THE UNIVERSITY OF MELBOURNE

Privacy Lecture 2

Your private data is valuable and, doing a Security Audit (cont.)

Dr Suelette Dreyfus
Department of Computing and Information Systems

1. Your data is valuable to you – and others
   - Dollar vs Data
2. The value of privacy, as provided by security, on society and particularly commerce
   - Some good old fashion hard data about what happens to consumers and commerce relating to security/privacy
3. Australian Privacy Principals - Overview
4. Part 2 of our Privacy Audit continues
5. Bonus Track – Extra Privacy and Security Steps

In every community, there is a necessary balance between the rights of the citizen and **companies**.. particularly around privacy

Is ours out of balance?

Dollar vs Data Experiment

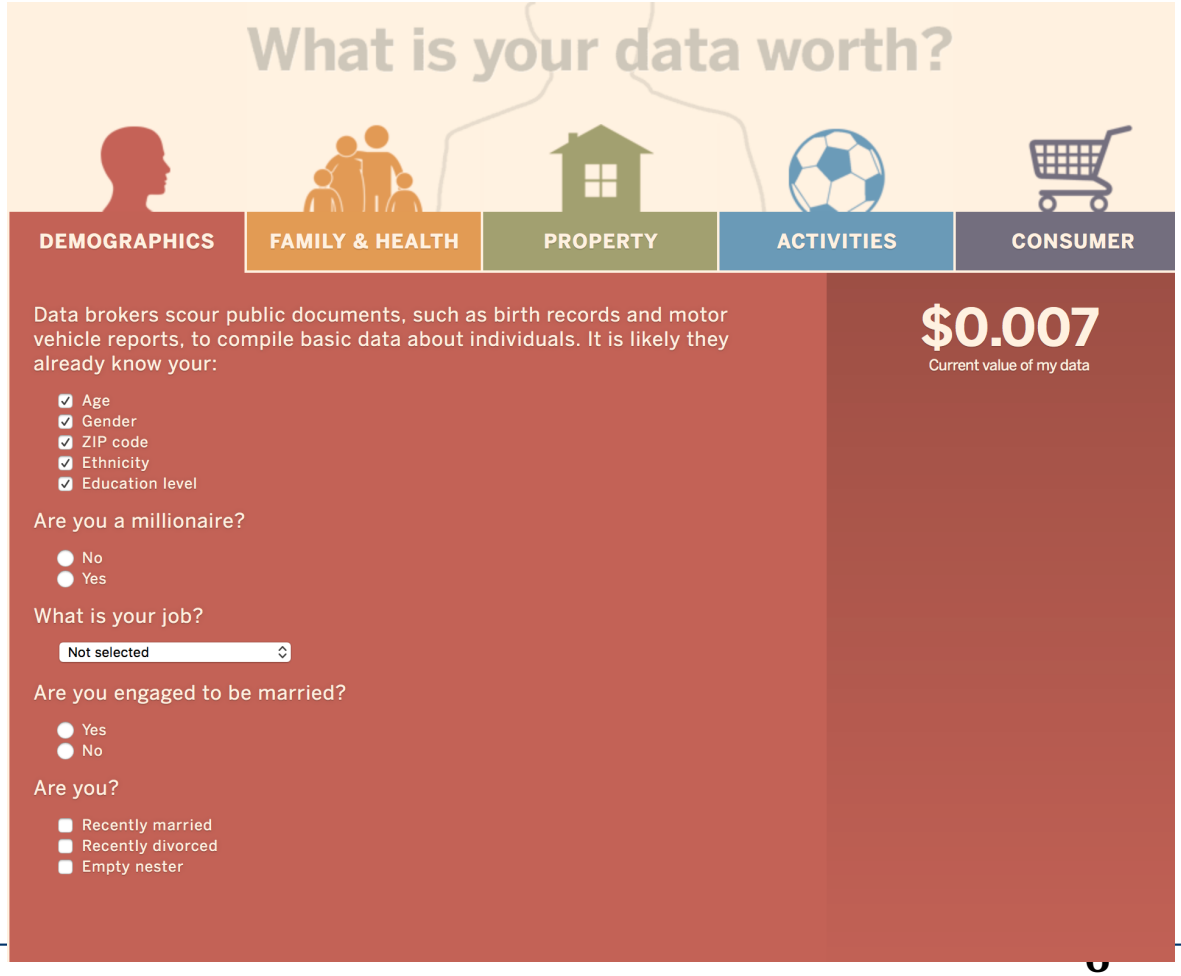
- How much is your personal information worth?
- Question: name 3 characteristics that increase the value of your data?

- **Name a piece of private info available about you that is actually online and is valuable?**
- How could this piece of information be valuable to others? Who do you think could use that information?
  - Institutions? Companies? The government? Your friends and family? Cybercriminals?
- What could they use it for?
- Would those ways of using your data help you? Hurt you? Neither?

Now Let's Test it!

http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html?ft_site=falcon

Or Search: 'How much is your personal data worth?' and FT



Customer privacy and security: Issues for business

- Customers want to feel their data is secure from unauthorised access, and their privacy is intact
- Ways of ensuring privacy through better security can be heavy-handed and clunky for the average user
- This puts them off – sometimes leading them to choose less secure options.. Thus risking their privacy
- Two issues: Integrity of the company 'harvesting' the data and using it **vs** Integrity/protection of that data from others

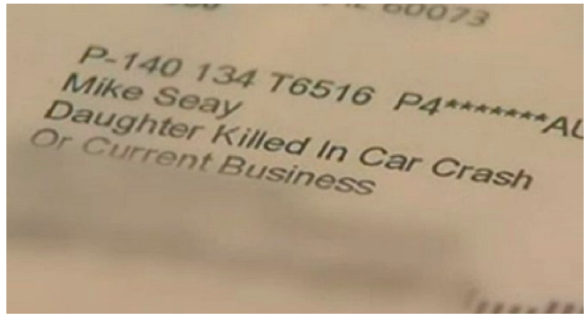
What data does the reseller have?

JAN 22, 2014 @ 12:09 PM 13,291 VIEWS The Little Blac

OfficeMax Blames Data Broker For 'Daughter Killed in Car Crash' Letter

Kashmir Hill, FORBES STAFF

Welcome to The Not-So Private Parts where technology & privacy collide FULL BIO



Yikes.

OfficeMax OMX +% is getting a lot of press these days and it has little to do with its office supply deals. It was a little too specific in targeting one of its customers, sending a mailing to a Chicago man named Mike Seay addressed to "Daughter Killed in Car Crash or Current Business." Seay's teenage daughter had been killed in a car accident a year earlier, as reported by NBC News. This was obviously traumatic for him.

US Company OfficeMax's #PRFail showed just how much data is gathered and sold on us all – and how very personal it can be.

Advertising mail out to:
"Daughter Killed in Car Crash or Current Business"
Seay's teenage daughter had been killed in a car accident

Hill, K. 2014. 'OfficeMax blames data broker for 'Daughter killed in car crash' letter', *Forbes*, Jan 22. See: http://www.forbes.com/sites/kashmirhill/2014/01/22/officemax-blames-data-broker-for-daughter-killed-in-car-crash-letter/#19458a786b0d

Even if the data kept is appropriate, is it secure 'enough' for 'privacy'?

Increasing large scale data breaches .. Leads to:

- Put higher security burdens on clients
- Leads to a diminished user-experience for the customer with the company
- On average, clients must remember more than 14 passwords
- Despite this, consumer perception of security have gotten worse!
- Issues around Digital security and privacy 'are eroding consumer trust online'

Source: Hasham, S. et al 2016. 'Is cybersecurity incompatible with digital convenience?,' McKinsey & Co. August. See: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/is-cybersecurity-incompatible-with-digital-convenience?cid=other-eml-alt-mip-mck-oth-1608

THE UNIVERSITY OF MELBOURNE

Erosion of consumer trust: The importance of Privacy and Security

What % of online households reported that concerns about online privacy and security stopped them from:

- Conducting financial transactions
- OR Buying goods or services
- Or posting on social networks
- OR Expressing opinions on controversial or political issues via the internet?

45%

Source: Goldberg, R. 2016. 'Lack of trust in internet privacy and security may deter economic and other online activities.' National Telecommunications & Information Administration, US Dept of Commerce. See: https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities

New realities for consumer behaviour online – Privacy and Security

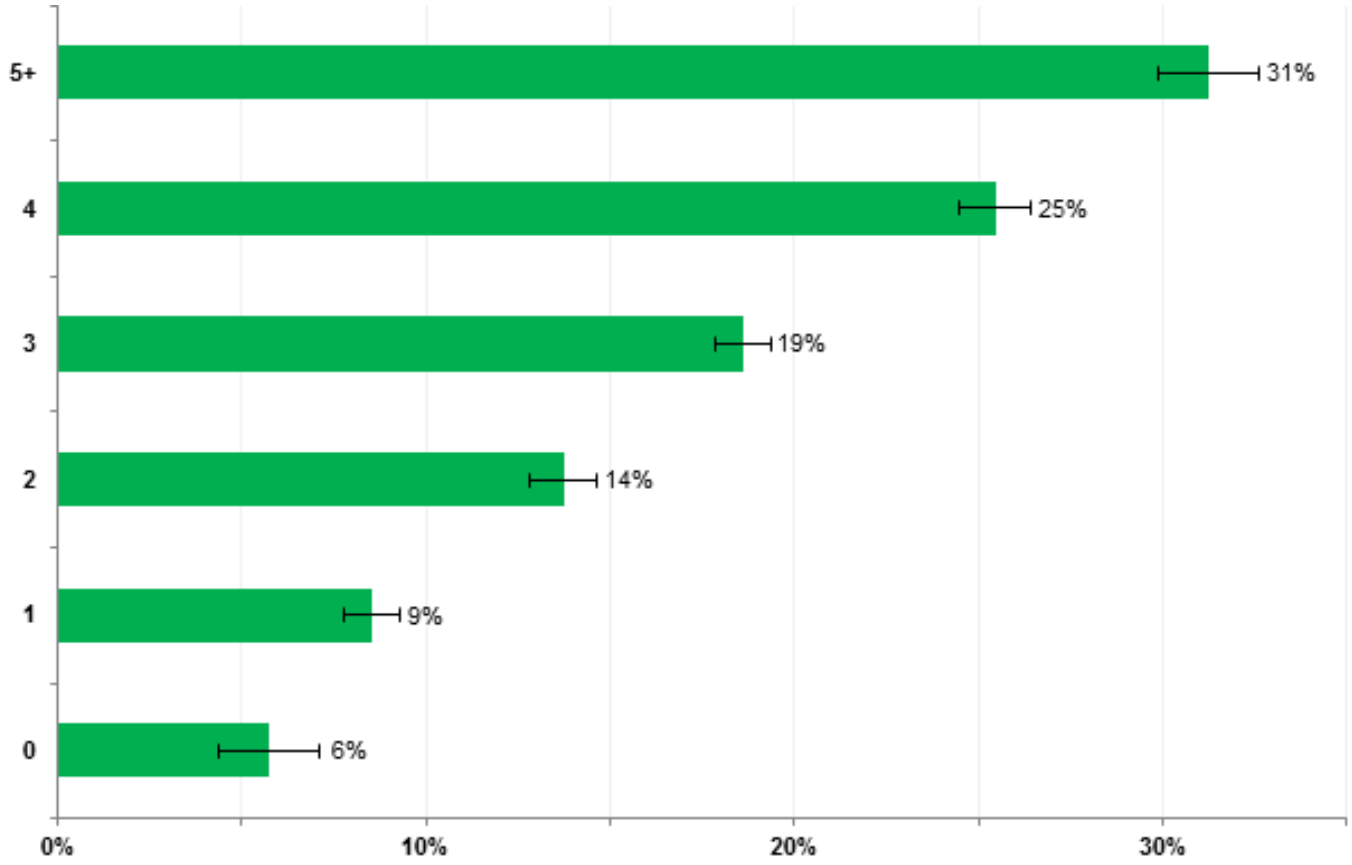
- 19% of Internet-using households (almost 19 million Americans) reported being impacted by an online security breach, identity theft or similar malicious activity during the 12 months before the July 2015 survey.
- 22% of Internet-using households that used a mobile data plan to go online outside the home experienced an online security breach.
- 84% of households had at least one specific privacy or security concern–and 40% had at least two.

Source: Goldberg, R. 2016. 'Lack of trust in internet privacy and security may deter economic and other online activities.' National Telecommunications & Information Administration, US Dept of Commerce. See: https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities

THE UNIVERSITY OF MELBOURNE

Internet Household reporting online security breaches

of different types of devices used in a household



Source: Goldberg, R. 2016. 'Lack of trust in internet privacy and security may deter economic and other online activities.' National Telecommunications & Information Administration, US Dept of Commerce. See: https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities

Internet Household reporting online security breaches

"Perhaps the most direct threat to maintaining consumer trust is negative personal experience."

"Security breaches appear to be more common among the most intensive Internet-using households."

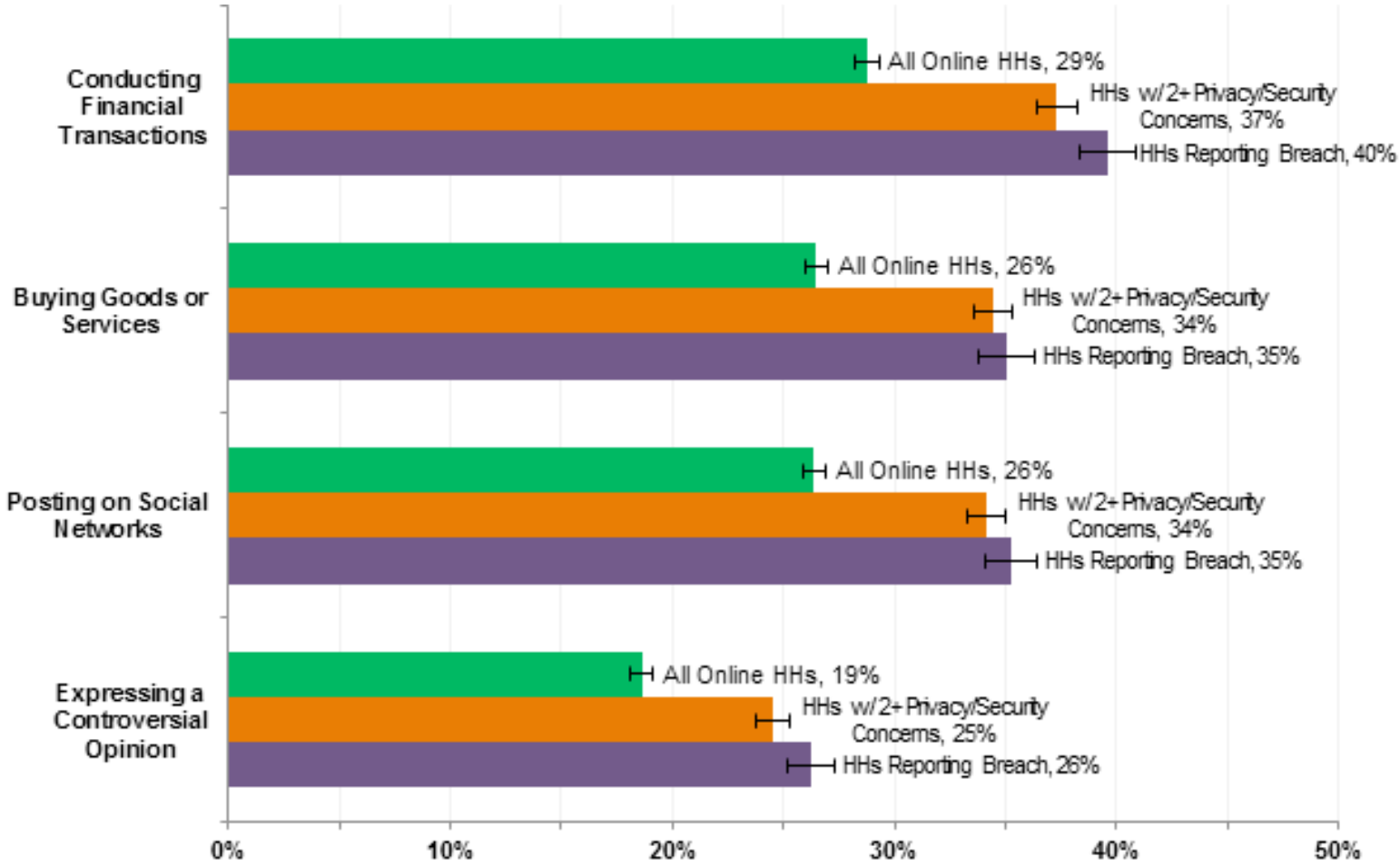
Source: Goldberg, R. 2016. 'Lack of trust in internet privacy and security may deter economic and other online activities.' National Telecommunications & Information Administration, US Dept of Commerce. See: https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities

