ricochet
About
Latest changes
GitHub
Sponsors
Anonymous instant messaging for real privacy
Ricochet is a different approach to instant messaging that doesn't trust anyone in protecting your privacy.
Eliminate metadata. Nobody knows who you are, who you talk to, or what you say.
Stay anonymous. Share what you want, without sharing your identity and location.
Nobody in the middle. There are no servers to monitor, censor, or hack.
Safe by default. Security isn't secure until it's automatic and easy to use.
Get started
WINDOWS
MAC
LINUX
The latest version is 1.1.2 (February 15, 2016). You can also build from source.
How it works
Ricochet uses the Tor network to reach your contacts without relying on messaging servers. It creates a hidden service, which is used to rendezvous with your contacts without revealing your location or IP address.
Instead of a username, you get a unique address that looks like ricochet:rs7ce36jsj24ogfw.
Other Ricochet users can use this address to send a contact request - asking to be added to your contacts list.
You can see when your contacts are online, and send them messages (and soon, files!). Your list of contacts is only known to your computer - never exposed to servers or network traffic monitoring.
Everything is encrypted end-to-end, so only the intended recipient can decrypt it, and anonymized, so nobody

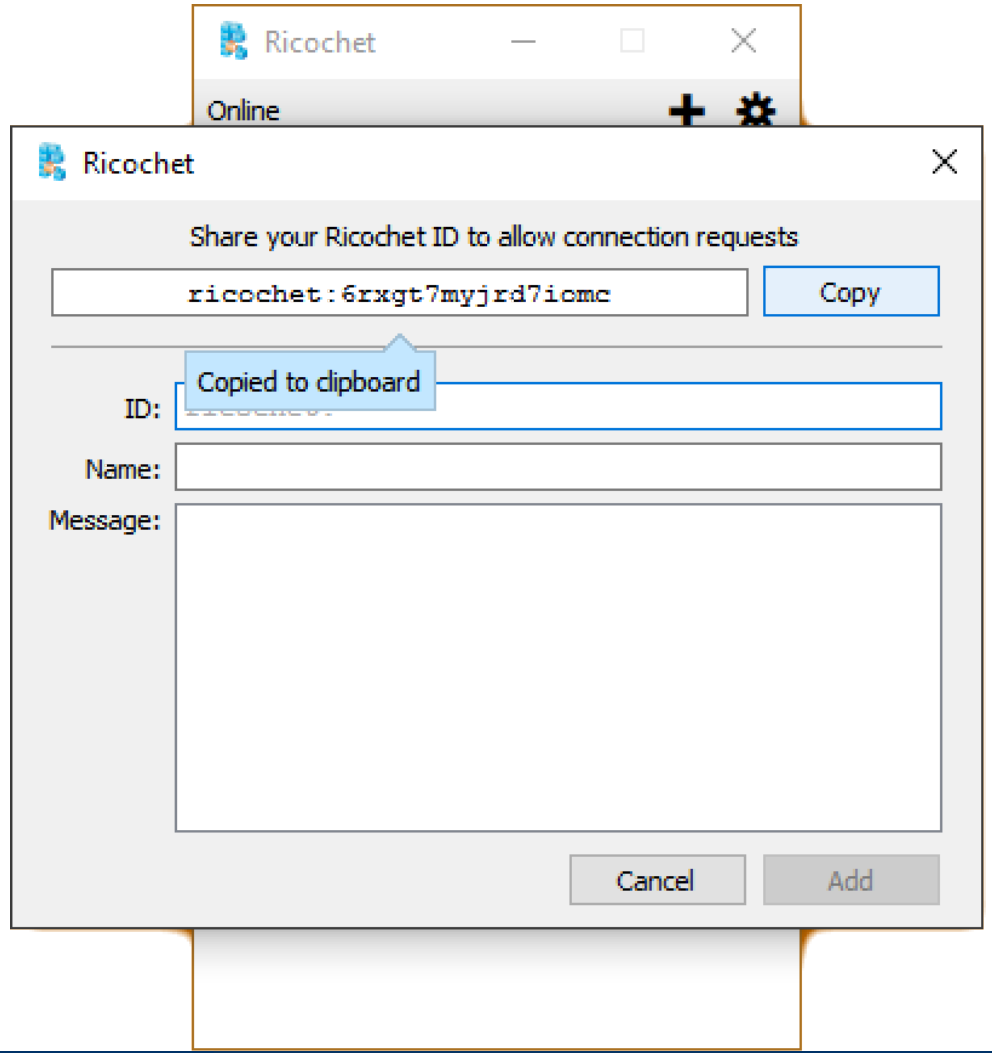
Ricochet


Setup - Ricochet
Welcome to the Ricochet Setup Wizard
This will install Ricochet on your computer.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel

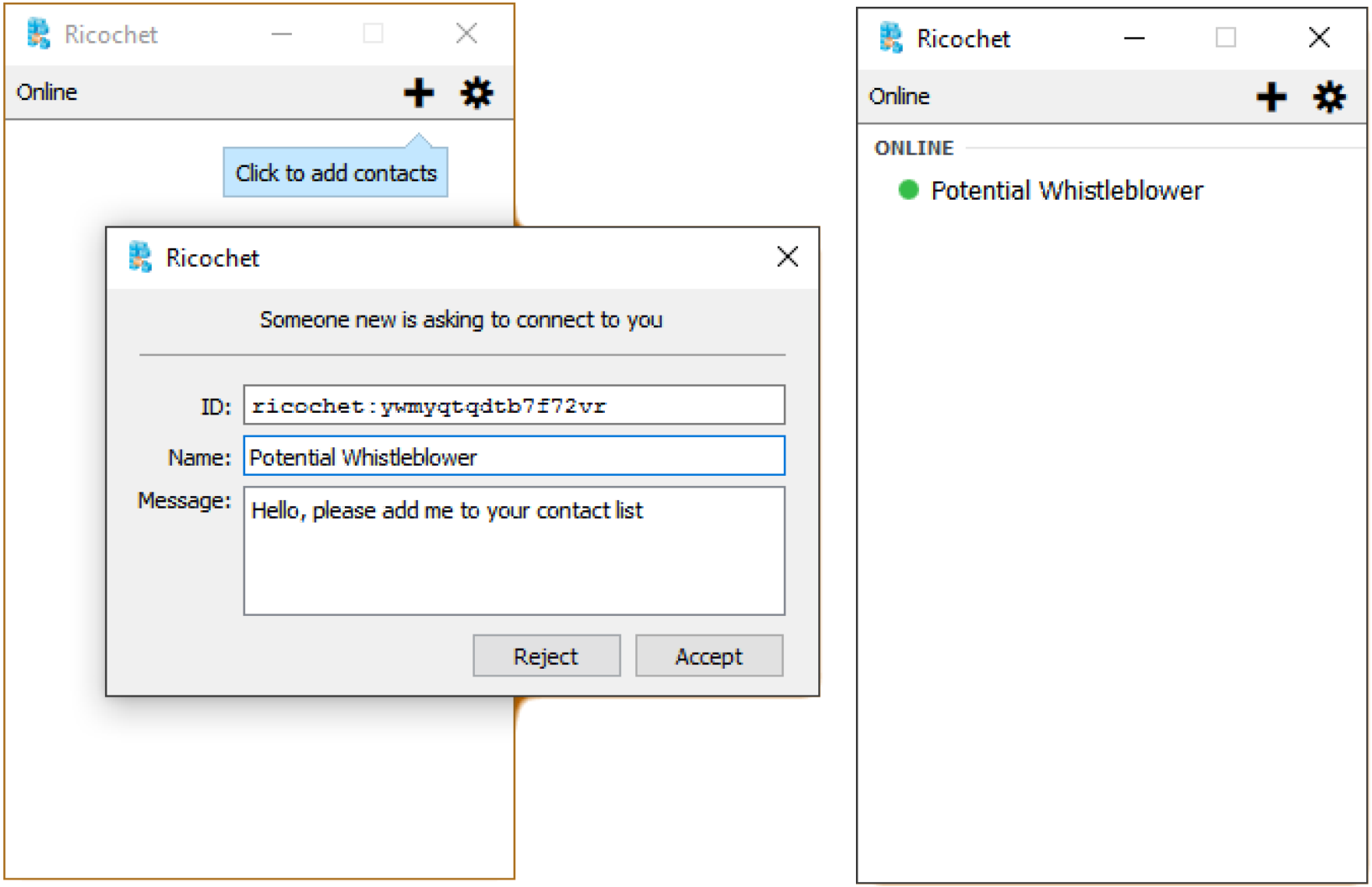

Ricochet
This computer's Internet connection is free of obstacles. I would like to connect directly to the Tor network.
Connect
This computer's Internet connection is censored, filtered, or proxied. I need to configure network settings.
Configure