THE UNIVERSITY OF MELBOURNE

Avoided online activities due to privacy and security concerns

Types of online transactions

"HH" are % of households with internet users



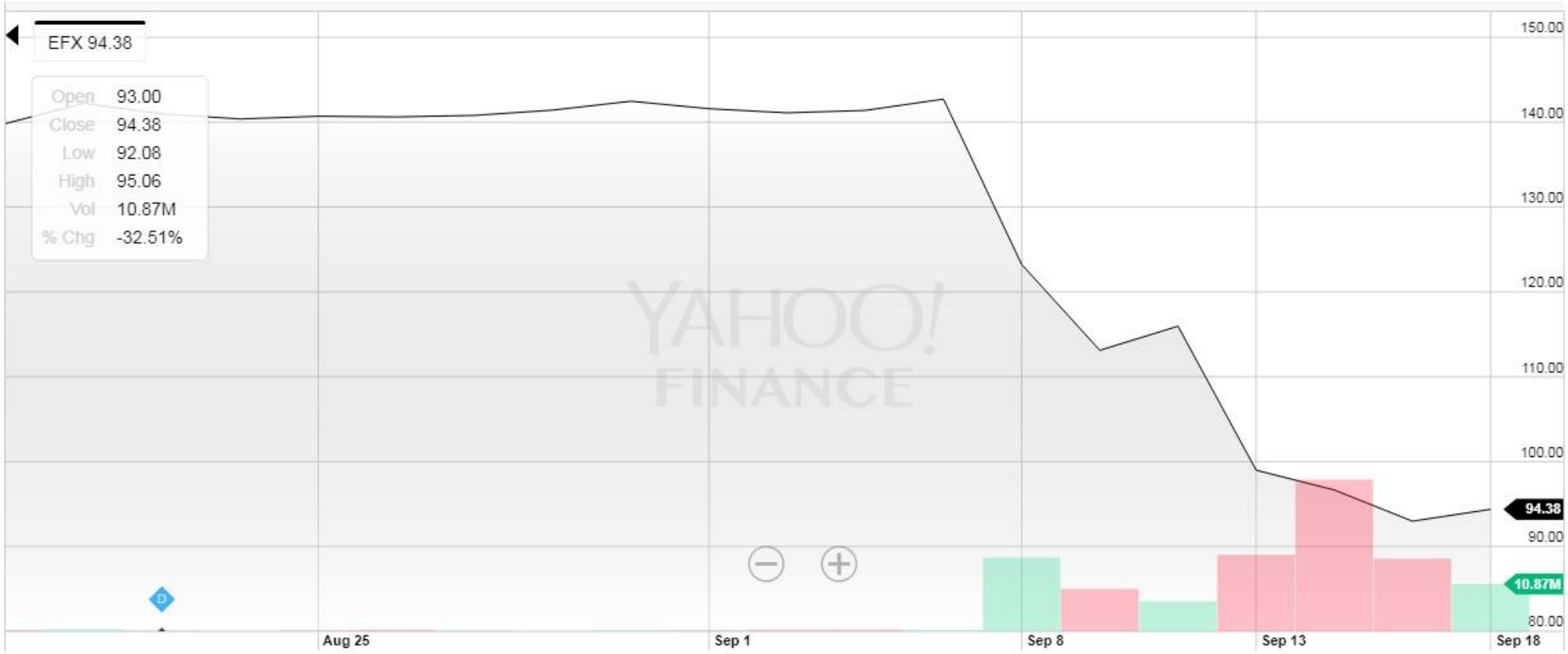
Source: Goldberg, R. 2016. 'Lack of trust in internet privacy and security may deter economic and other online activities.' National Telecommunications & Information Administration, US Dept of Commerce. See: https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities . Note: % of households with internet users

Equifax Case Study

- Equifax has said that the breach that exposed sensitive data for as many as 143 million US consumers started on May 13 and lasted until July 30.
- The company didn't disclose the breach until September 7.
- Used a critical vulnerability in the Apache Struts Web app framework – already an exploit in the wild being used at the time – let hackers get foothold
- Known bug, trivial to exploit = reporting of string of attacks in MARCH. Open Source project had patched vulnerability then. 2 x working exploits were publically available.
- PATCH, PATCH, PATCH!

Equifax:

Case Study:
The financial impact of breached data security on a company



Trade offs between privacy/security and convenience: what customers say in the commercial world

- 30% prioritize ease and convenience over security
- Want 'basic level' operating behind the scenes but say 'having access to account information without the need to enter a password (eg with automatic device recognition) is attractive or very attractive.'
- Reject notion of a 'one-time password sent to them for every login'

Source: Hasham, S et al. 2016. 'Is cybersecurity incompatible with digital convenience?' McKinsey&Co. See: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/is-cybersecurity-incompatible-with-digital-convenience?cid=other-eml-alt-mip-mck-oth-1608.

THE UNIVERSITY OF MELBOURNE

How to keep privacy through good security with high adoption among users

- ‘Device or number recognition and omnichannel authentication (customers do not want to be treated like strangers just because they are on a different device)’
- ‘The remaining 20 percent prefer a verification phone call.’
- ‘Log-in credentials should be the same across all channels; allow for customers to log in on one channel in order to use another, eliminating duplicative authentications’

Source: Hasham, S et al. 2016. ‘Is cybersecurity incompatible with digital convenience?’ McKinsey&Co. See: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/is-cybersecurity-incompatible-with-digital-convenience?cid=other-eml-alt-mip-mck-oth-1608.

How to get high adoption of privacy-enhancing good security among users (Continued)

- Better visual user experience matters.
- 'Inconsistent design, poor error messaging, clunky comms, site slowness or unavailability' make it less appealing to the end user to accept security that will improve their privacy

Source: Hasham, S et al. 2016. 'Is cybersecurity incompatible with digital convenience?' McKinsey&Co. See: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/is-cybersecurity-incompatible-with-digital-convenience?cid=other-eml-alt-mip-mck-oth-1608.

Privacy Policy

- A company's **privacy policy** describes how it gathers, uses, discloses, and manages a customer's information.

Australian Privacy Principles – Legal Background

- Australian Information Commissioner Act
- The *Australian Information Commissioner Act 2010* (AIC Act) establishes the Office of the Australian Information Commissioner (OAIC).
  three primary functions:
  - **privacy** functions, conferred by the *Privacy Act 1988* (Privacy Act) and other laws
  - **freedom of information** functions, in particular, oversight of the operation of the *Freedom of Information Act 1982* (FOI Act) and review of decisions made by agencies and ministers under that Act
  - **government information policy** functions, conferred on the Australian Information Commissioner under the *Australian Information Commissioner Act 2010* (AIC Act).

Australian Privacy Principles – Legal Background

- "Australian Privacy Principles (APPs), in schedule 1 of the *Privacy Act 1988*(Privacy Act), outline how most Australian and Norfolk Island Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses (collectively called 'APP entities') must handle, use and manage personal information.
- APPs are not prescriptive, each APP entity needs to consider how the principles apply to its own situation."

What are the most important principles of privacy?

Exercise: With a partner, think about what areas of information management need to be covered by privacy principles.

THE UNIVERSITY OF MELBOURNE

Australian Privacy Principles -

- APP 1 — Open and transparent management of personal information
- APP 2 — Anonymity and pseudonymity
- APP 3 — Collection of solicited personal information
- APP 4 — Dealing with unsolicited personal information
- APP 5 — Notification of the collection of personal information
- APP 6 — Use or disclosure of personal information
- APP 7 — Direct marketing
- APP 8 — Cross-border disclosure of personal information
- APP 9 — Adoption, use or disclosure of government related identifiers
- APP 10 — Quality of personal information
- APP 11 — Security of personal information
- APP 12 — Access to personal information
- APP 13 — Correction of personal information

Australian Privacy Principles – Not Prescriptive

- "Separate APPs that deal with the use and disclosure of personal information for the purpose of direct marketing (APP 7), cross-border disclosure of personal information (APP 8) and the adoption, use and disclosure of government related identifiers (APP 9)."
- more stringent obligations on APP entities who handle 'sensitive information':
  - health (including predictive genetic information)
  - racial or ethnic origin
  - political opinions
  - membership of a political association, professional or trade association or trade union
  - religious beliefs or affiliations
  - philosophical beliefs
  - sexual orientation or practices
  - criminal record
  - biometric information that is to be used for certain purposes
  - biometric templates.

Malicious damage to assets – in less than 60 seconds

USB Kill Video

https://www.youtube.com/watch?v=3hbuhFwFsDU

The Importance of Encryption in Email to Privacy

- **"The security of people's communication is very important to me"**
  - Edward Snowden's first email approach to journalist Glenn Greenwald

"The email's .. stated purpose was to urge me to begin using PGP encryption so that 'Cincinnatus' could communicate things in which, he said, he was certain I would be interested."

- Glenn Greenwald in '*No place to hide*'

THE UNIVERSITY OF MELBOURNE

Why Security Audit again?

Laura,

At this stage I can offer nothing more than my word. I am a senior government employee in the intelligence community. I hope you understand that **contacting you is extremely high risk** and you are willing to agree to the following precautions before I share more. This will not be a waste of your time.

The following sounds complex, but should only take minutes to complete **for someone technical**. I would like to confirm out of email that the keys we exchanged were not intercepted and replaced by your surveillants. Please confirm that no one has ever had **a copy of your private key** and that it uses a **strong passphrase**. Assume your adversary is capable **of one trillion** guesses per second. If the device you store the private key and enter your passphrase on has been hacked, it is trivial to decrypt our communications.

Understand that the above steps are not bullet proof, and are intended only to give us breathing room. In the end if you publish the source material, I will likely be immediately implicated. This must not deter you from releasing the information I will provide.

Thank you, and be careful.

Citizen Four

Big Five – Security Audit (Revisited)

1. Time to complete our Role-Play Security Audit!

2. This is how you make sure someone's system is secure – hands on learning to 'cement' the concepts in your memory, (and get some practical skills in the meantime)

3. Find your buddy (same or new), choose the opposite role to last time

Big Five – Security Audit (Revisited)

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

THE UNIVERSITY OF MELBOURNE

Encrypt data in Transit: what Encrypted message system? (Desktop & Phone)

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 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.

THE UNIVERSITY OF MELBOURNE

signal

Steps:

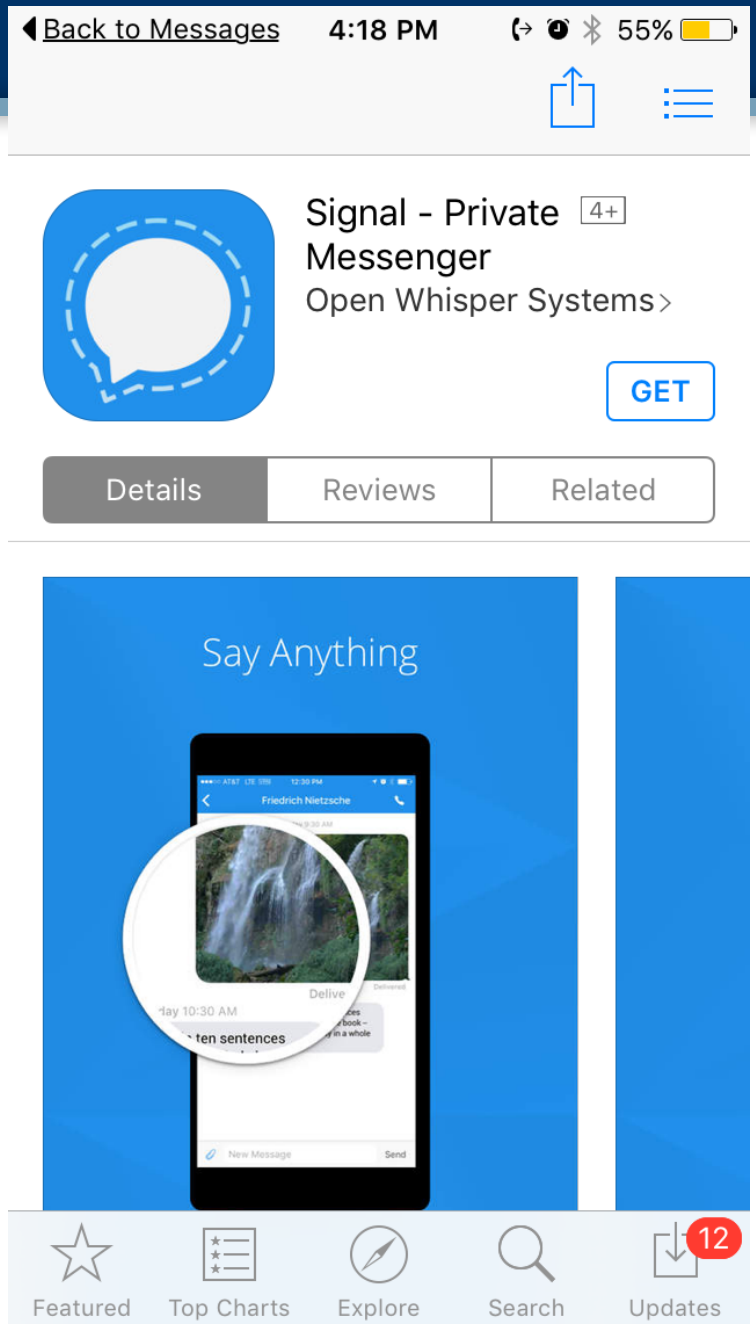
Find a buddy: share phone numbers

Open your App store in your smartphone

Search: Signal Private Messenger (by Whisper Open Systems)

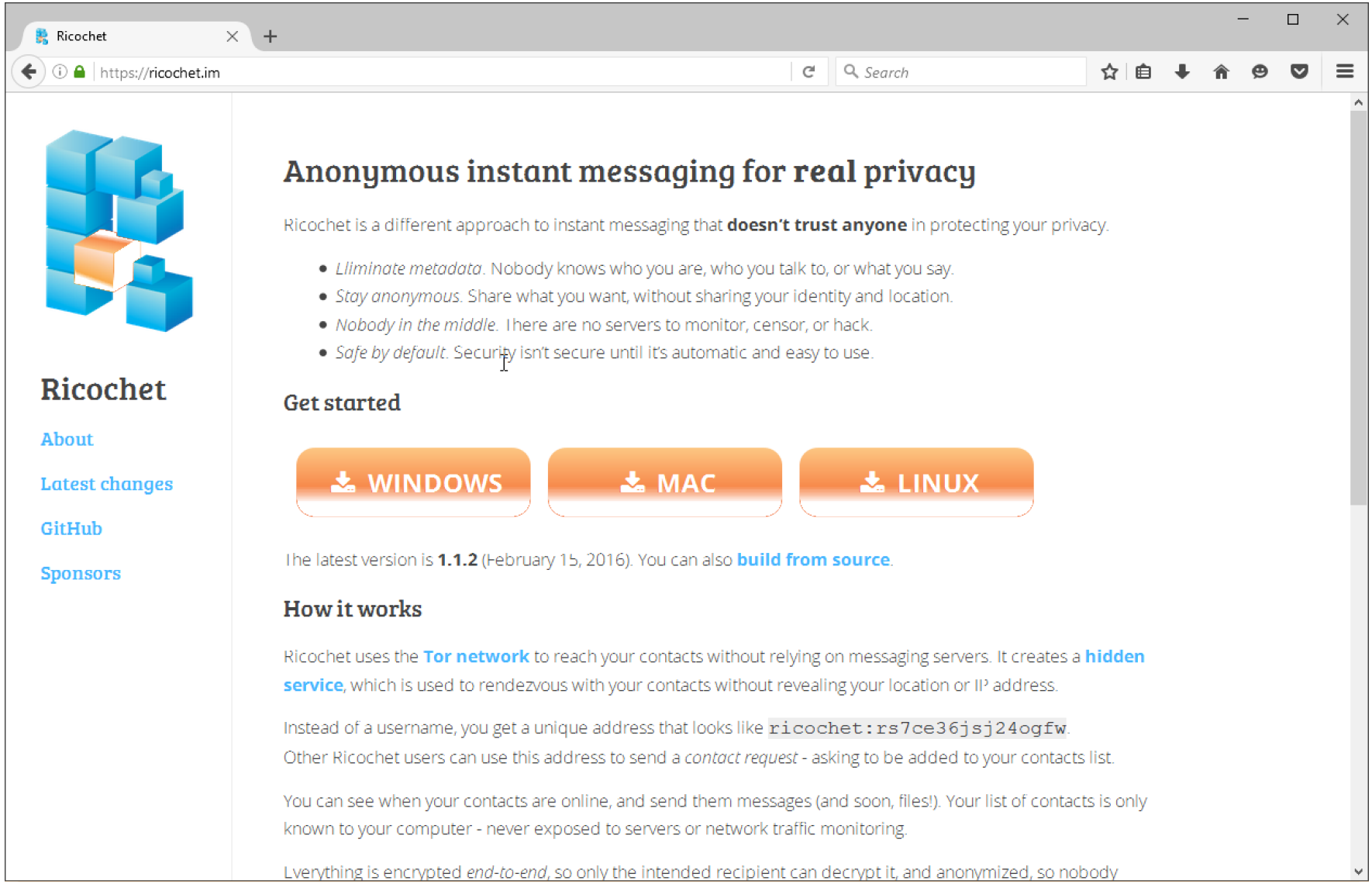
Be sure you get the right App!

Download
Open

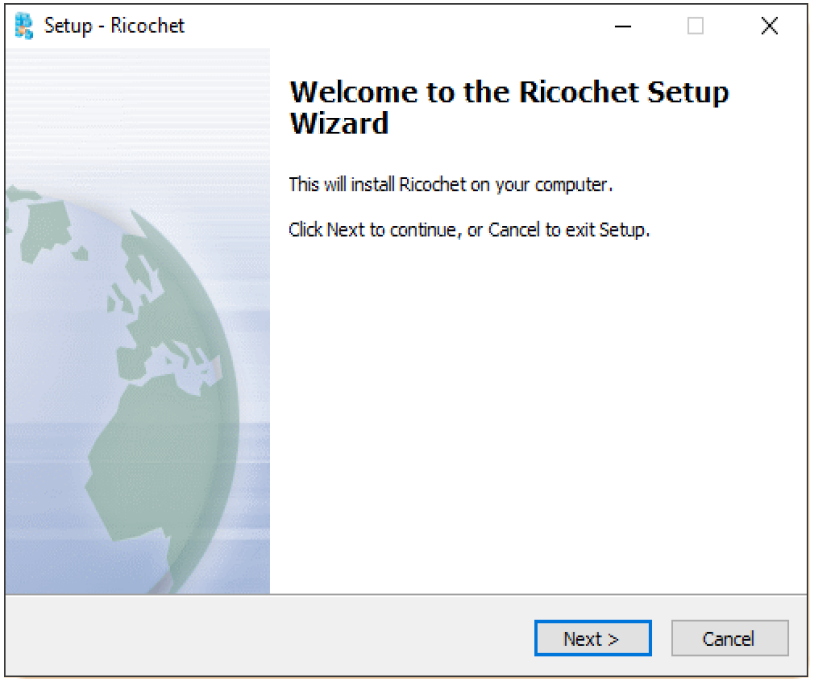


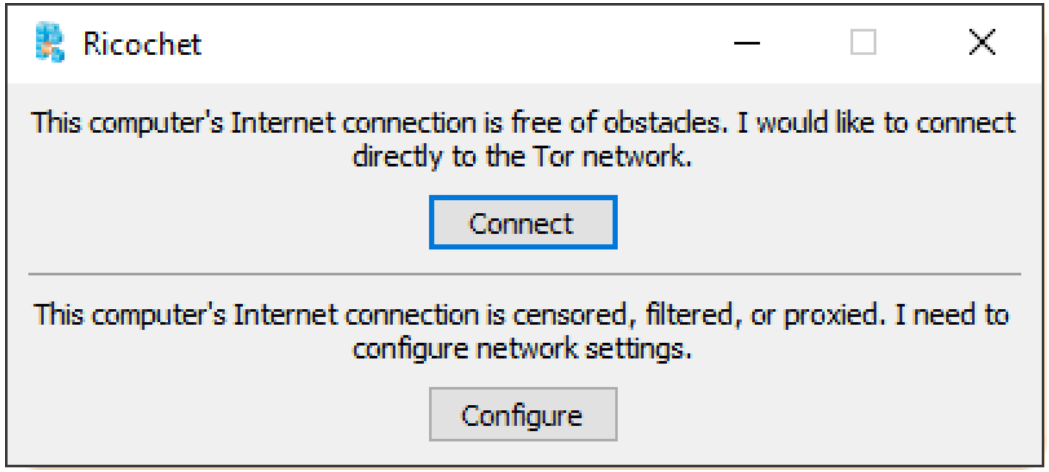
THE UNIVERSITY OF MELBOURNE

Ricochet

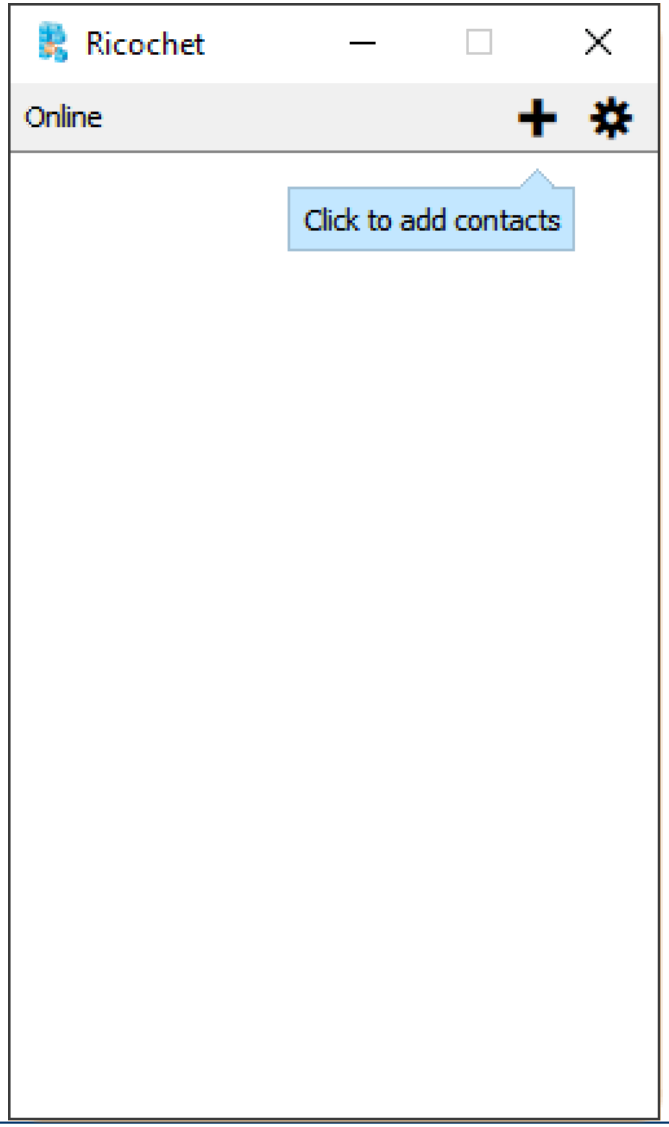


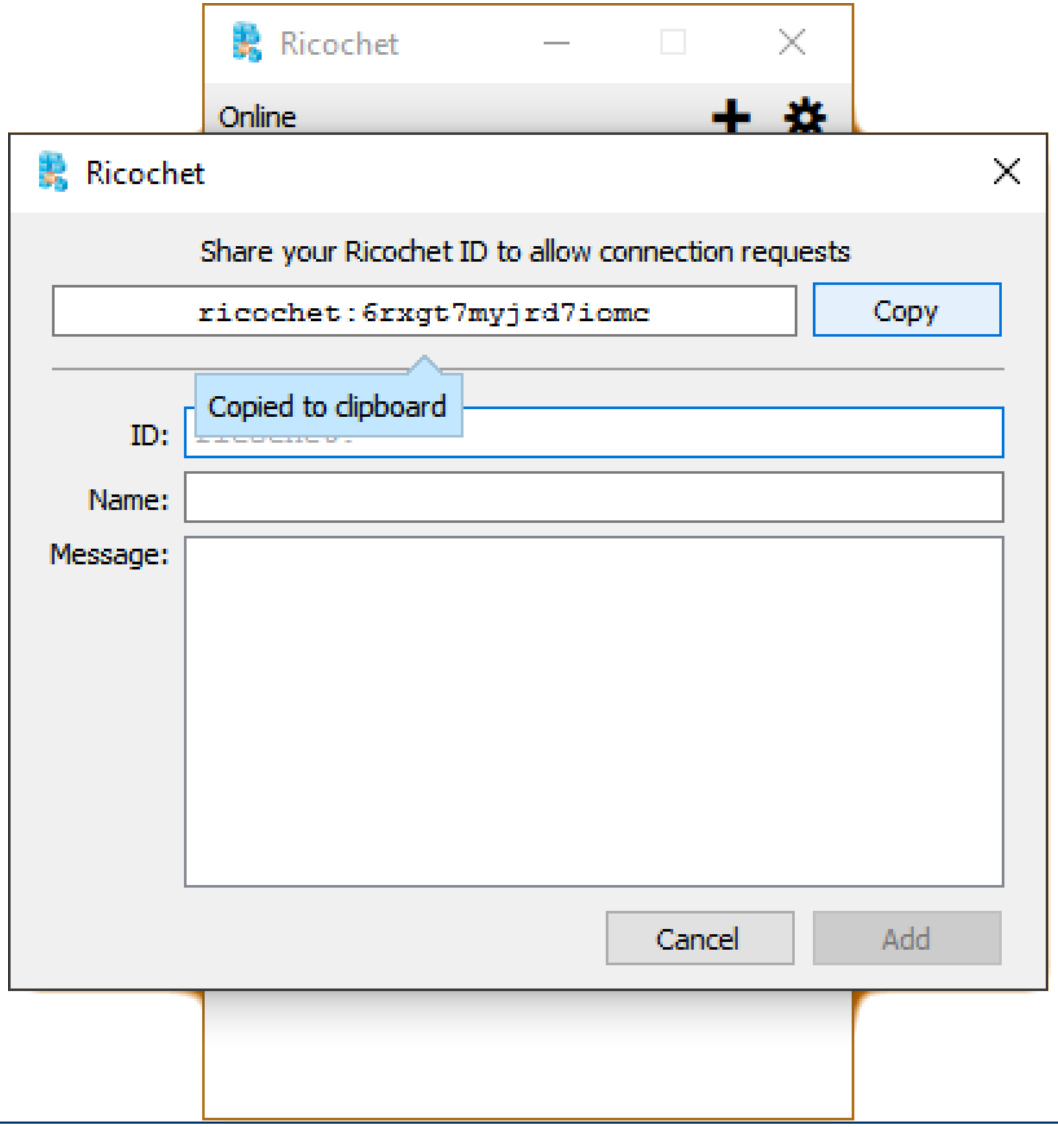
Ricochet


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

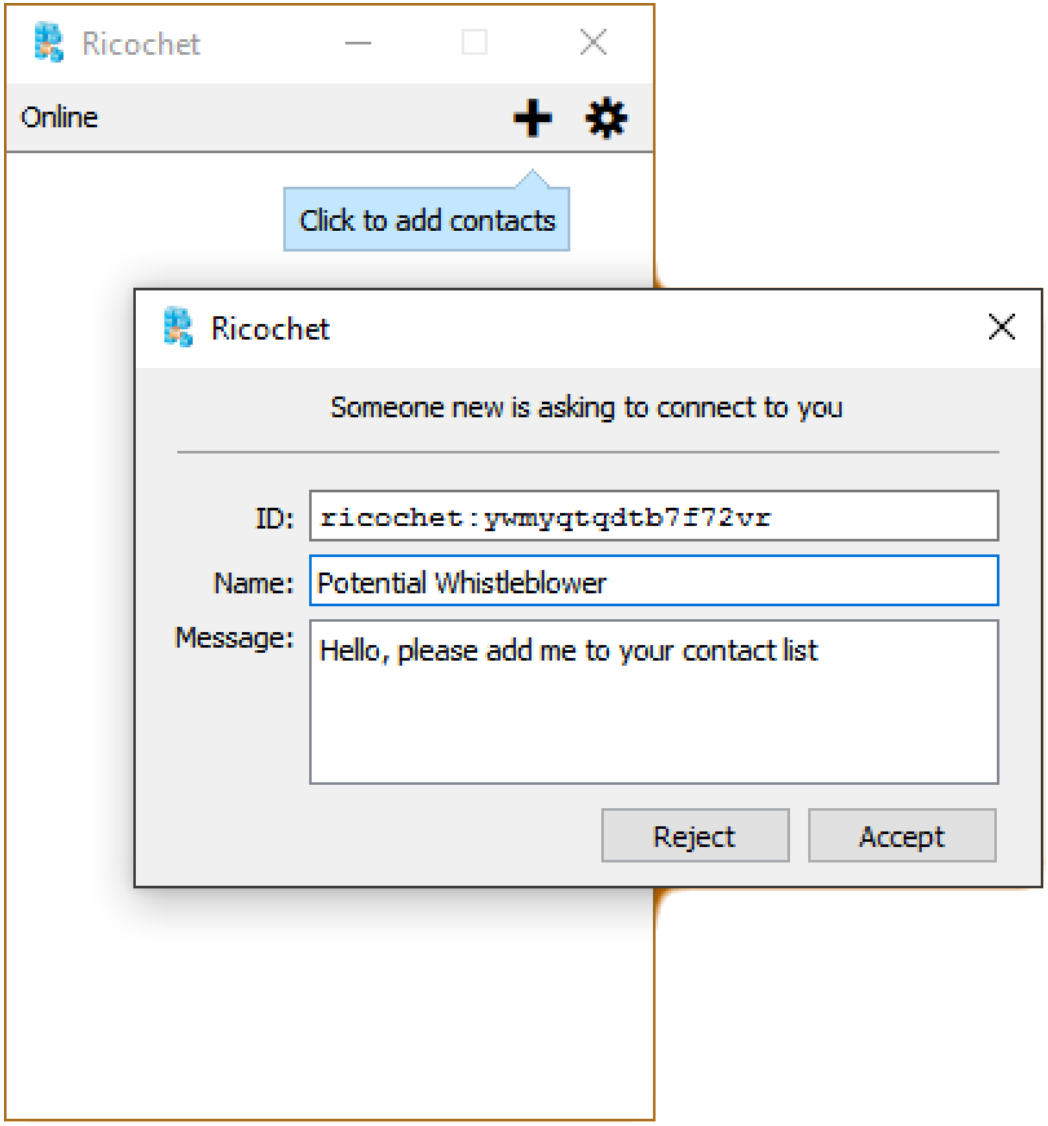

Ricochet
This computer's Internet connection is free of obstacles. I would like to connect directly to the Tor network.
Connect
This computer's Internet connection is censored, filtered, or proxied. I need to configure network settings.
Configure

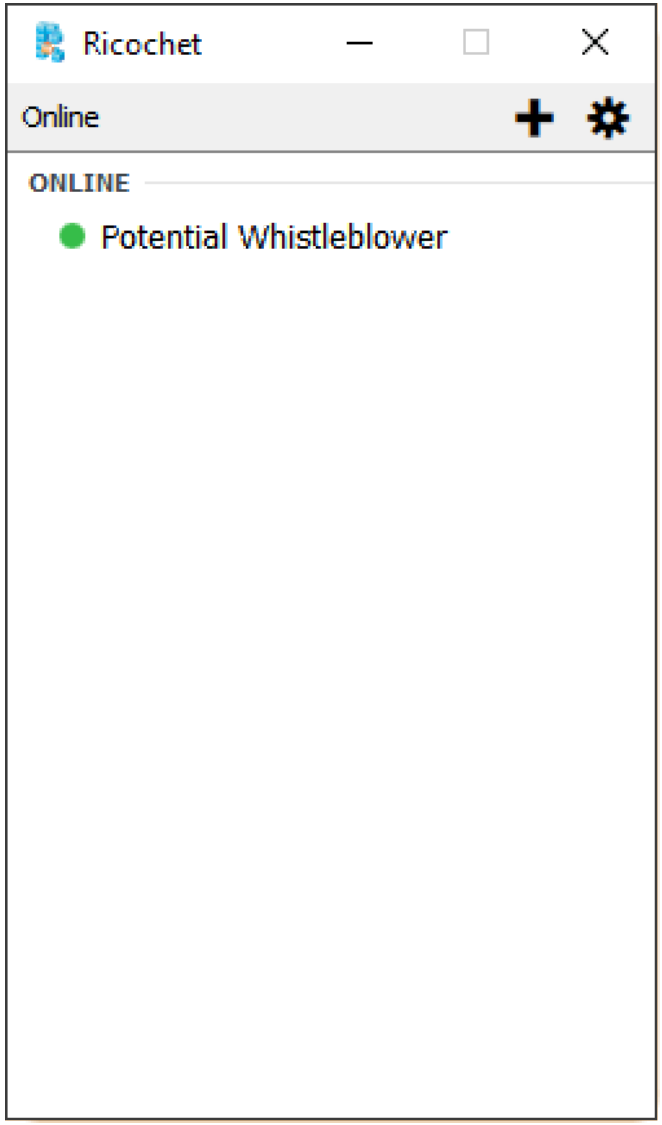
Ricochet


Ricochet
Online
Click to add contacts

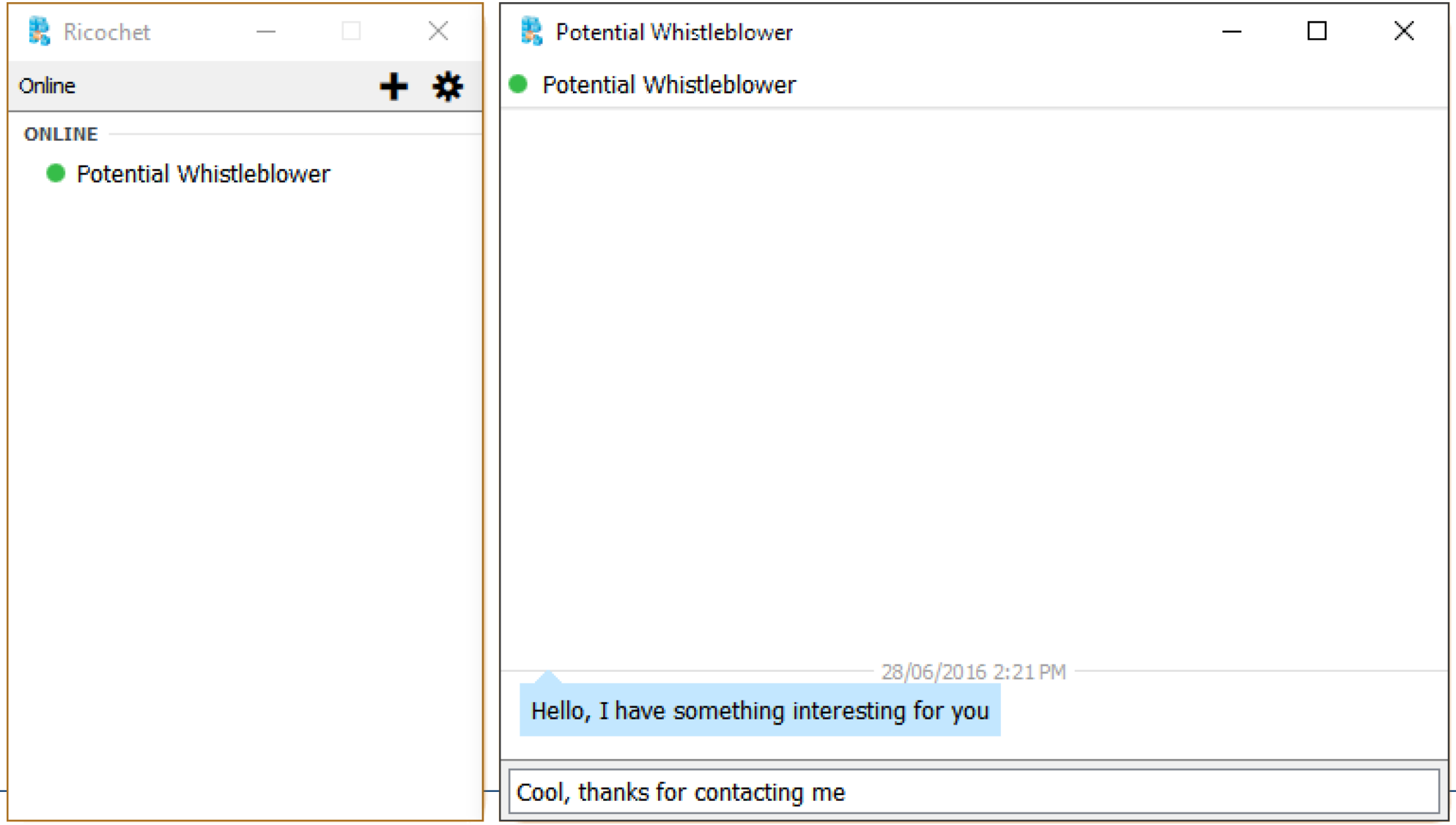

Ricochet
Online
Ricochet
Share your Ricochet ID to allow connection requests
ricochet:6rxgt7myjrd7iomc
Copy
Copied to clipboard
ID:
Name:
Message:
Cancel
Add