Ricochet

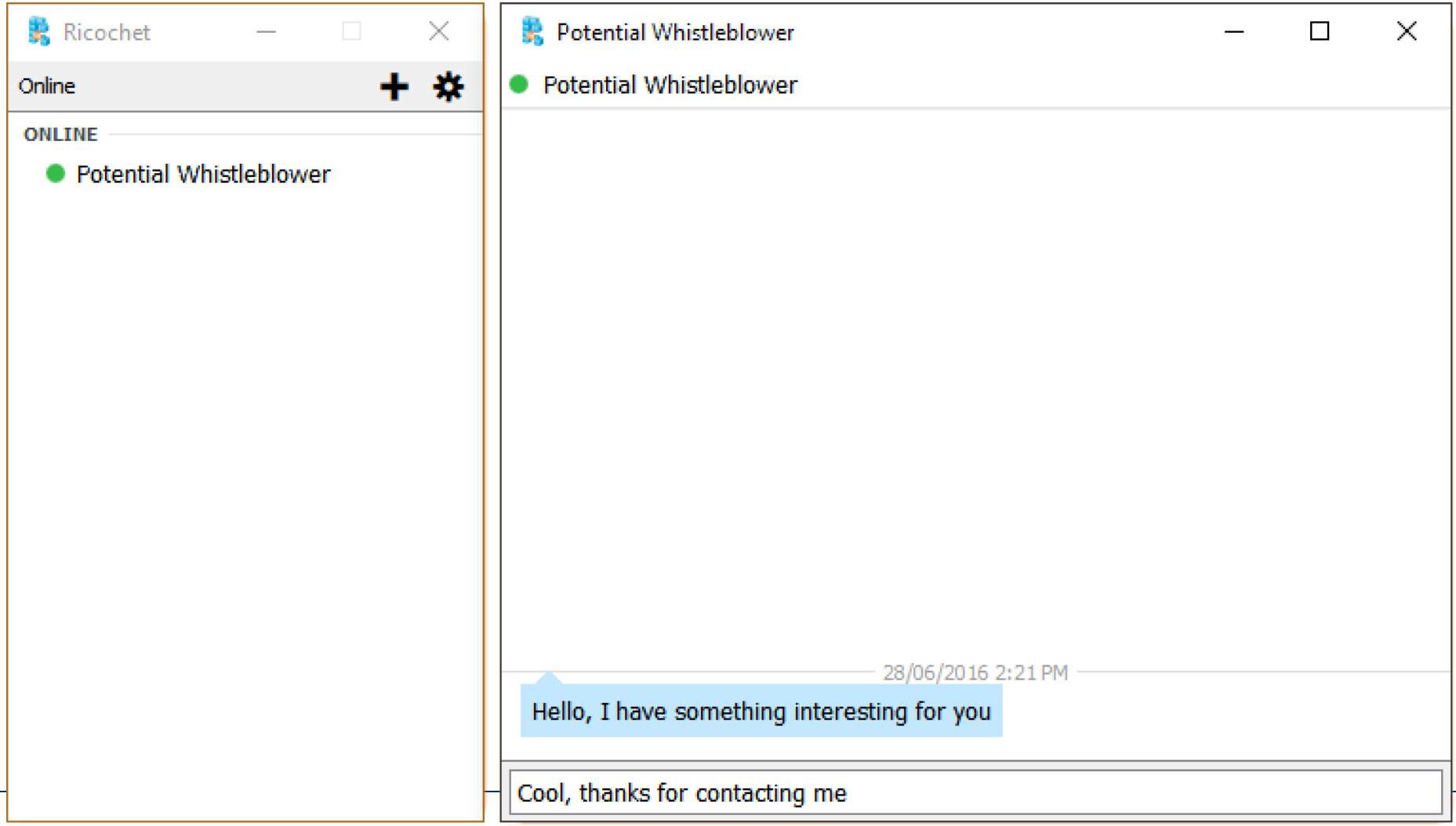

Ricochet
Online
Click to add contacts


Ricochet
Online
Ricochet
Share your Ricochet ID to allow connection requests
ricochet:6rxgt7myjrd7iomc
Copy
Copied to clipboard
ID:
Name:
Message:
Cancel
Add

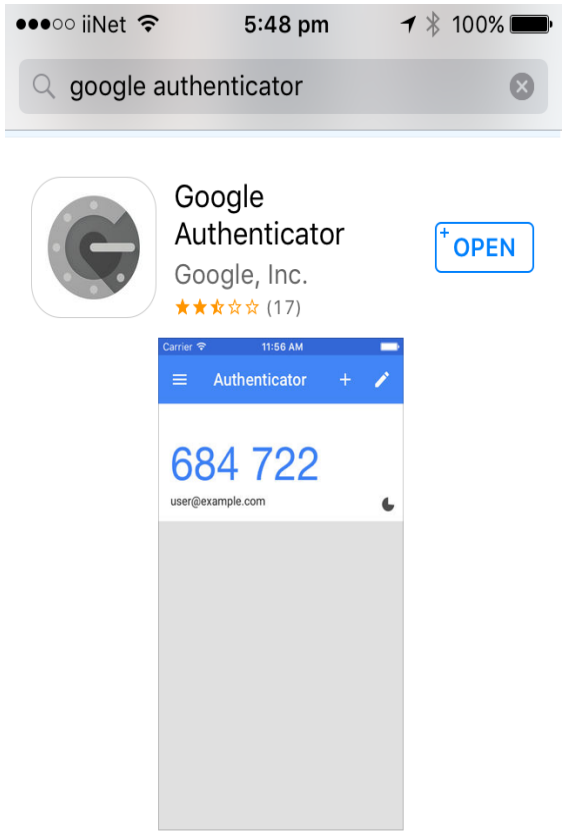
Ricochet

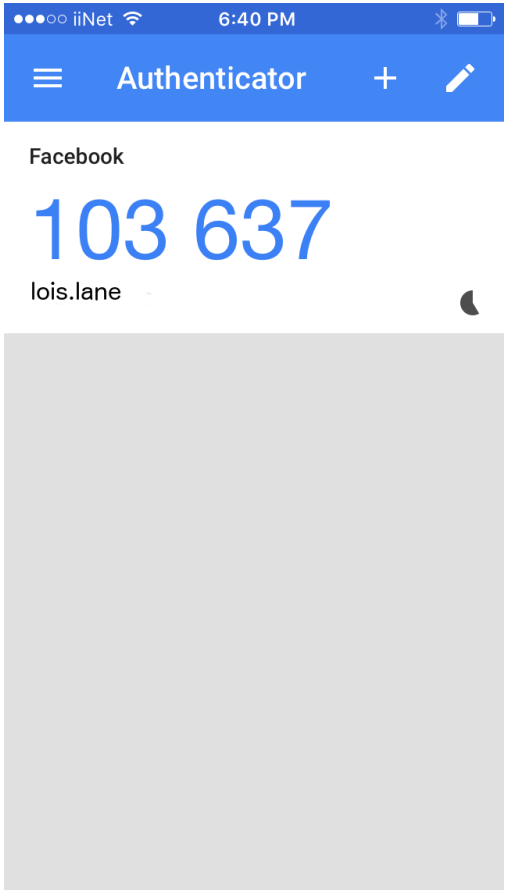

Ricochet
Online
Click to add contacts
Ricochet
Someone new is asking to connect to you
ID:
ricochet:ywmyqtqdtb7f72vr
Name:
Potential Whistleblower
Message:
Hello, please add me to your contact list
Reject
Accept
Ricochet
Online
ONLINE
Potential Whistleblower

Ricochet


Ricochet
Online
ONLINE
Potential Whistleblower
Potential Whistleblower
Potential Whistleblower
28/06/2016 2:21 PM
Hello, I have something interesting for you
Cool, thanks for contacting me