Ricochet

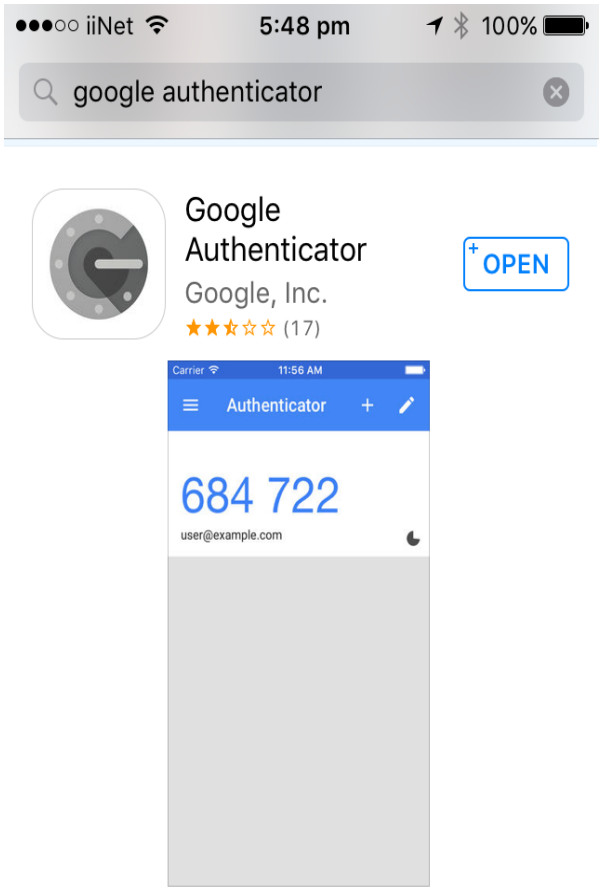

Ricochet
Online
Click to add contacts
Ricochet
Someone new is asking to connect to you
ID:
ricochet:ywmyqtqdtb7f72vr
Name:
Potential Whistleblower
Message:
Hello, please add me to your contact list
Reject
Accept