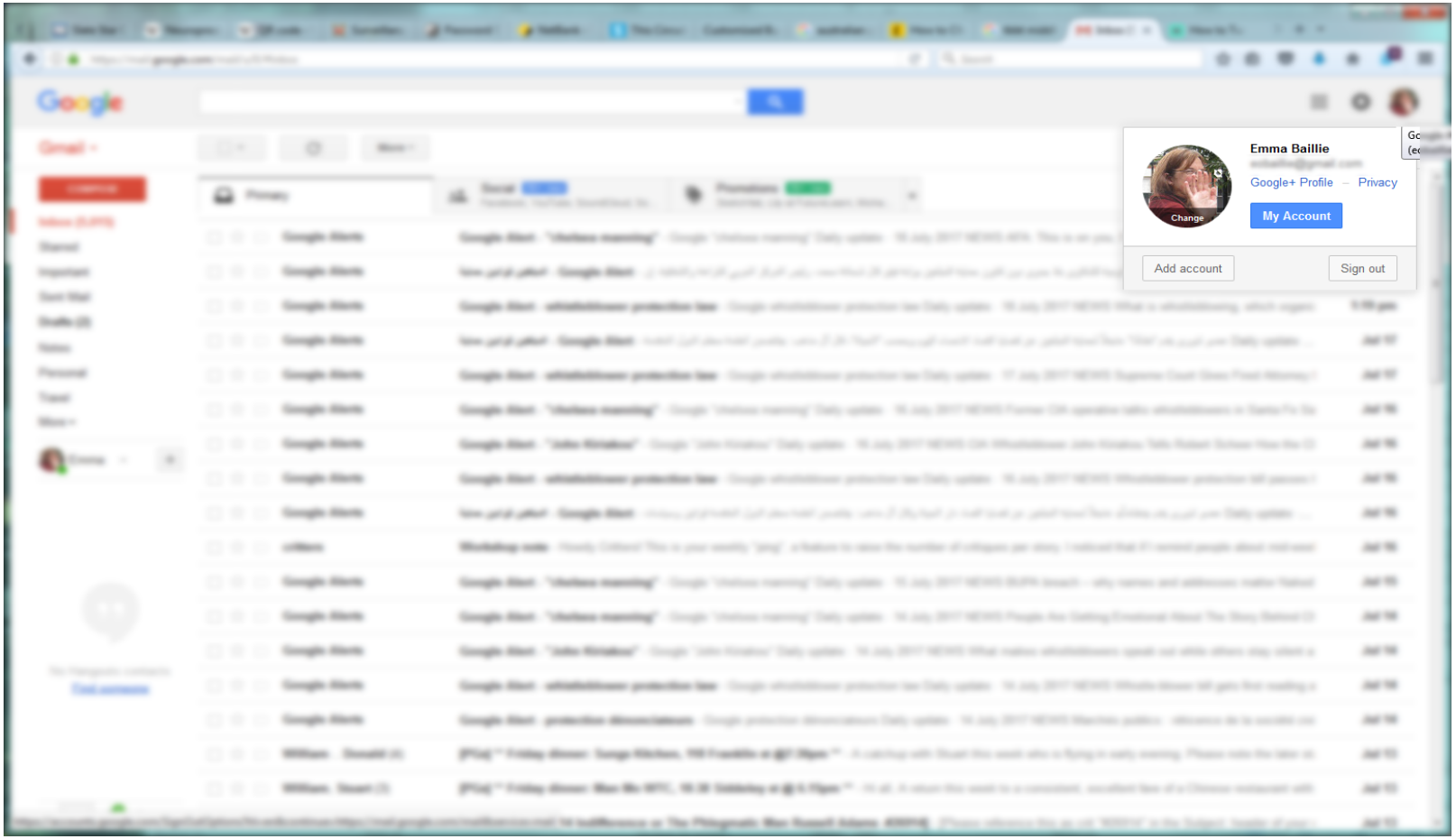
Google Authenticator



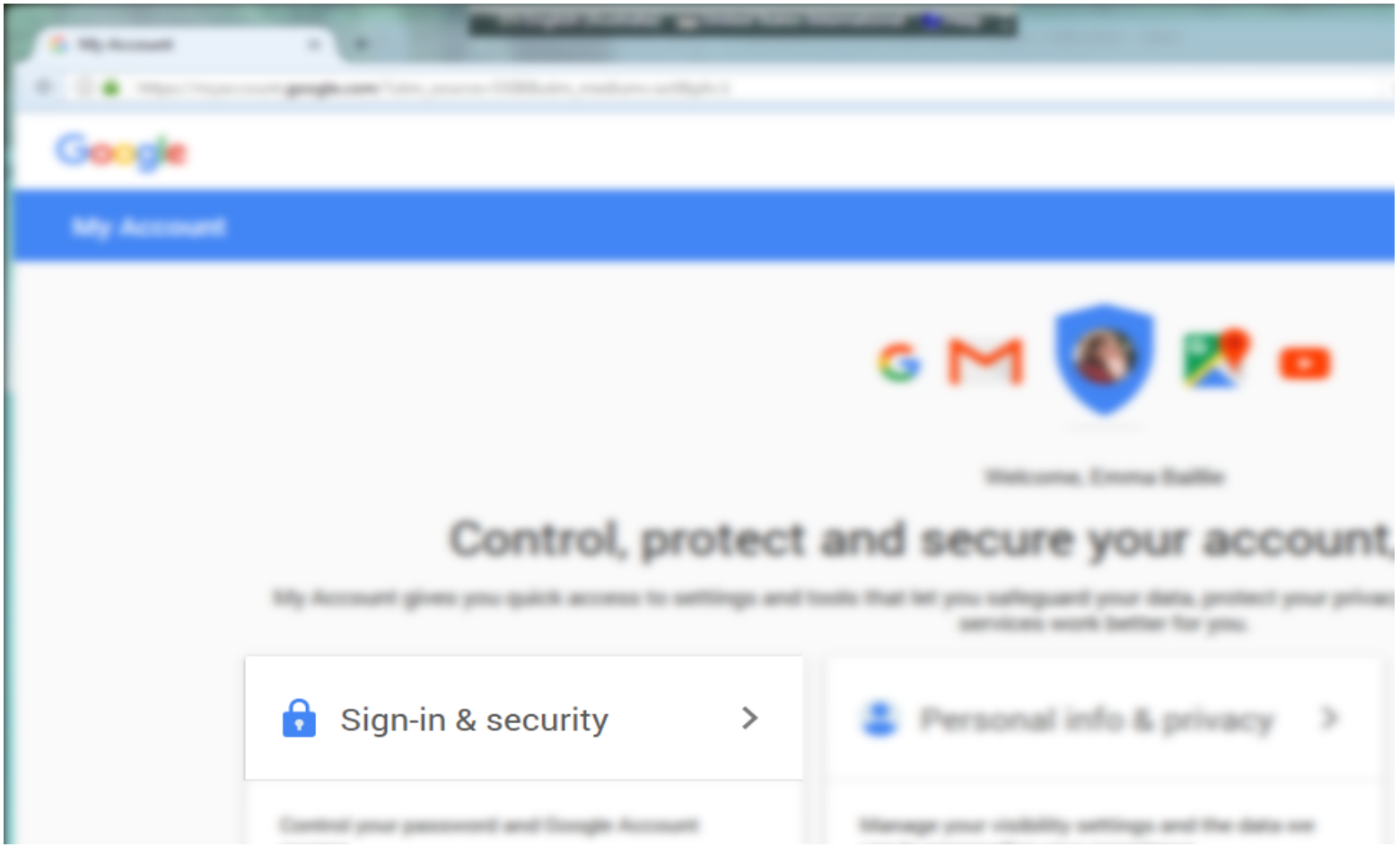


THE UNIVERSITY OF MELBOURNE

2 Factor Authenticaion - gmail

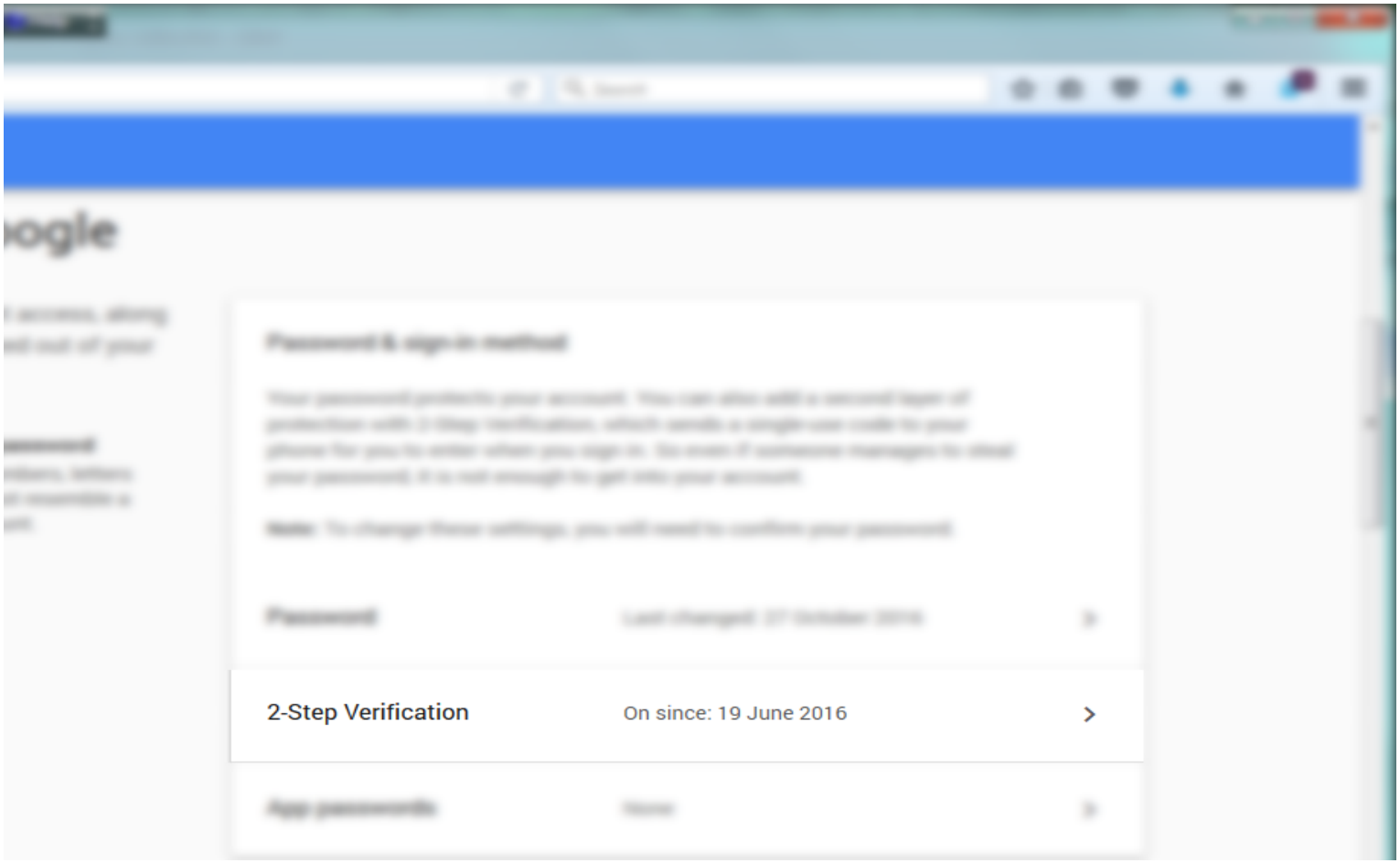


2fa - gmail

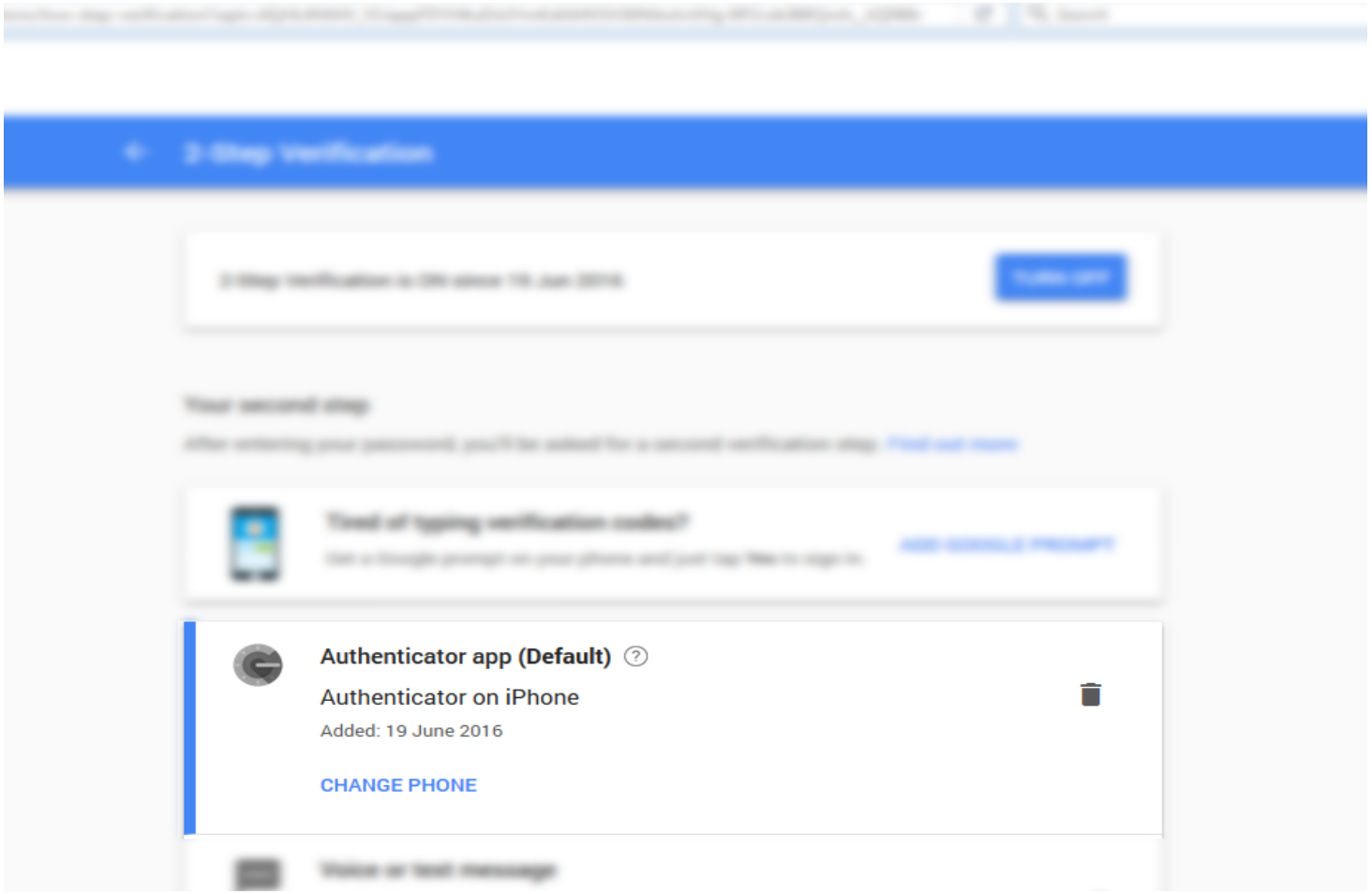

Google
My Account
Control, protect and secure your account
Sign-in & security
Personal info & privacy