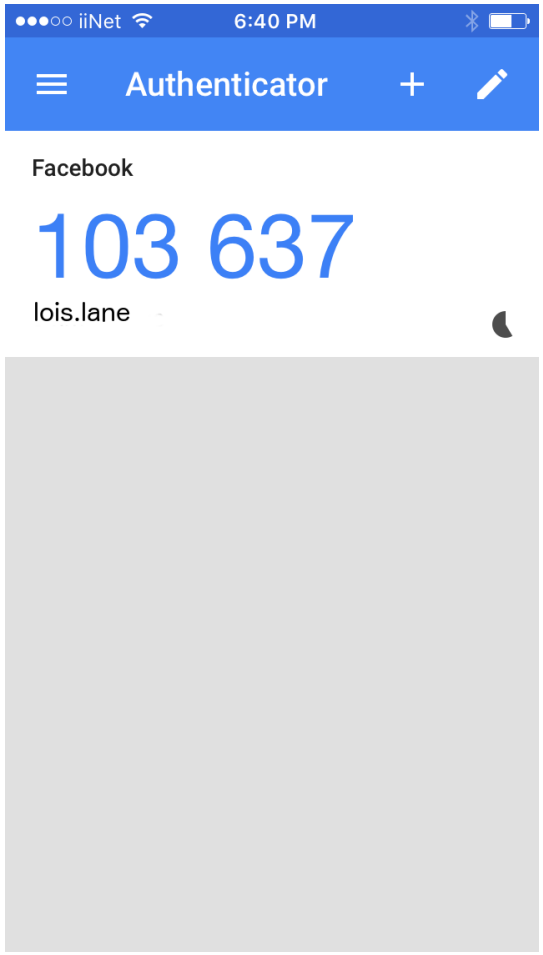

Ricochet
Online
ONLINE
Potential Whistleblower

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

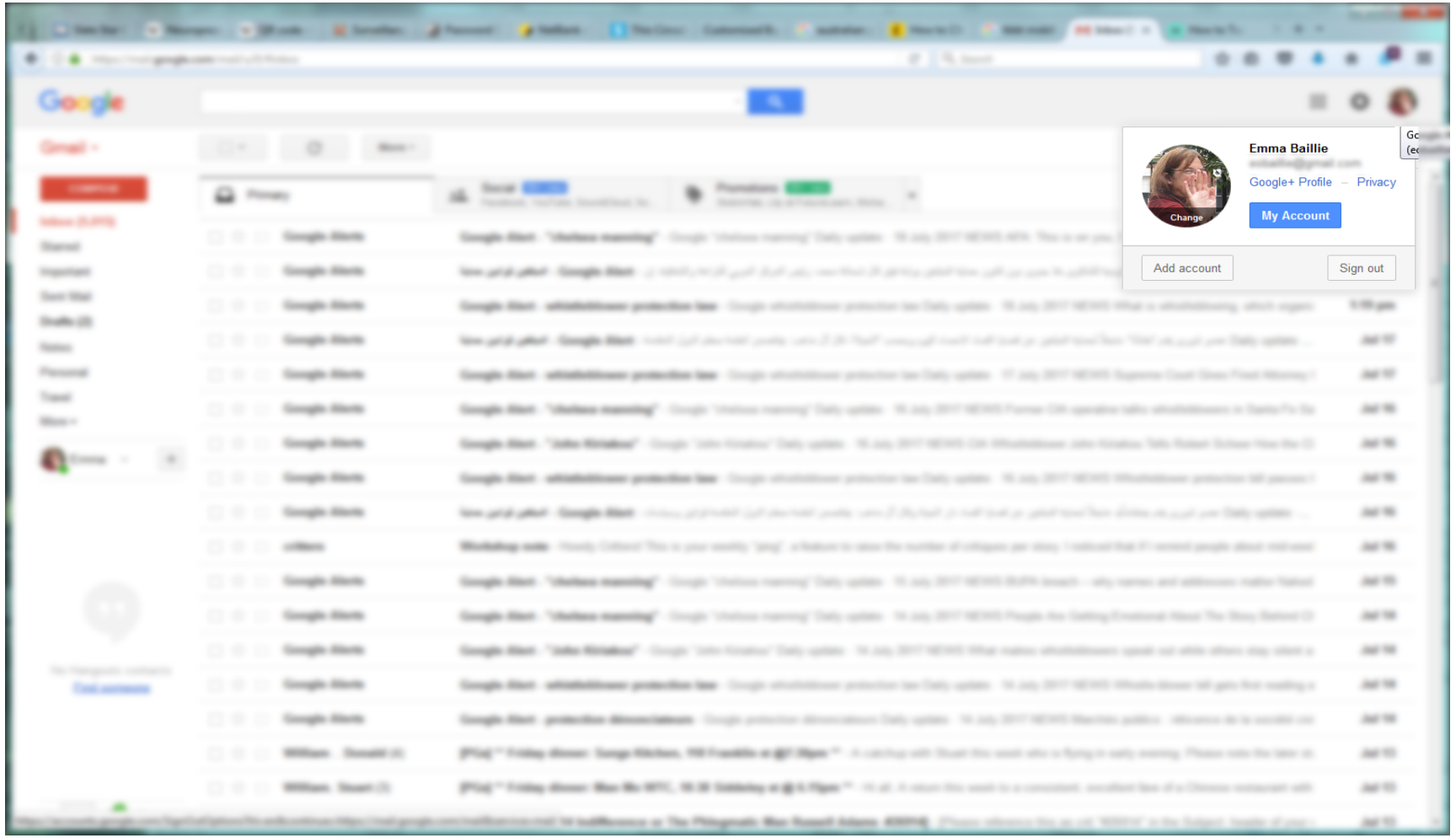
OTP for mfa - Google Authenticator





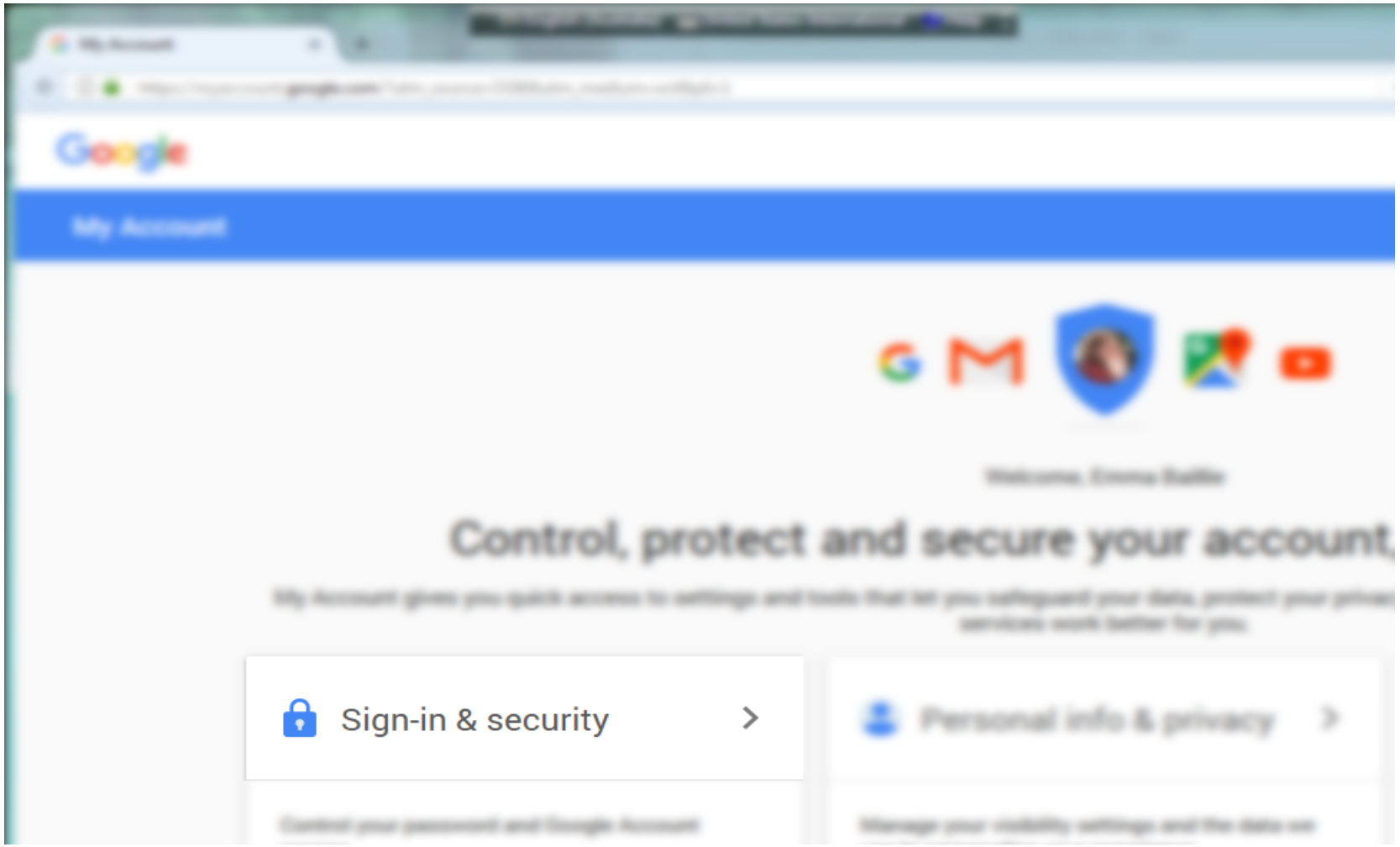
THE UNIVERSITY OF MELBOURNE

2 Factor Authentication - Gmail



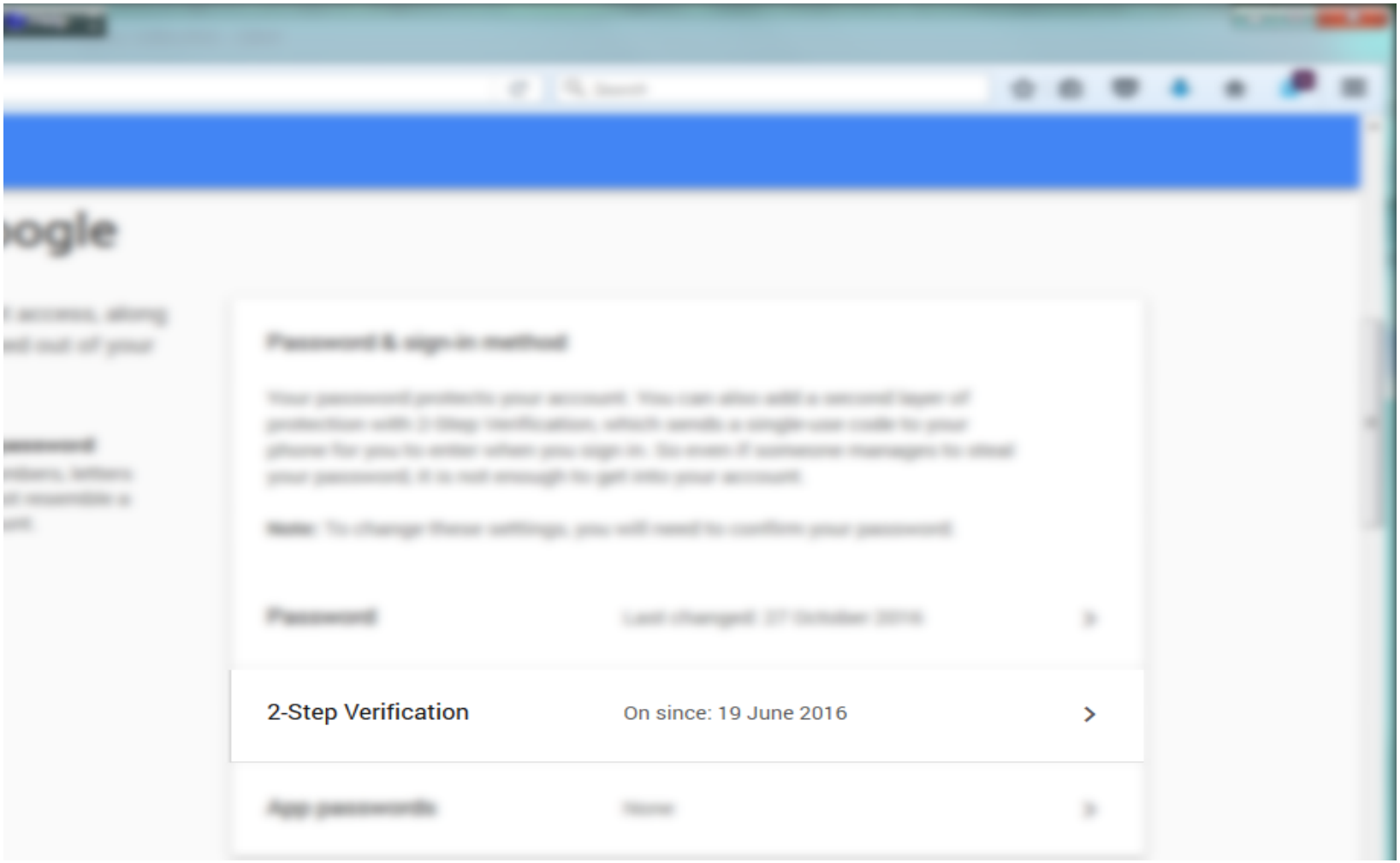
THE UNIVERSITY OF MELBOURNE

2fa - gmail

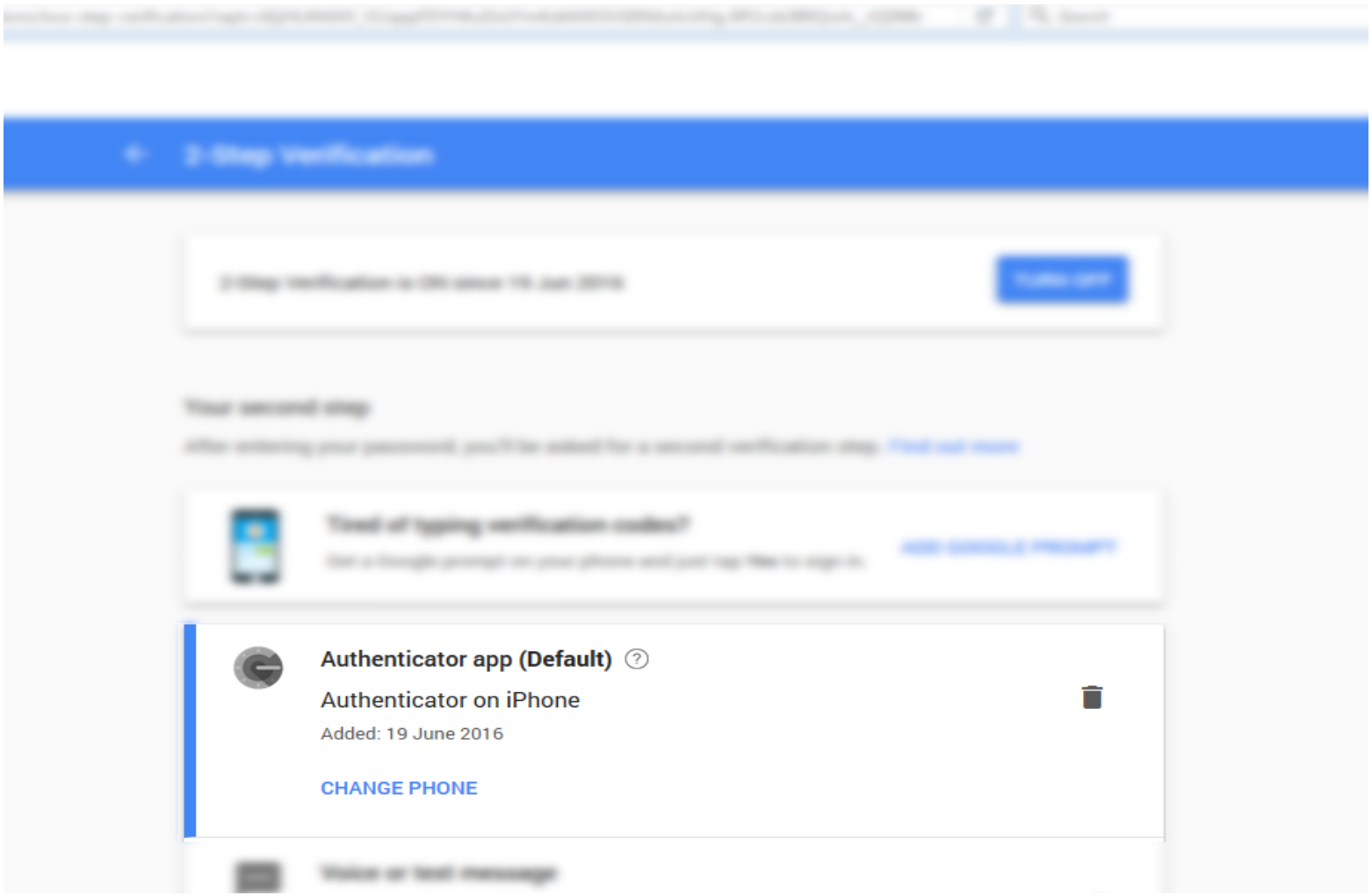


THE UNIVERSITY OF MELBOURNE

2fa - gmail



2fa - gmail


2-Step Verification
Your second step
Authenticator app (Default)
Authenticator on iPhone
Added: 19 June 2016
CHANGE PHONE

THE UNIVERSITY OF MELBOURNE

2fa – gmail – Recovery codes

Set up alternative second step

Set up at least one backup option so that you can sign in even if your other second steps aren't available.

Backup codes

These printable one-time passcodes allow you to sign in when away from your phone, like when you're traveling.

SET UP

Google prompt

Get a Google prompt on your phone and just tap **Yes** to sign in.

ADD PHONE

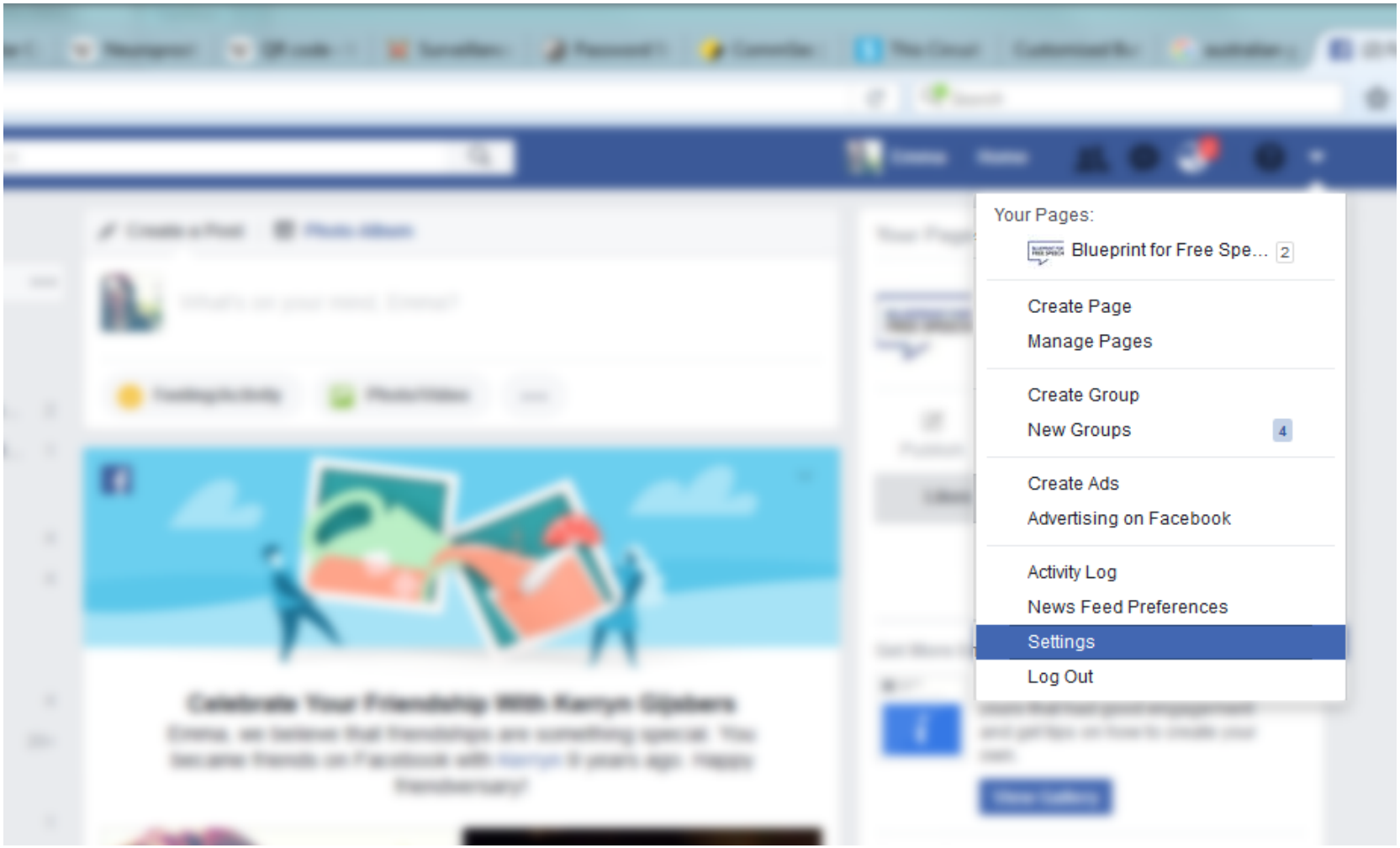
Security Key

A Security Key is a small physical device used for signing in. It plugs into your computer's USB port. Learn more

ADD SECURITY KEY

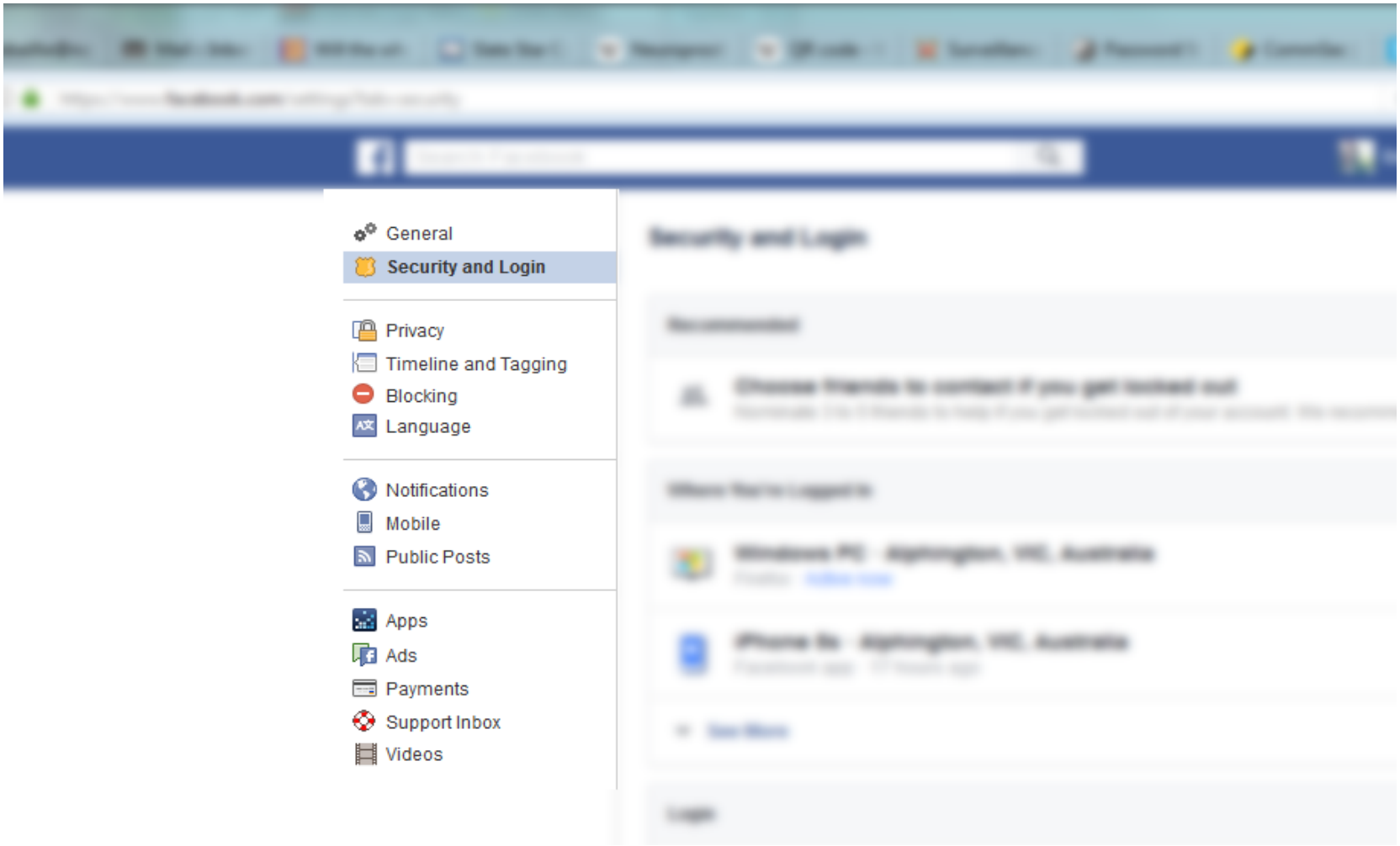
THE UNIVERSITY OF MELBOURNE

2fa - Facebook



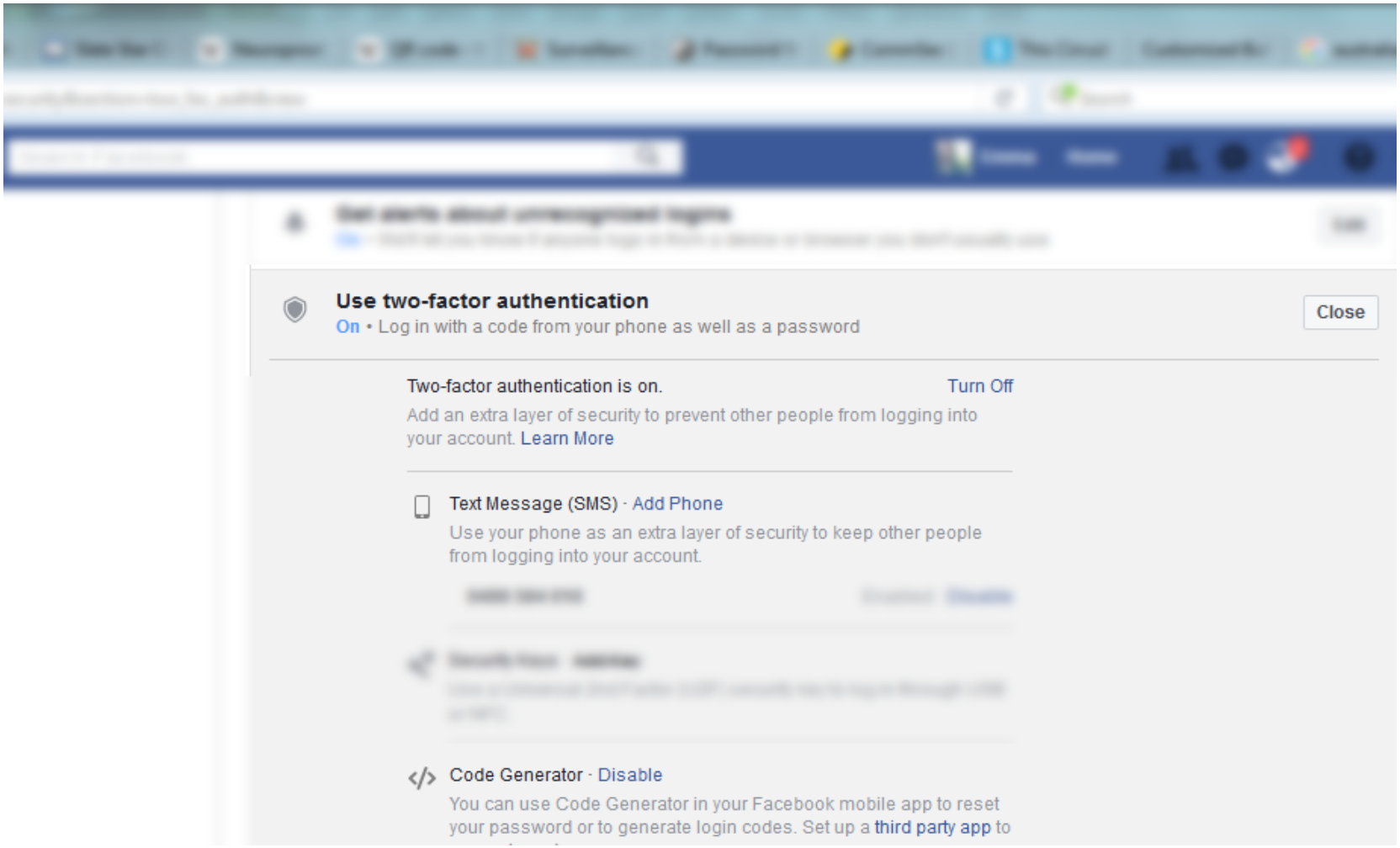
THE UNIVERSITY OF MELBOURNE

2fa - Facebook



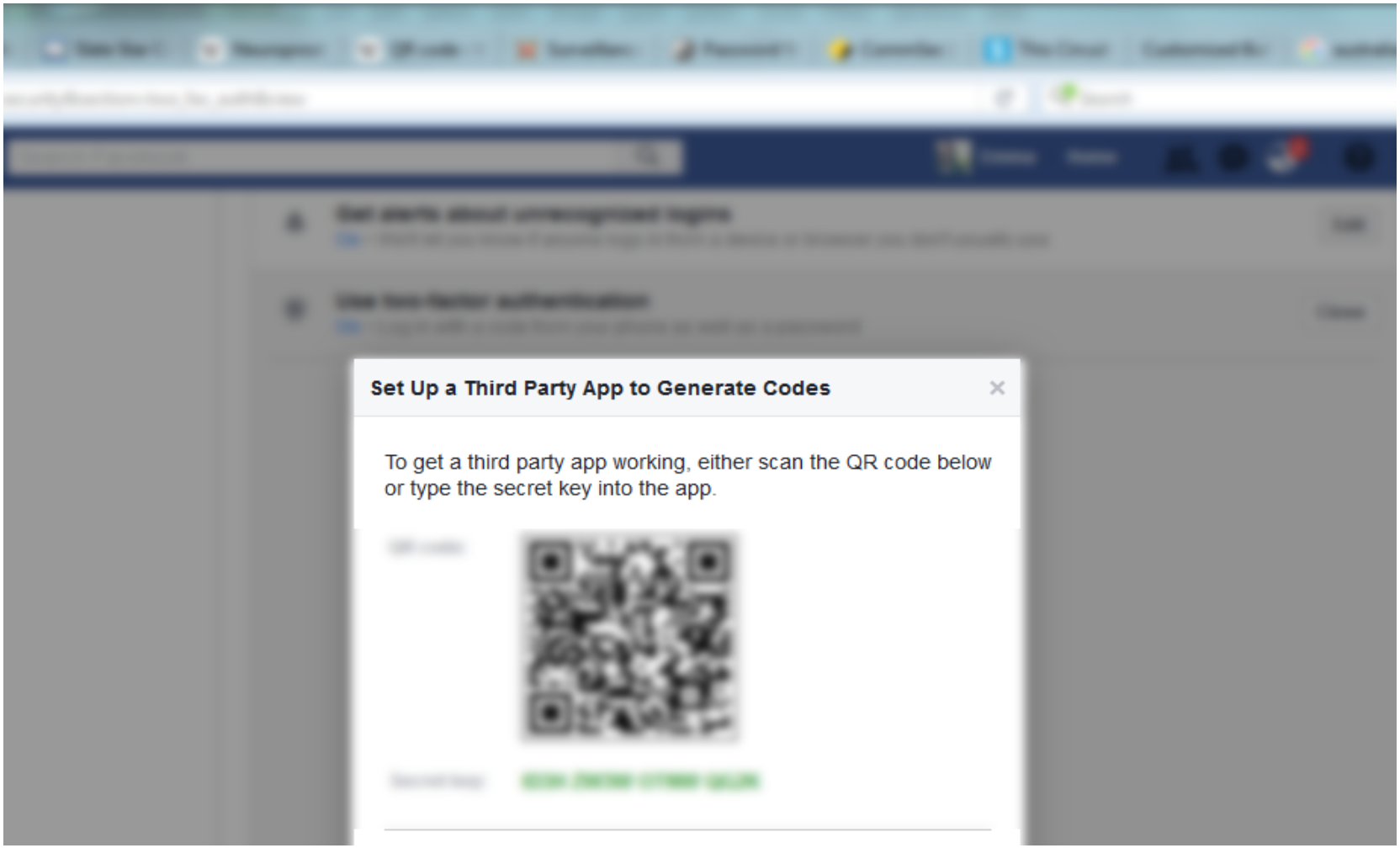
THE UNIVERSITY OF MELBOURNE

2fa - Facebook



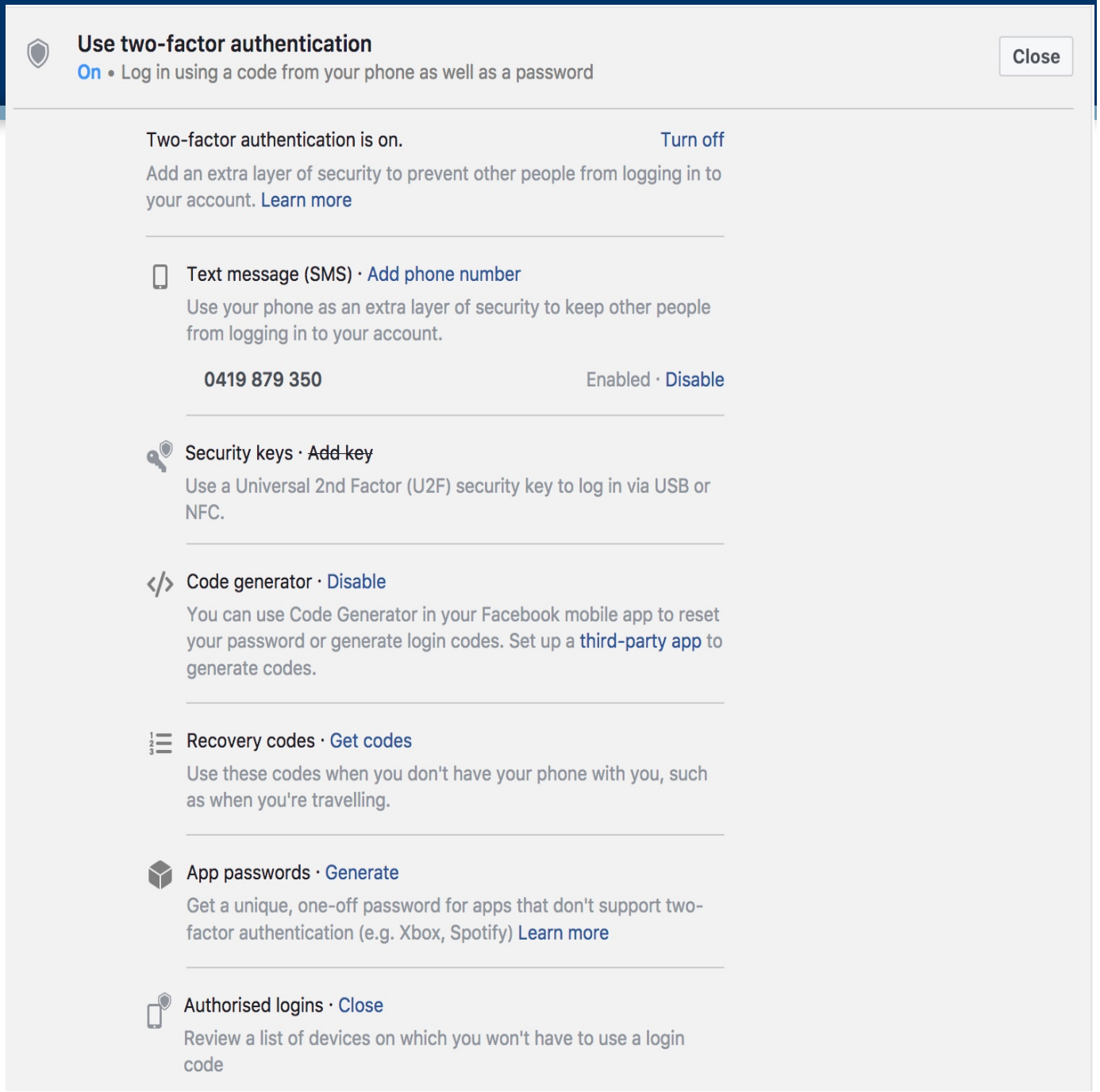
THE UNIVERSITY OF MELBOURNE

2fa - Facebook



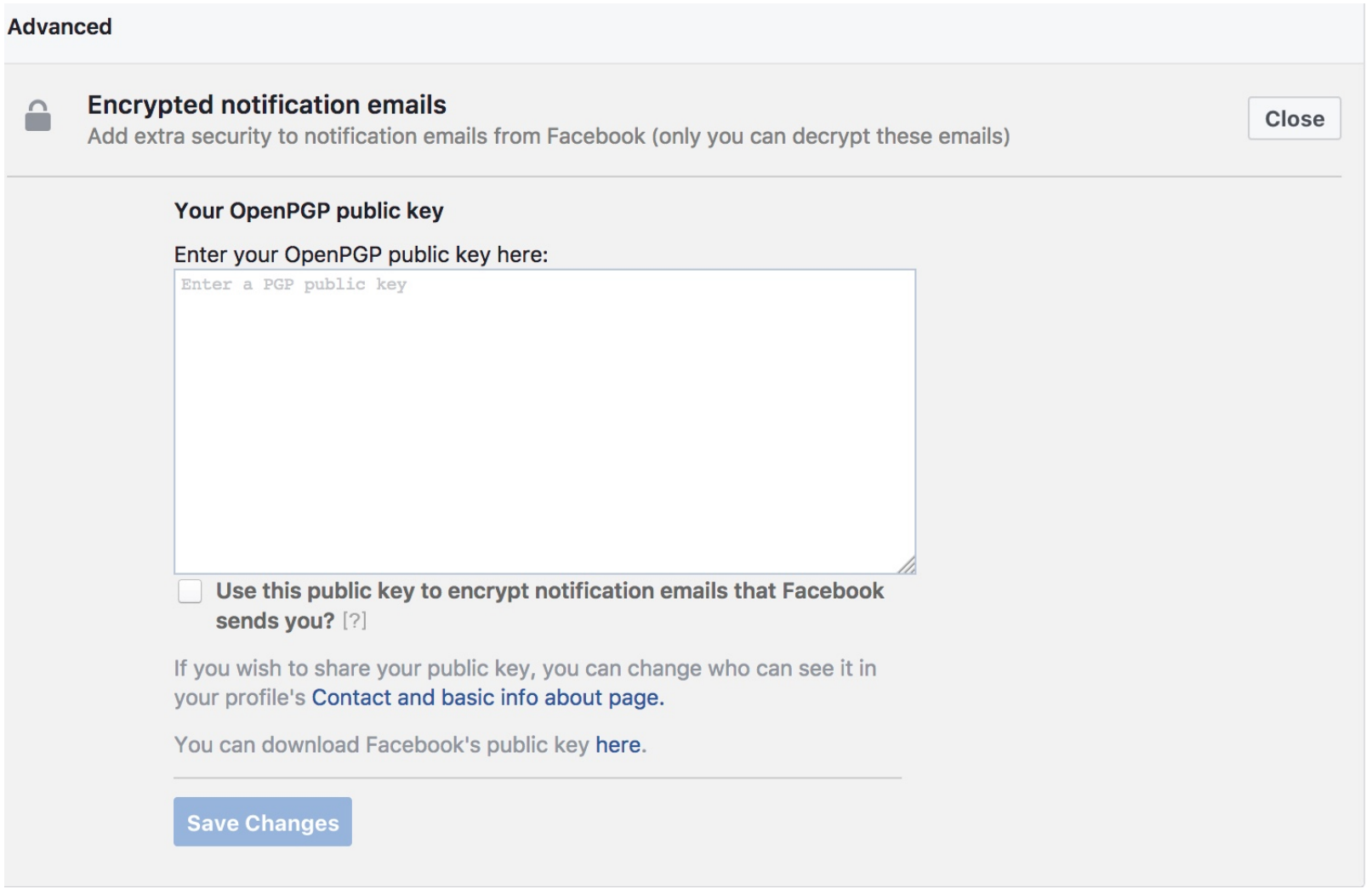
THE UNIVERSITY OF MELBOURNE

2fa Facebook



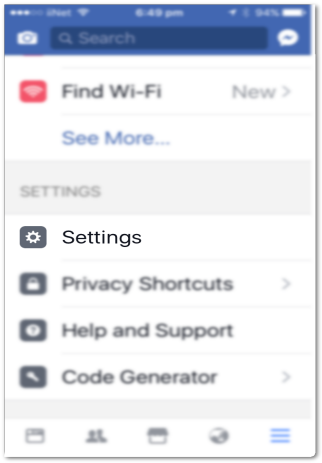
THE UNIVERSITY OF MELBOURNE

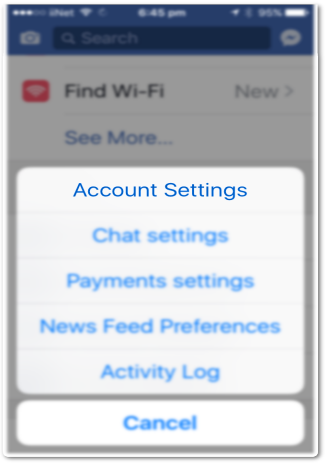
2fa – Facebook – GPG Public Key

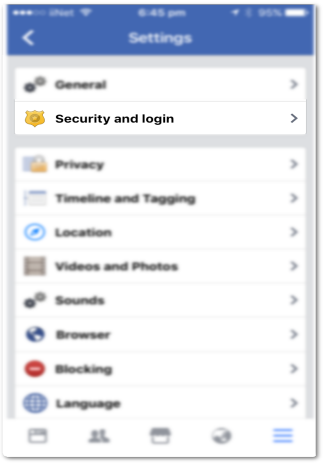


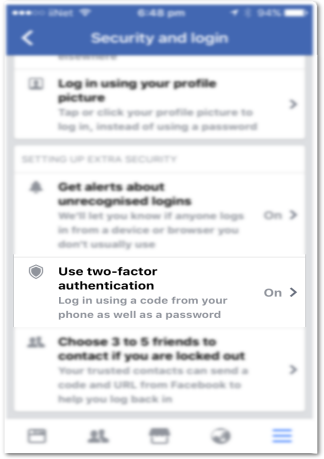
THE UNIVERSITY OF MELBOURNE

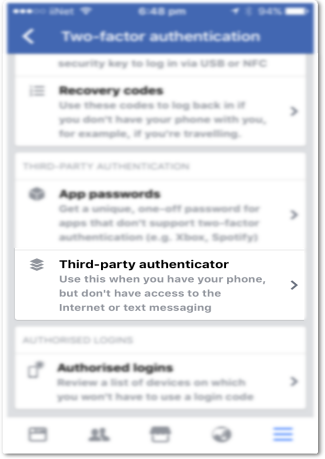
2fa – Facebook setup on Phones

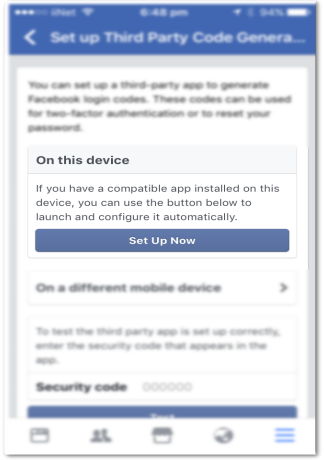






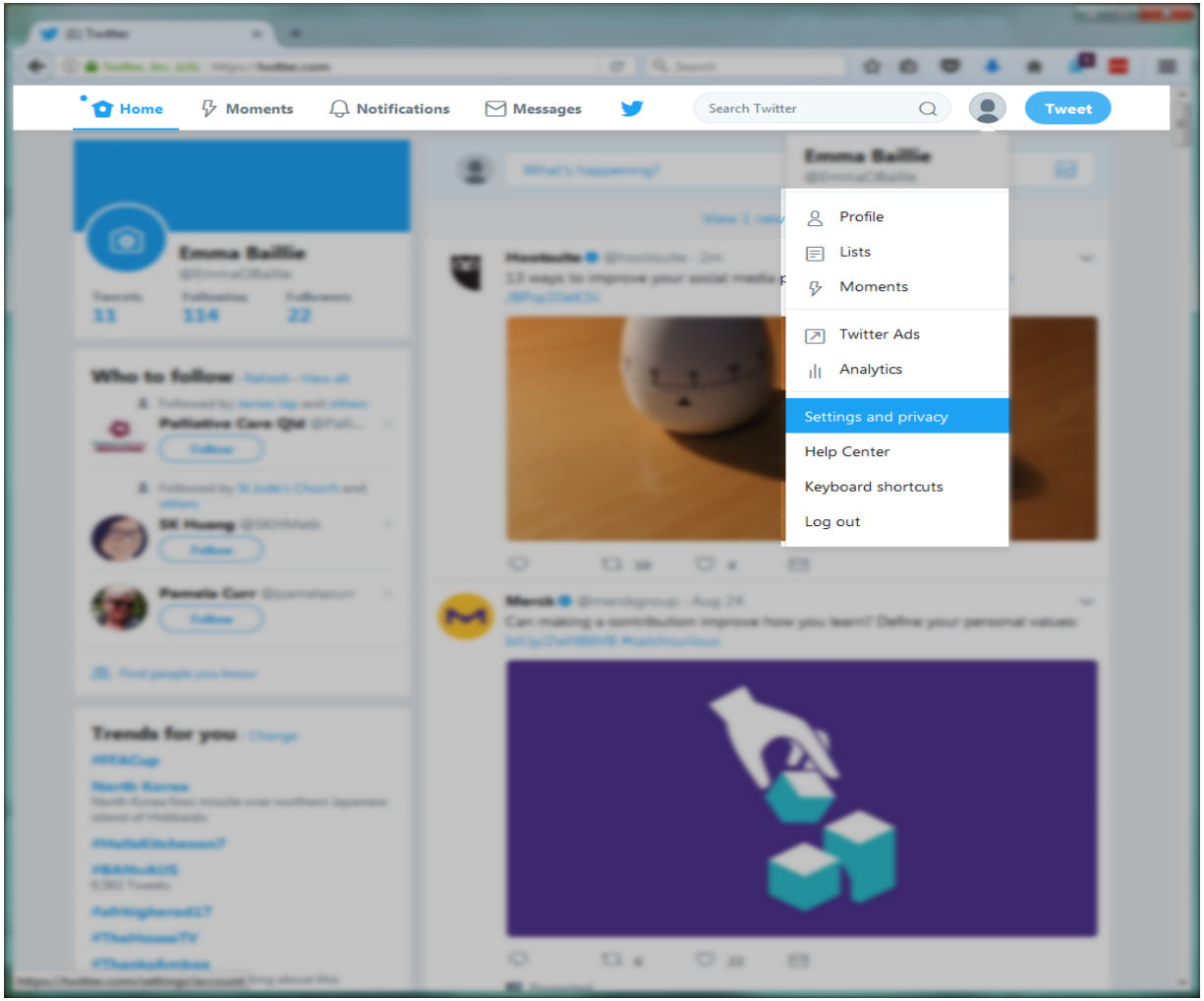






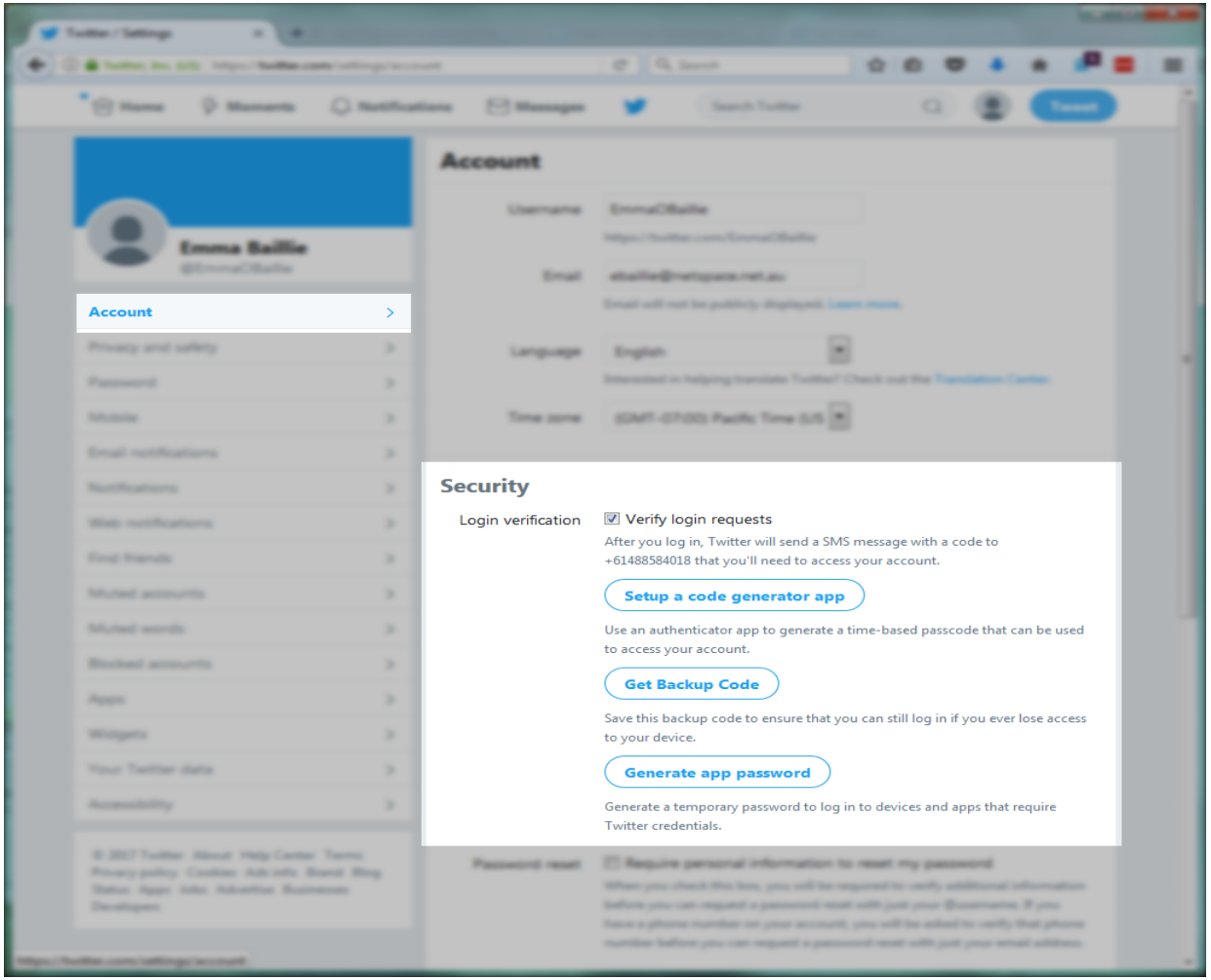