THE UNIVERSITY OF MELBOURNE

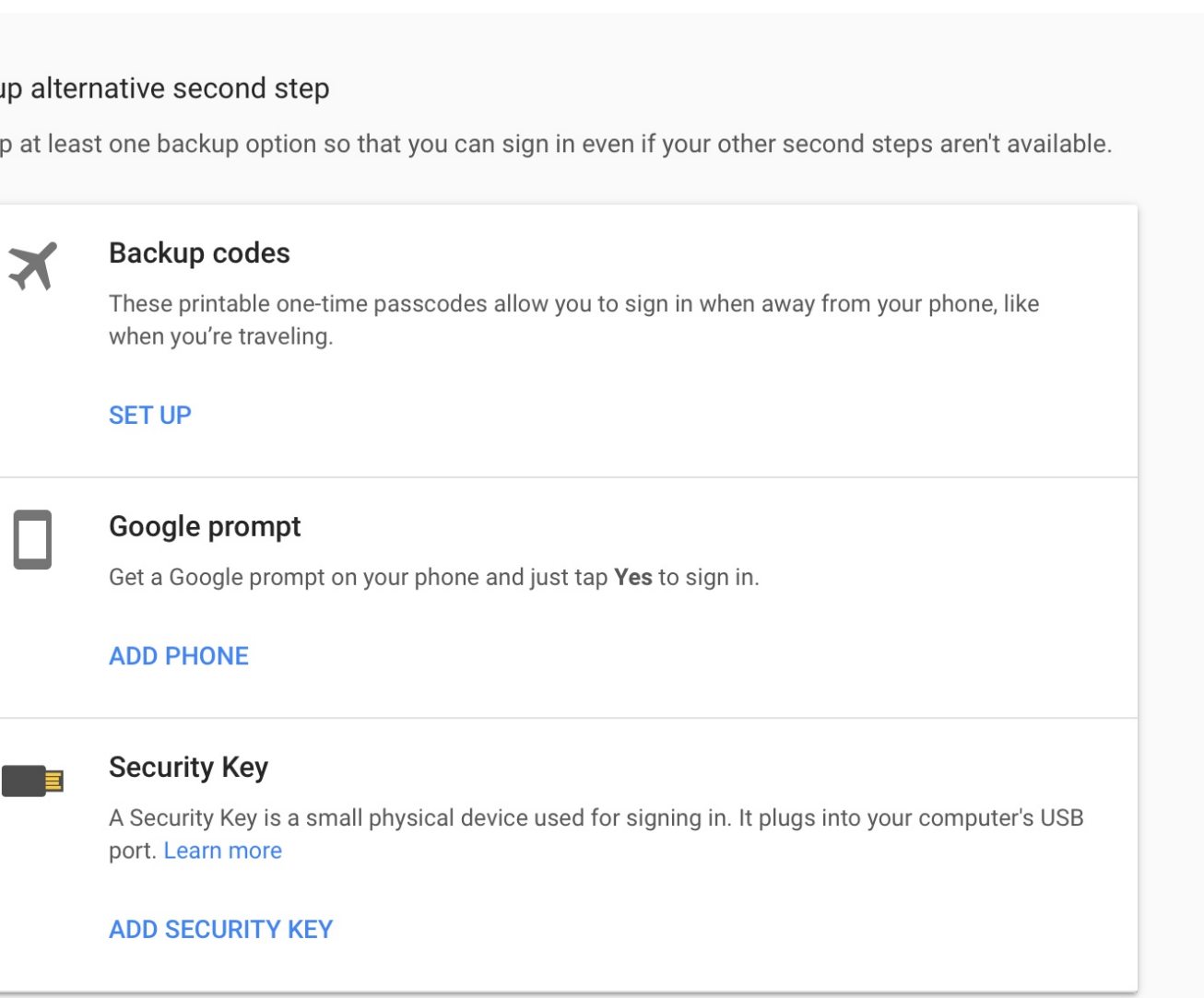
2fa - gmail



2fa - gmail

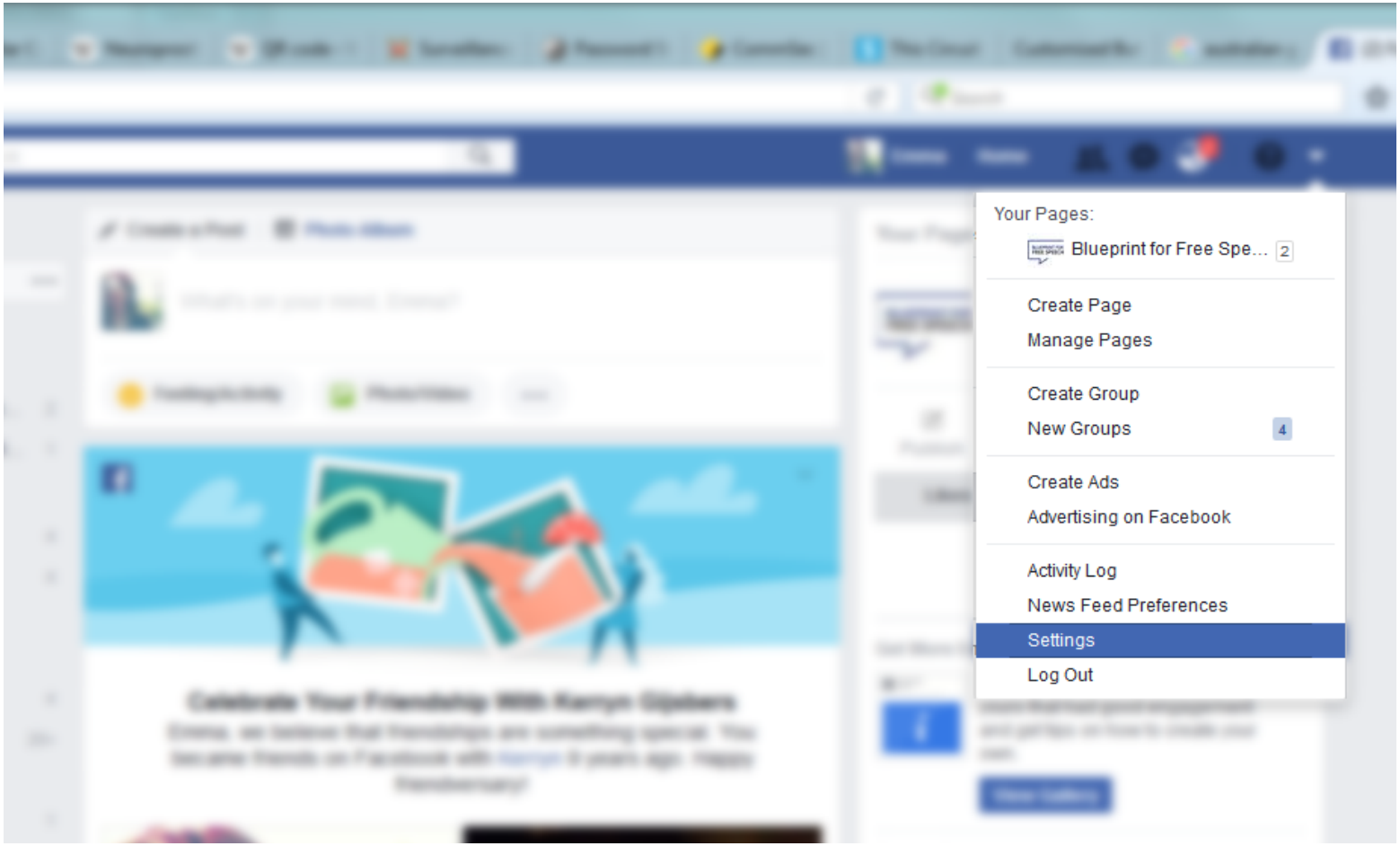

Authenticator app (Default)
Authenticator on iPhone
Added: 19 June 2016
CHANGE PHONE

2fa – gmail – Recovery codes



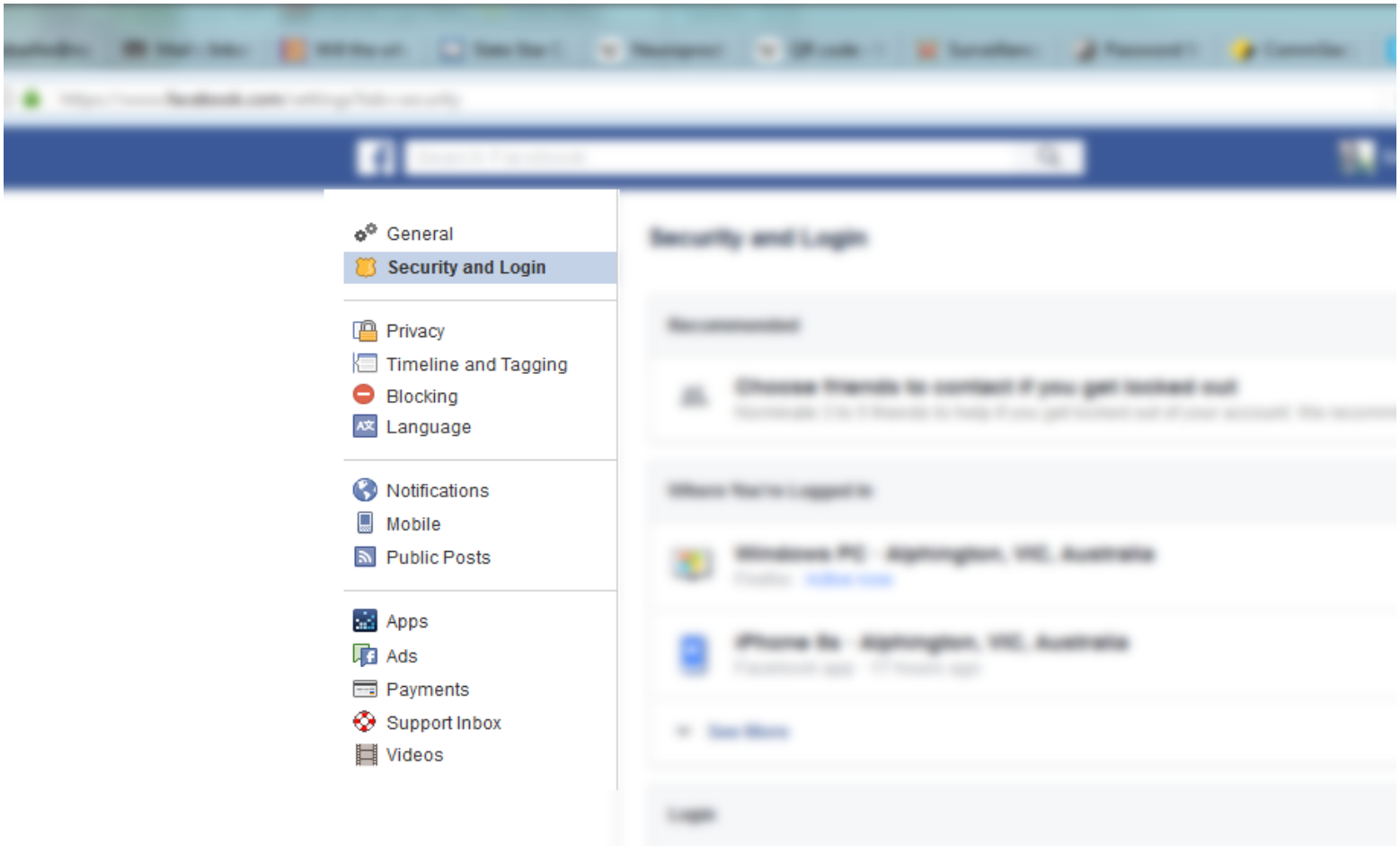
THE UNIVERSITY OF MELBOURNE

2fa - Facebook

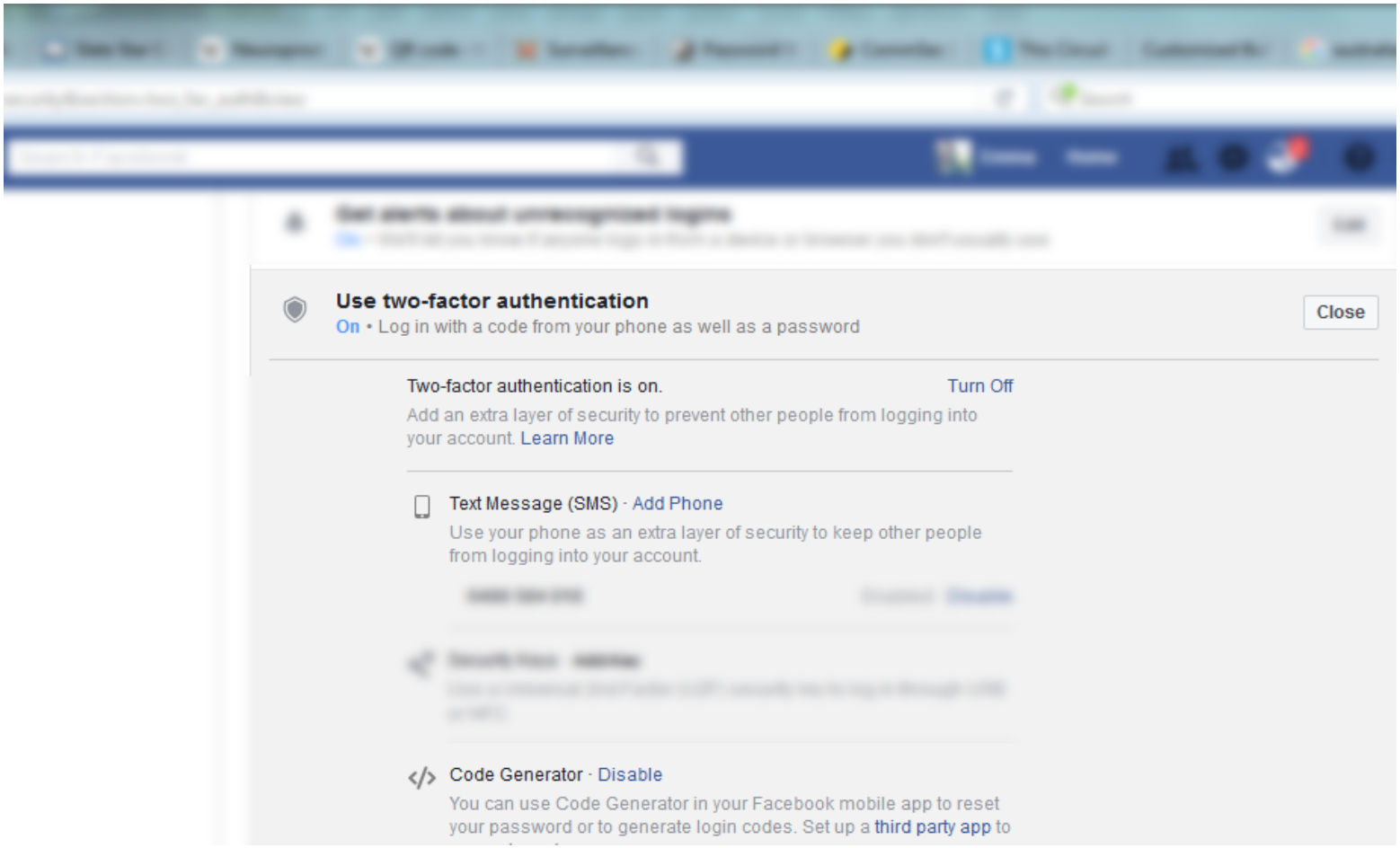


THE UNIVERSITY OF MELBOURNE

2fa - Facebook

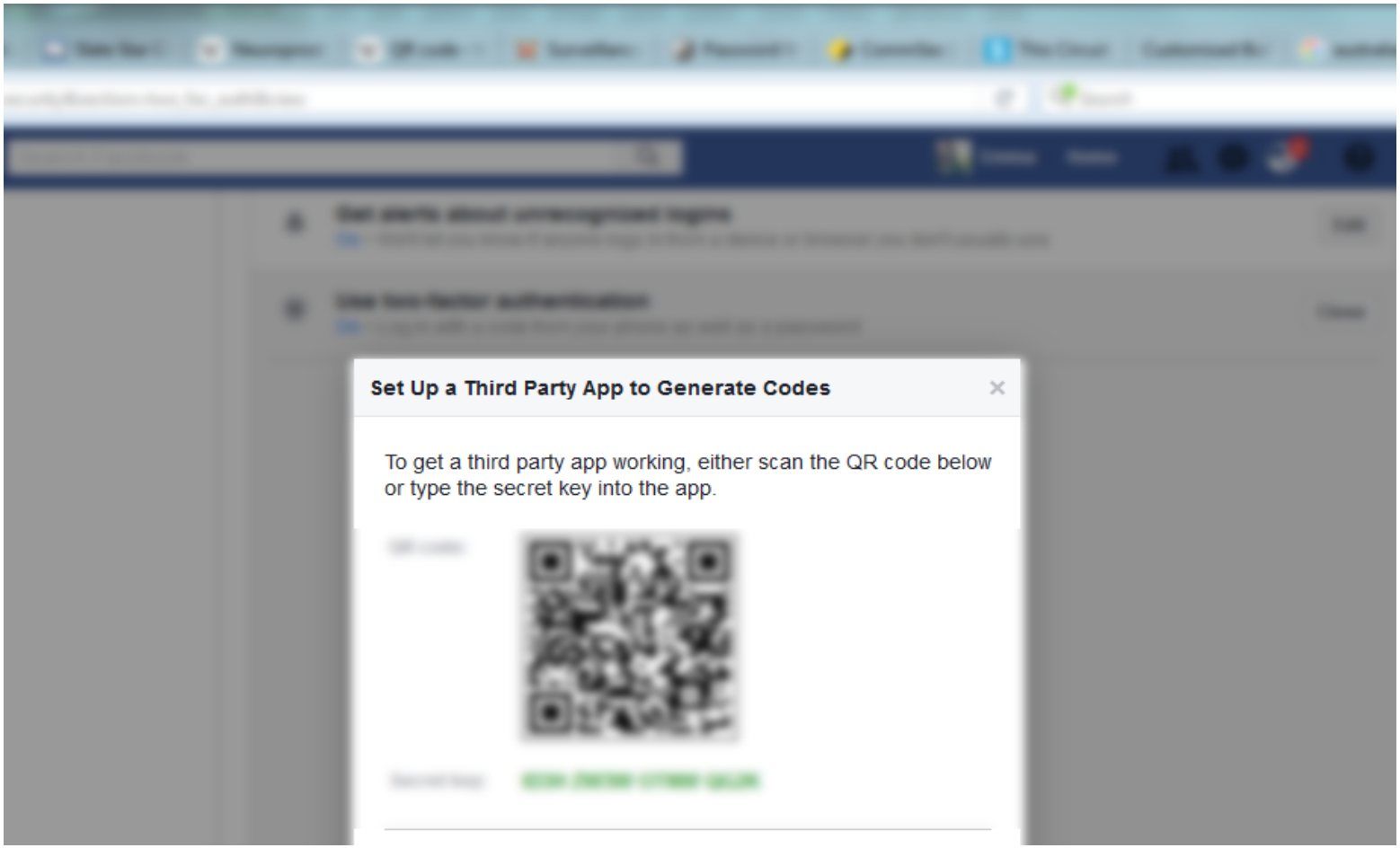


2fa - Facebook



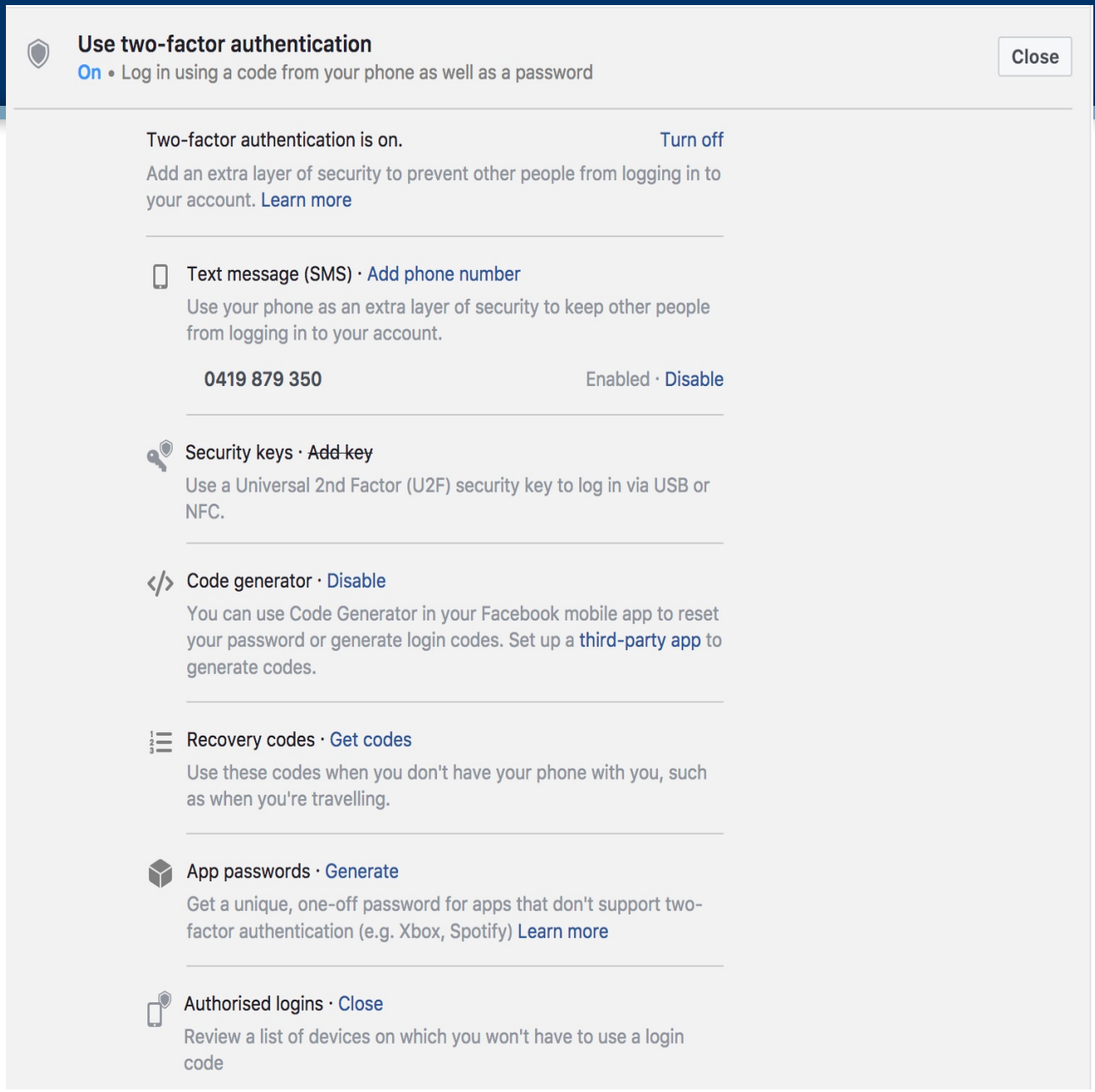
THE UNIVERSITY OF MELBOURNE

2fa - Facebook

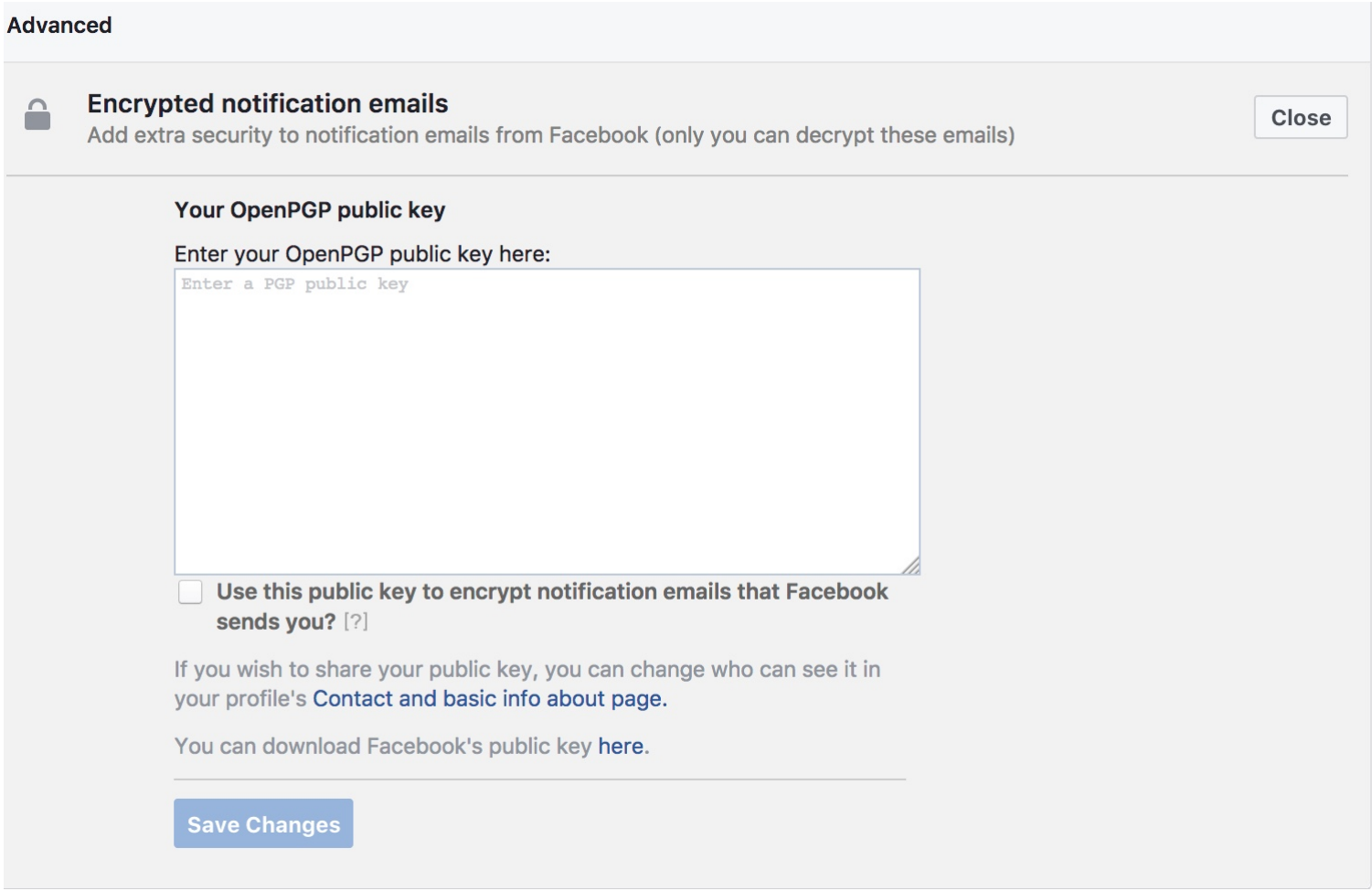


THE UNIVERSITY OF MELBOURNE

2fa Facebook

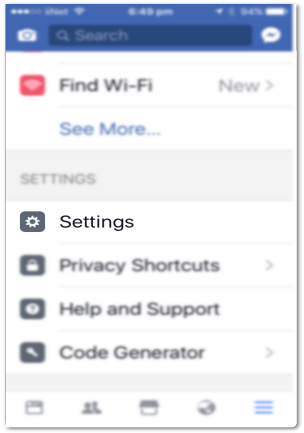


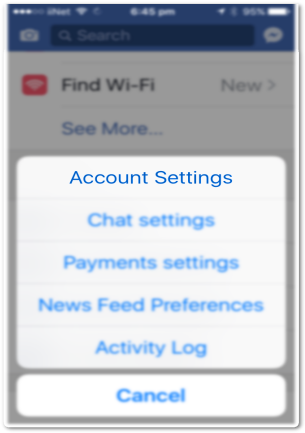
2fa – Facebook – GPG Public Key

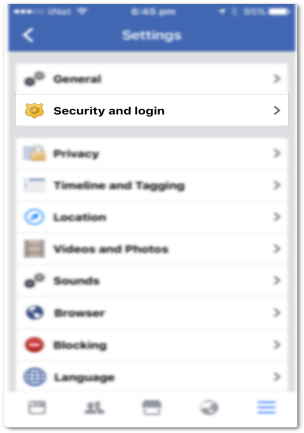