THE UNIVERSITY OF MELBOURNE

2fa - Twitter

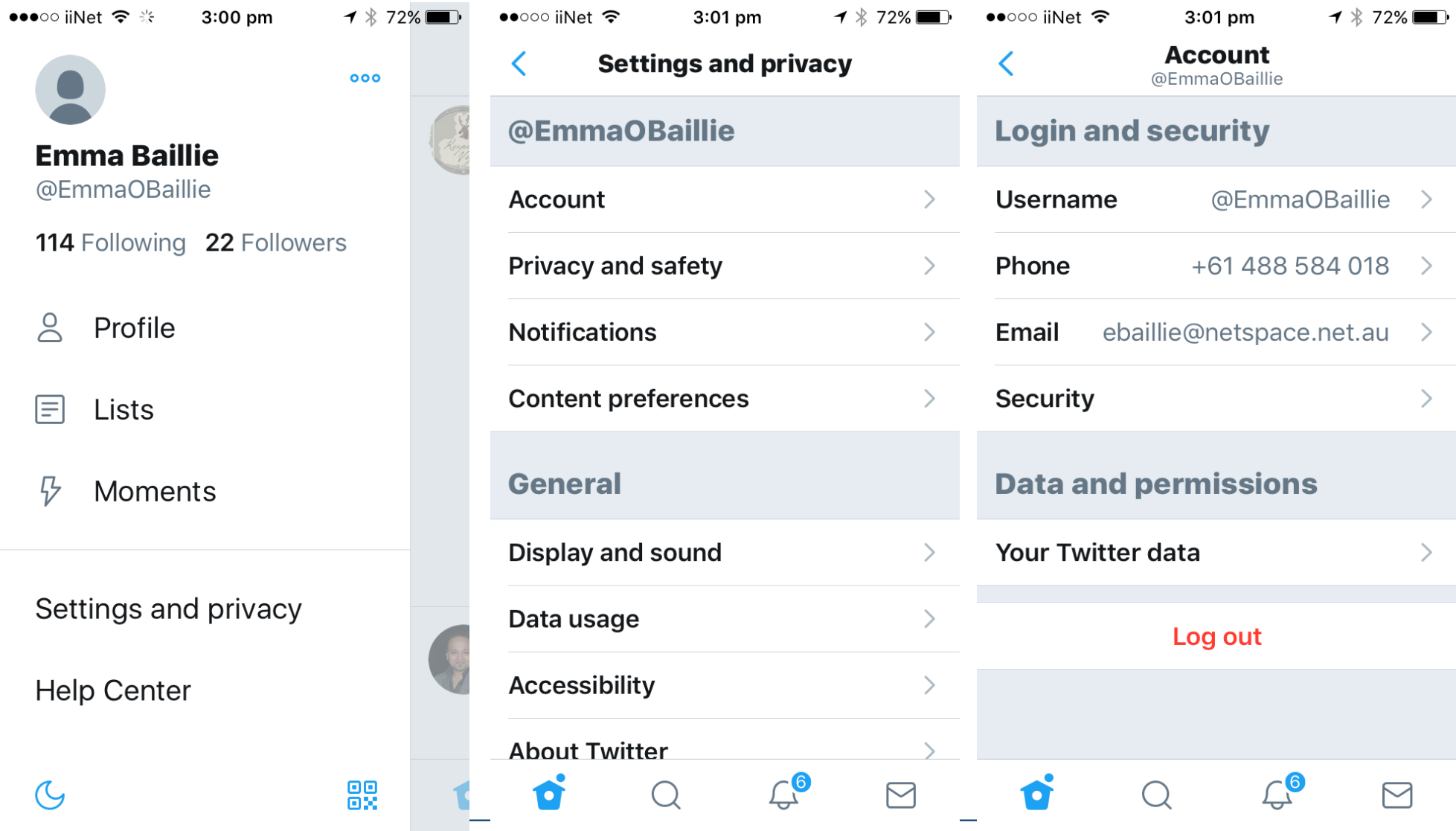


THE UNIVERSITY OF MELBOURNE

2fa - Twitter

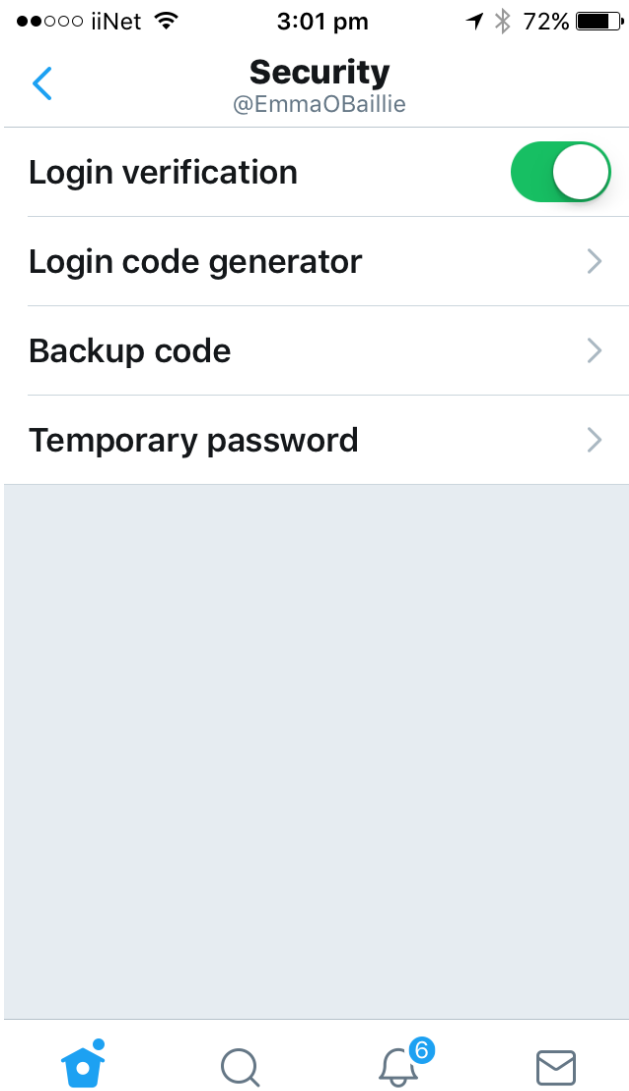


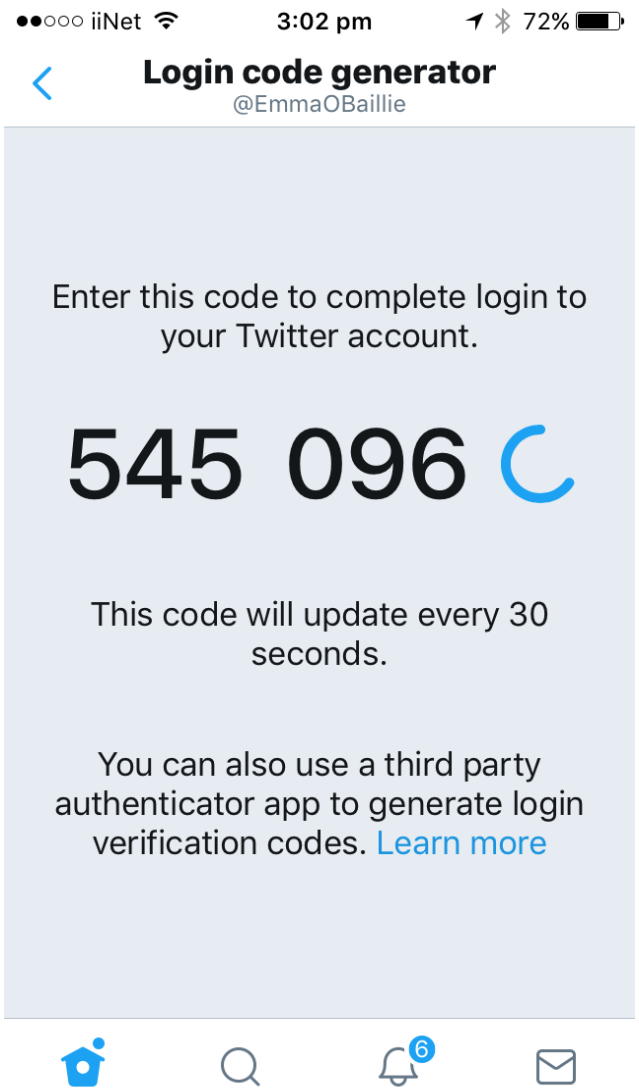
2fa - Twitter

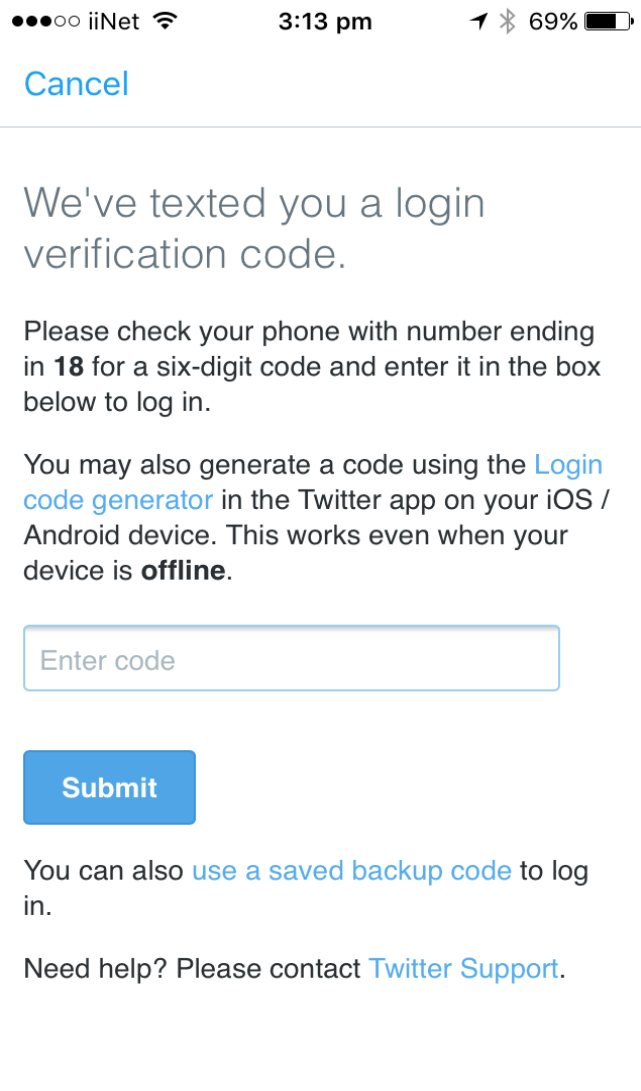

●●●○○ iiNet 3:00 pm 72%
Emma Baillie
@EmmaOBaillie
114 Following 22 Followers
Profile
Lists
Moments
Settings and privacy
Help Center
●●○○○ iiNet 3:01 pm 72%
Settings and privacy
@EmmaOBaillie
Account
Privacy and safety
Notifications
Content preferences
General
Display and sound
Data usage
Accessibility
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

THE UNIVERSITY OF MELBOURNE

2fa - Twitter







Bonus Tracks: For added privacy

1. Tweak your IM settings
   - WhatsApp

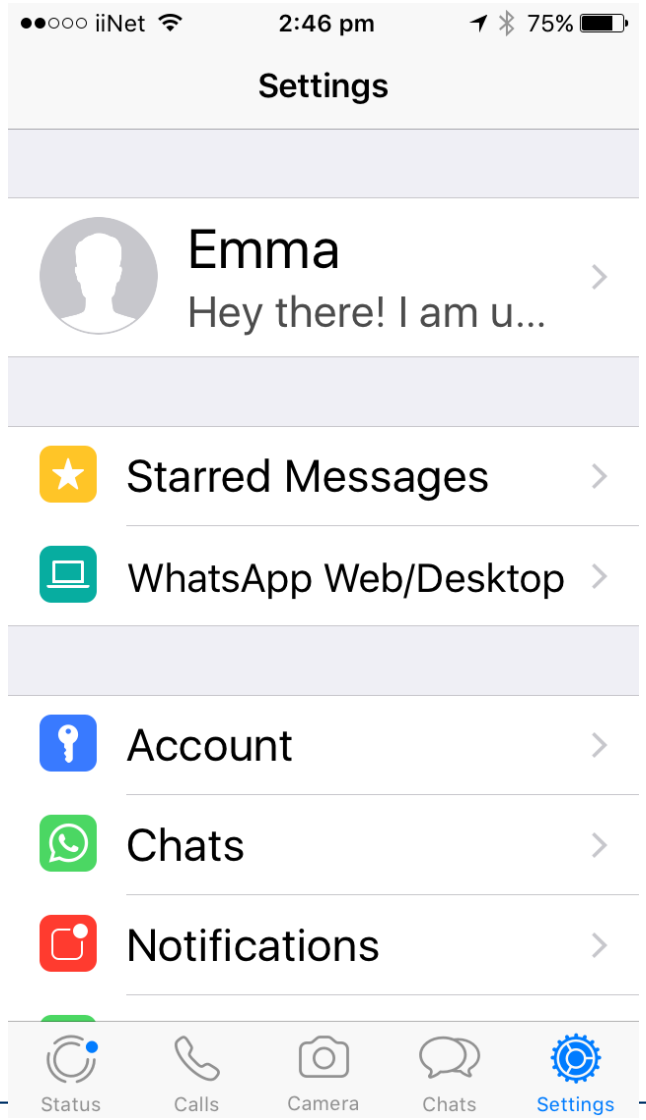
2. Think paper printouts are safer? Think again

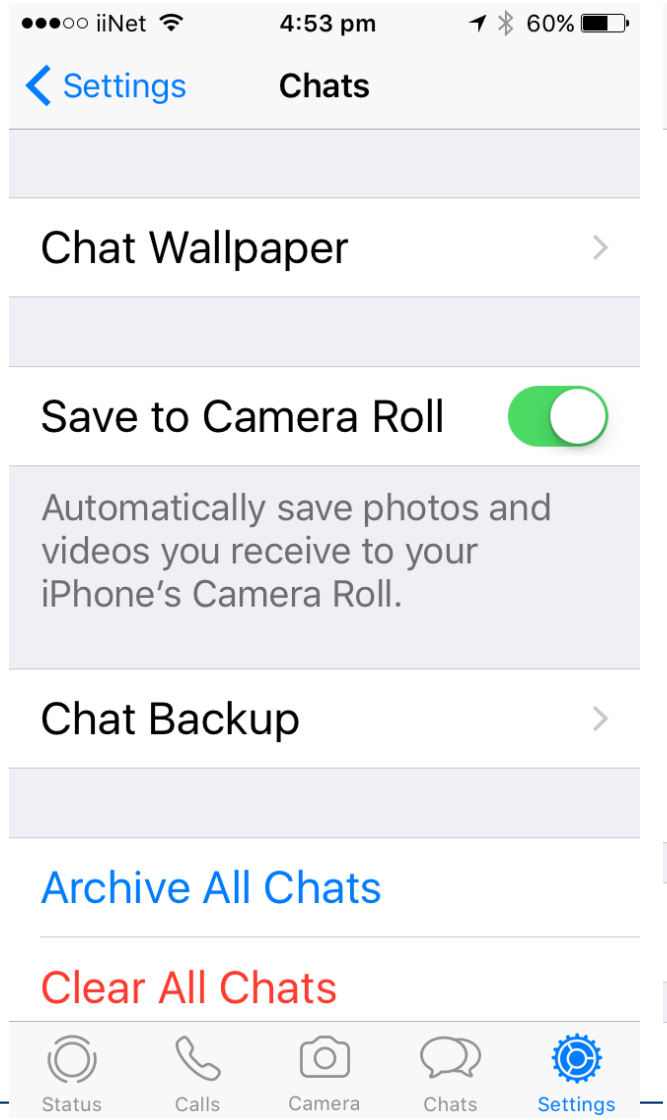
3. Turn off Bluetooth when you're not using it!