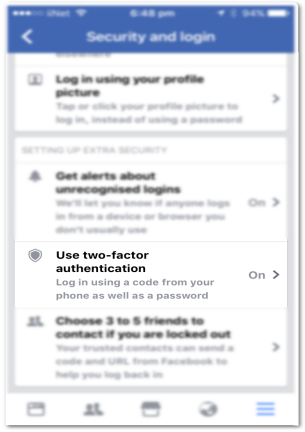
THE UNIVERSITY OF MELBOURNE

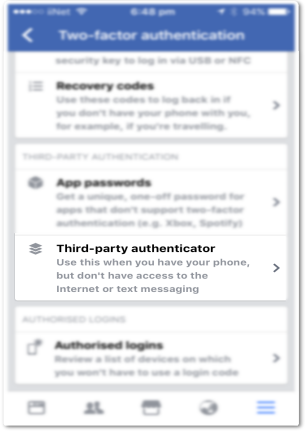
2fa – Facebook setup on Phones

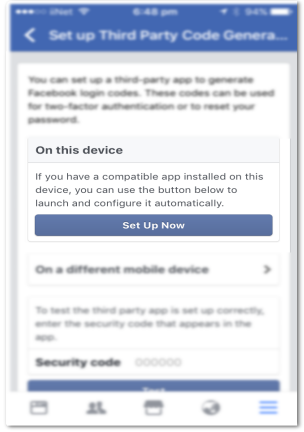




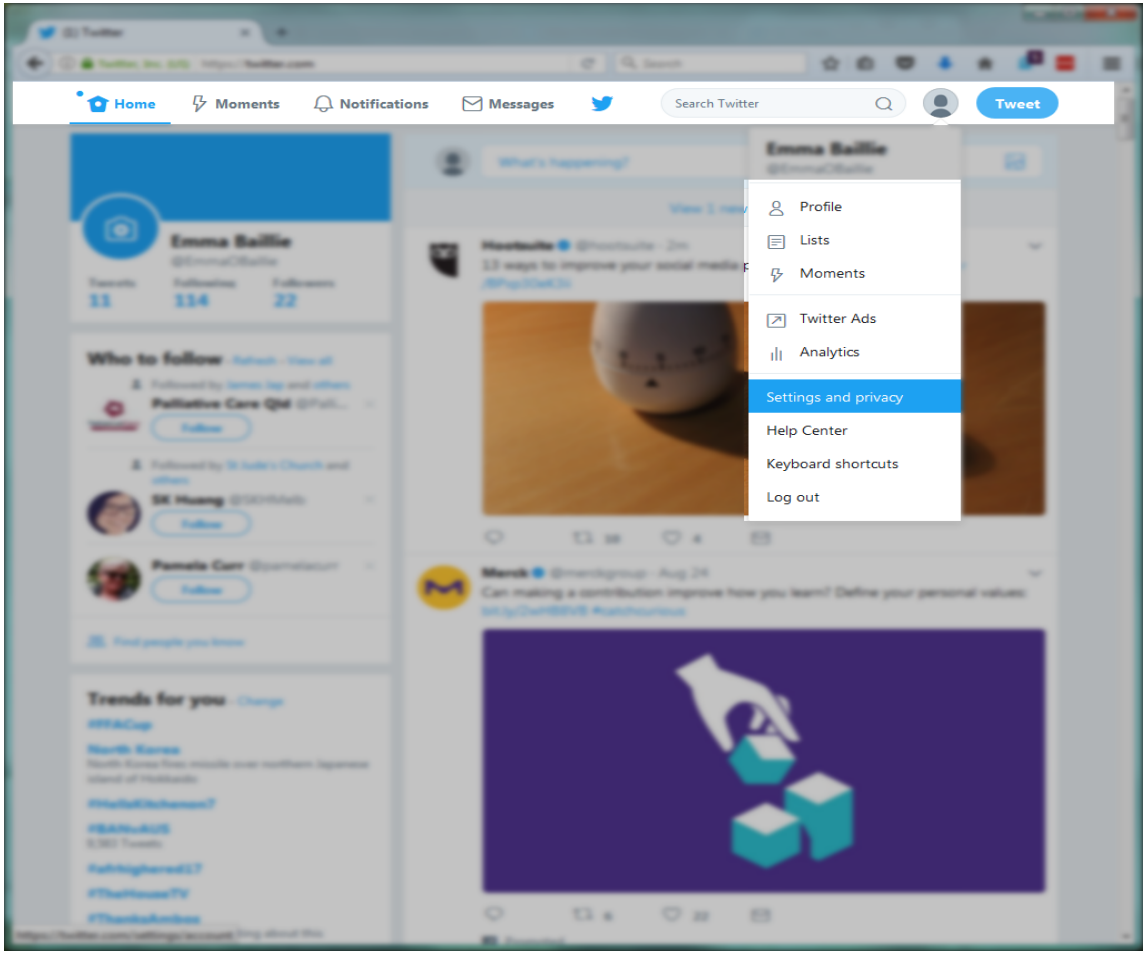




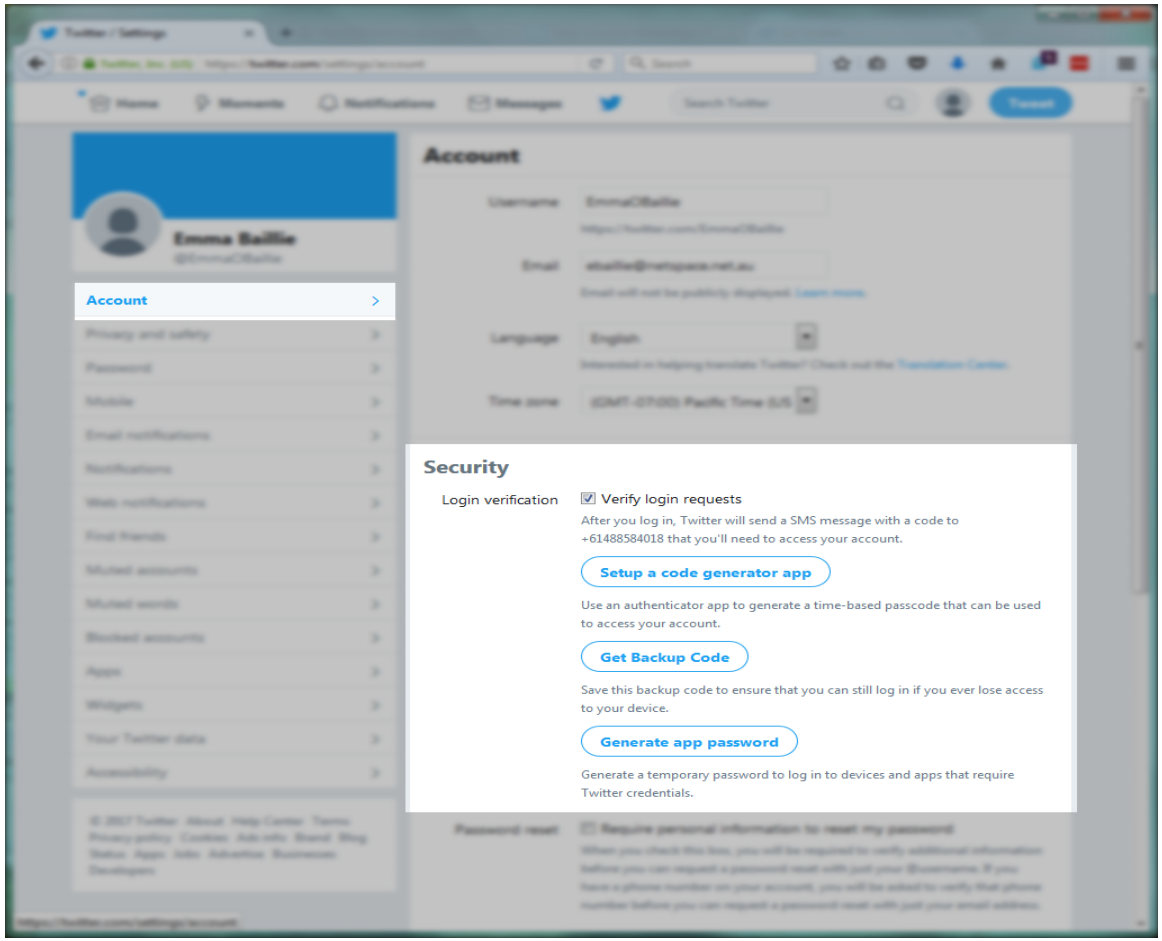




2fa - Twitter

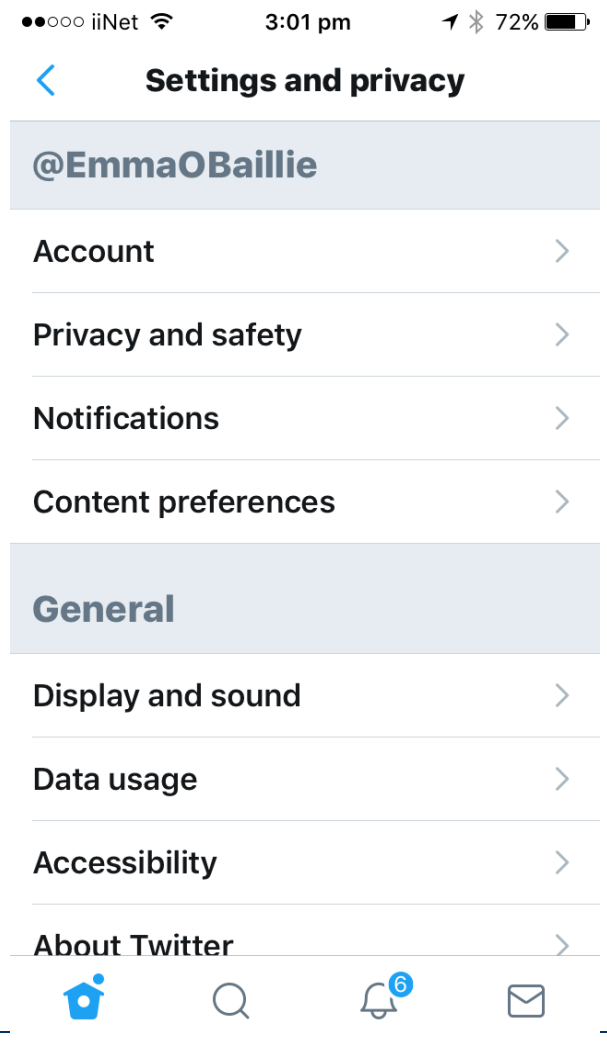

Home
Moments
Notifications
Messages
Search Twitter
Tweet
Emma Baillie
Profile
Lists
Moments
Twitter Ads
Analytics
Settings and privacy
Help Center
Keyboard shortcuts
Log out
Who to follow
Trends for you

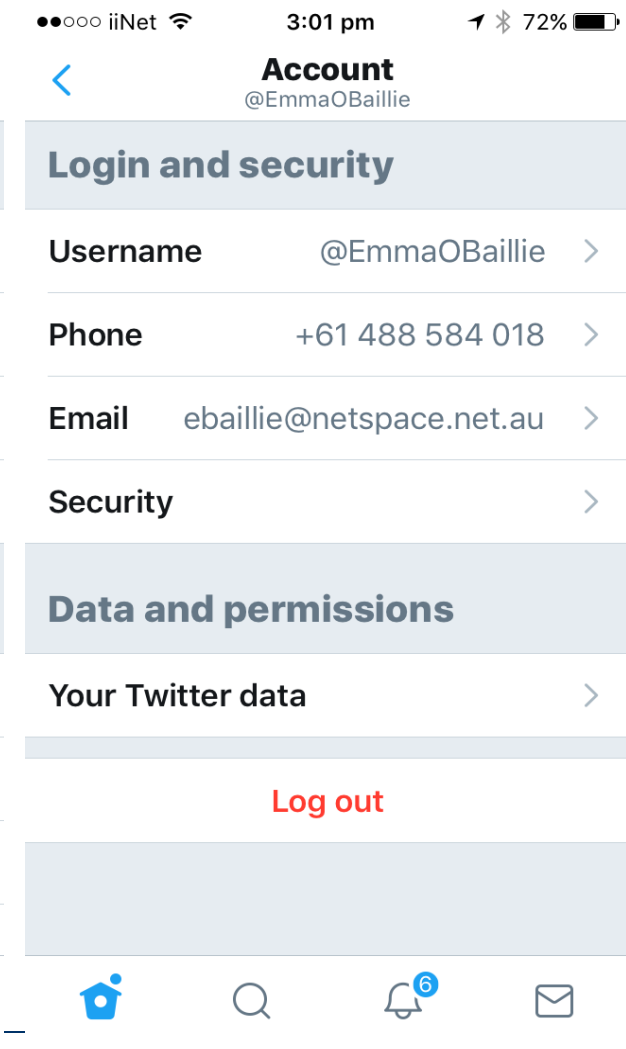
2fa - Twitter


Account
Emma Baillie
Account
Security
Login verification
Verify login requests
After you log in, Twitter will send a SMS message with a code to +61488584018 that you'll need to access your account.
Setup a code generator app
Use an authenticator app to generate a time-based passcode that can be used to access your account.
Get Backup Code
Save this backup code to ensure that you can still log in if you ever lose access to your device.
Generate app password
Generate a temporary password to log in to devices and apps that require Twitter credentials.

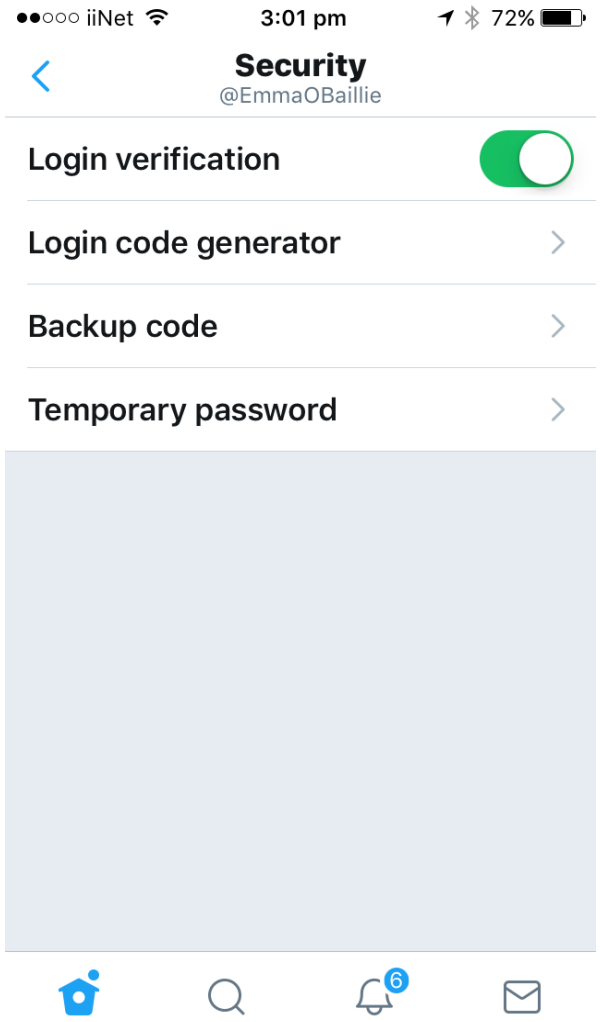
2fa - Twitter

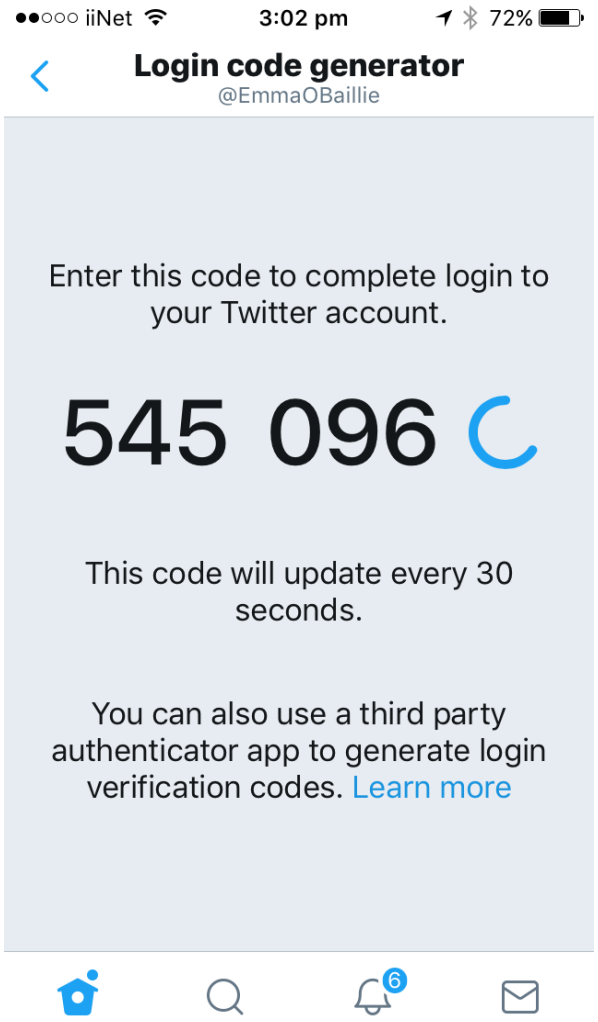

●●●○○ iiNet 3:00 pm 72%
Emma Baillie
@EmmaOBaillie
114 Following 22 Followers
Profile
Lists
Moments
Settings and privacy
Help Center

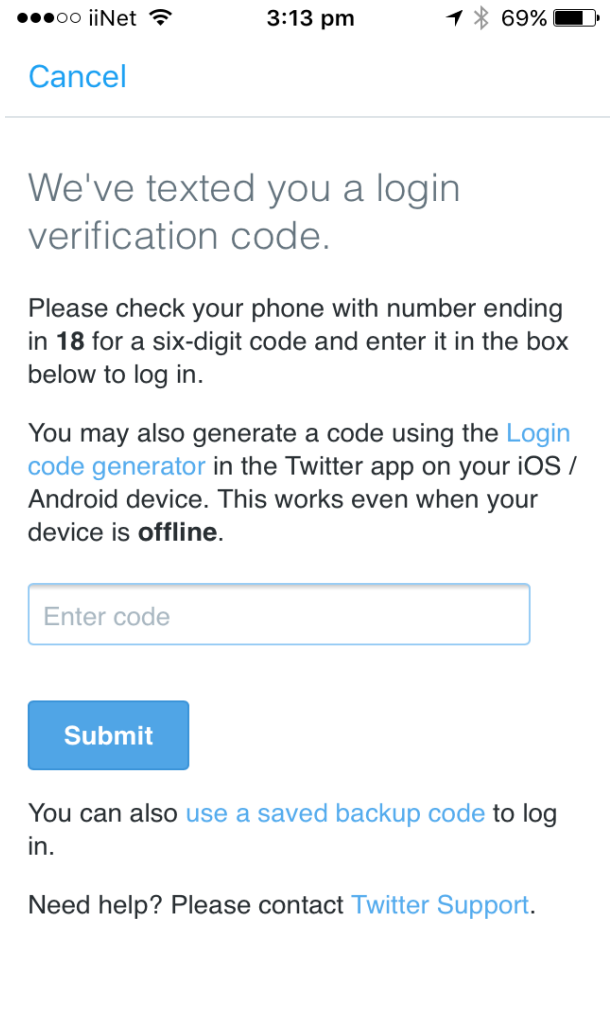

●●○○○ iiNet 3:01 pm 72%
Settings and privacy
@EmmaOBaillie
Account
Privacy and safety
Notifications
Content preferences
General
Display and sound
Data usage
Accessibility
About Twitter


●●○○○ iiNet 3:01 pm 72%
Account
@EmmaOBaillie
Login and security
Username @EmmaOBaillie
Phone +61 488 584 018
Email ebaillie@netspace.net.au
Security
Data and permissions
Your Twitter data
Log out

2fa - Twitter

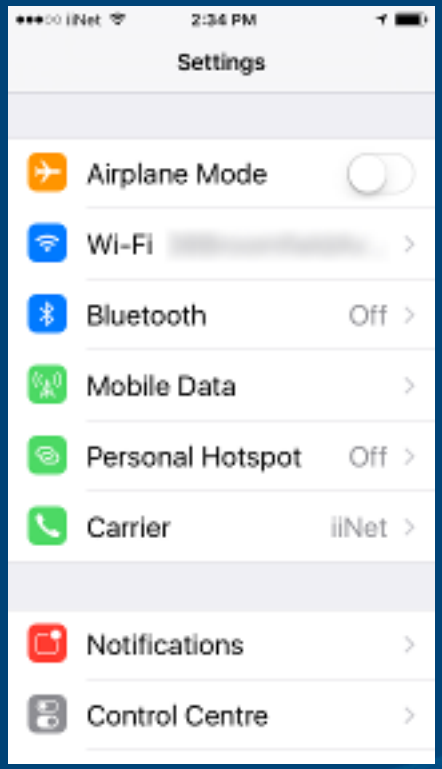

●●○○○ iiNet 3:01 pm 72%
Security
@EmmaOBaillie
Login verification
Login code generator
Backup code
Temporary password

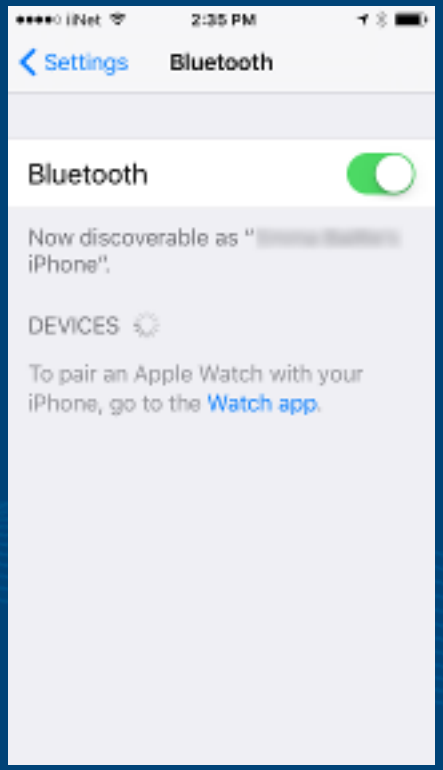

●●○○○ iiNet 3:02 pm 72%
Login code generator
@EmmaOBaillie
Enter this code to complete login to your Twitter account.
545 096
This code will update every 30 seconds.
You can also use a third party authenticator app to generate login verification codes. Learn more

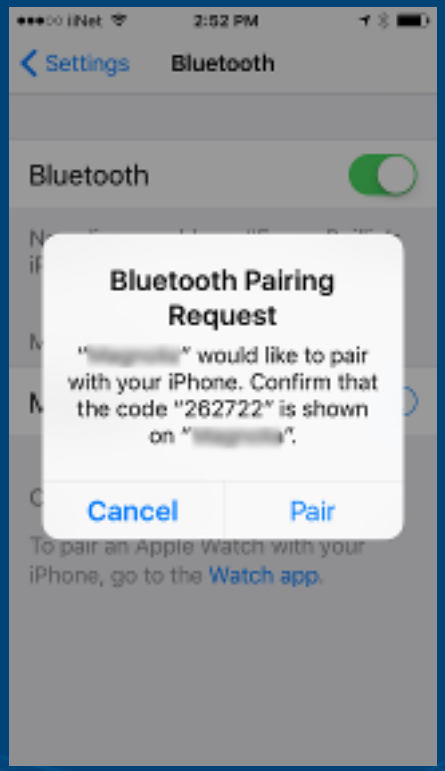

●●●○○ iiNet 3:13 pm 69%
Cancel
We've texted you a login verification code.
Please check your phone with number ending in 18 for a six-digit code and enter it in the box below to log in.
You may also generate a code using the Login code generator in the Twitter app on your iOS / Android device. This works even when your device is offline.
Enter code
Submit
You can also use a saved backup code to log in.
Need help? Please contact Twitter Support.

Bonus Track: Turn off Bluetooth

Bluetooth in your phone's settings







With special thanks to the following for material that has been adapted and incorporated:

TROPE: Teachers' Resources for Online Privacy Education, which is supported by a grant from the National Science Foundation: DGE-1419319, with additional support from NSF grants EEC-1405547 and CCF-0424422 and from IISME. Any opinions, findings, and conclusions or recommendations are those of the originators and do not necessarily reflect the views of the National Science Foundation.

Thoughtworks workshop training CryptoParty Melbourne trainers