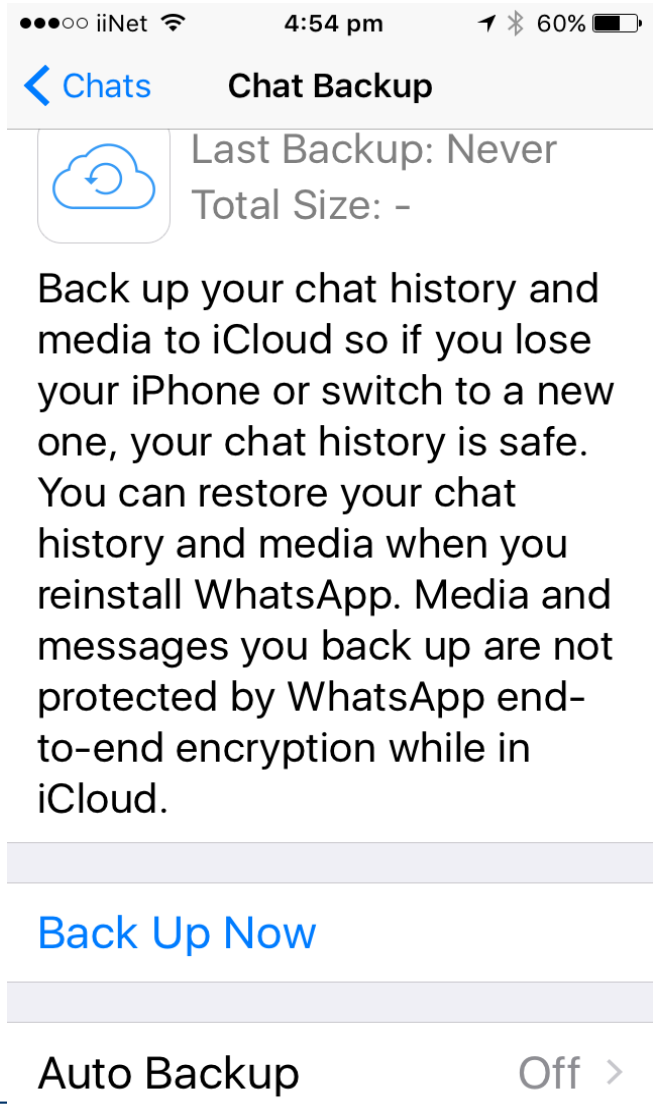
4. Browse with More Privacy

THE UNIVERSITY OF MELBOURNE

Whatsapp – removing cloud backup

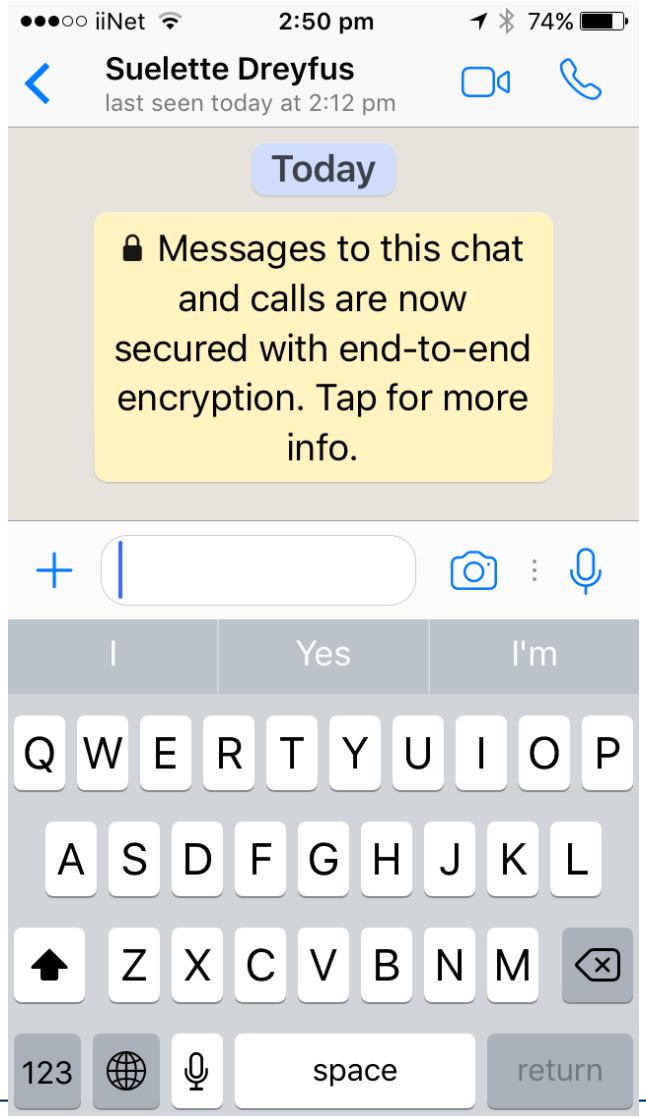


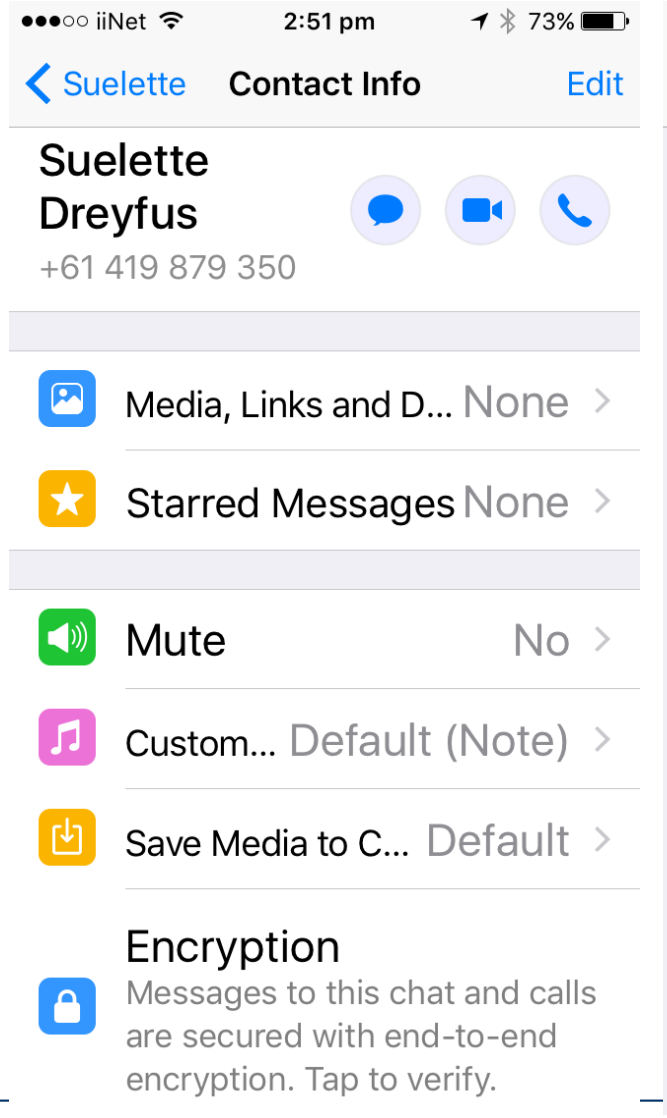


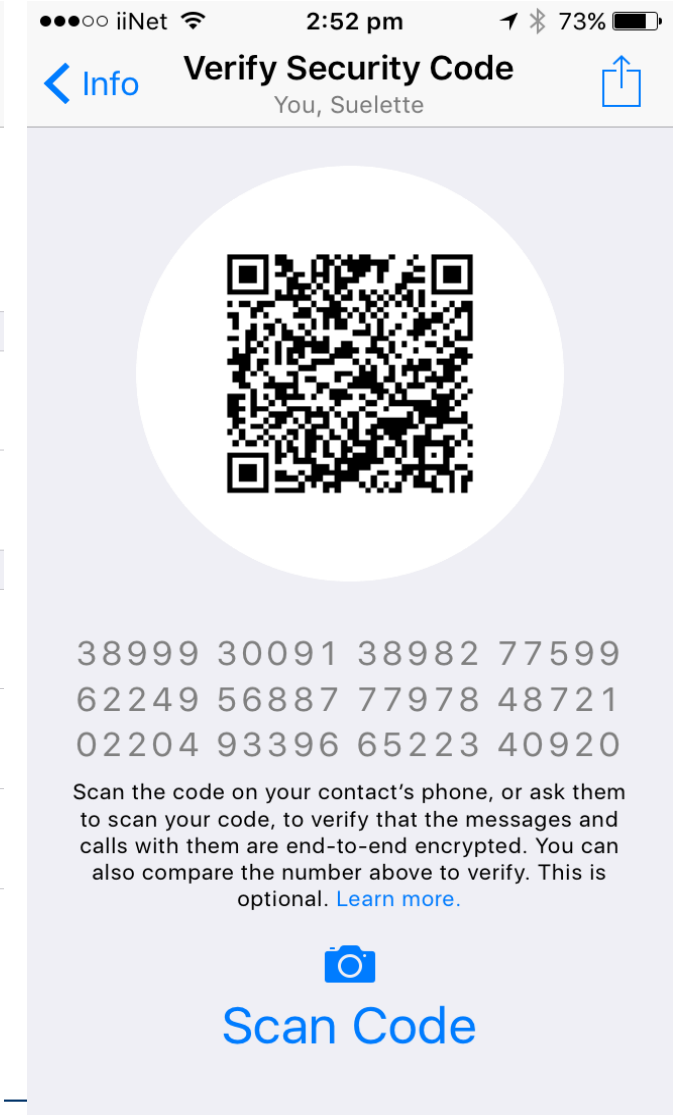


THE UNIVERSITY OF MELBOURNE

Whatsapp – Key Verification like Signal

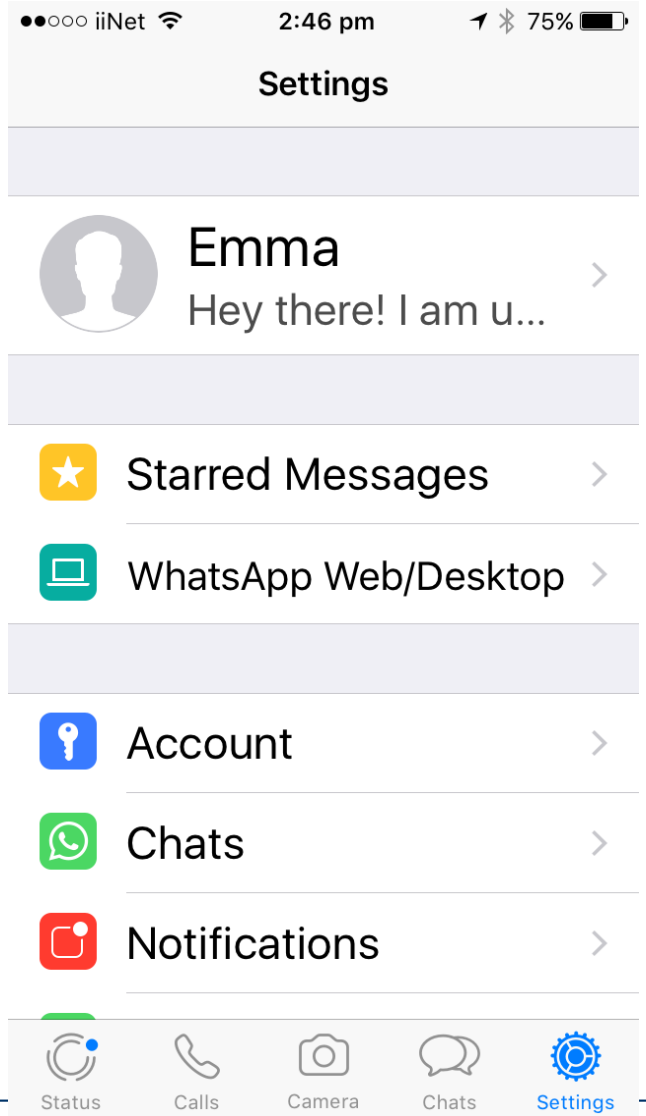


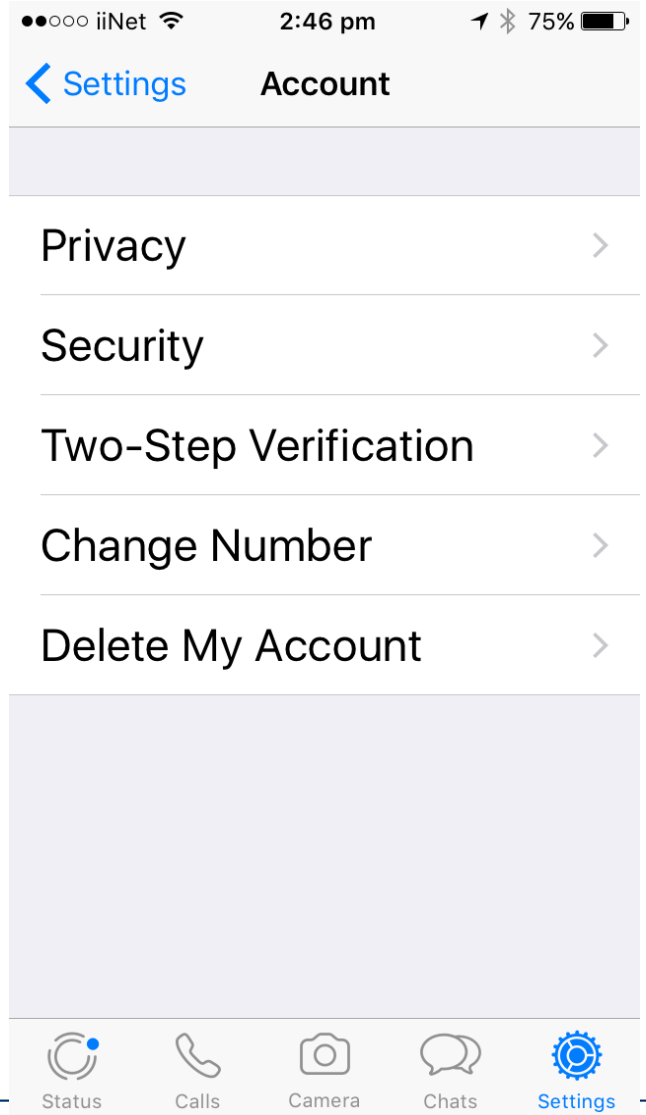


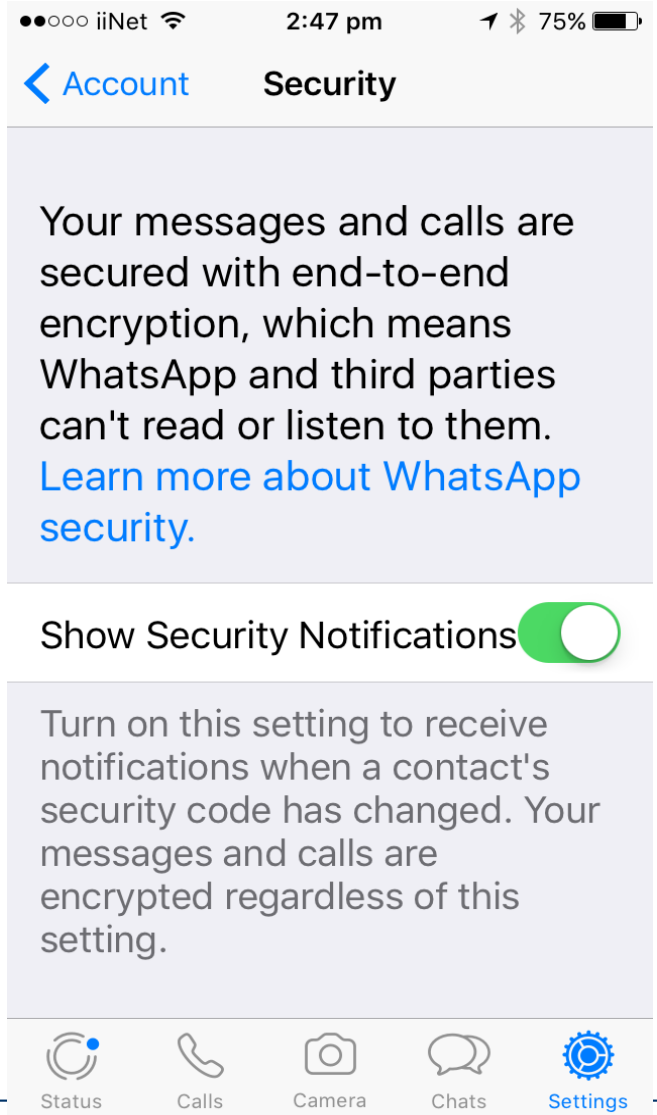


THE UNIVERSITY OF MELBOURNE

Whatsapp – security notifications

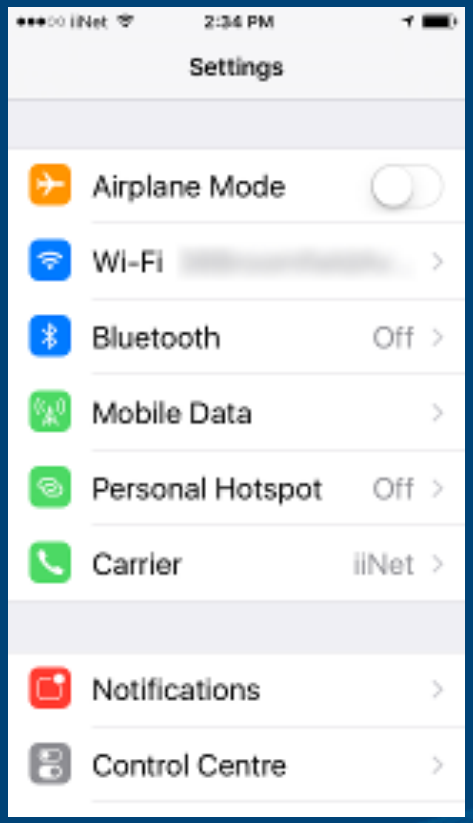


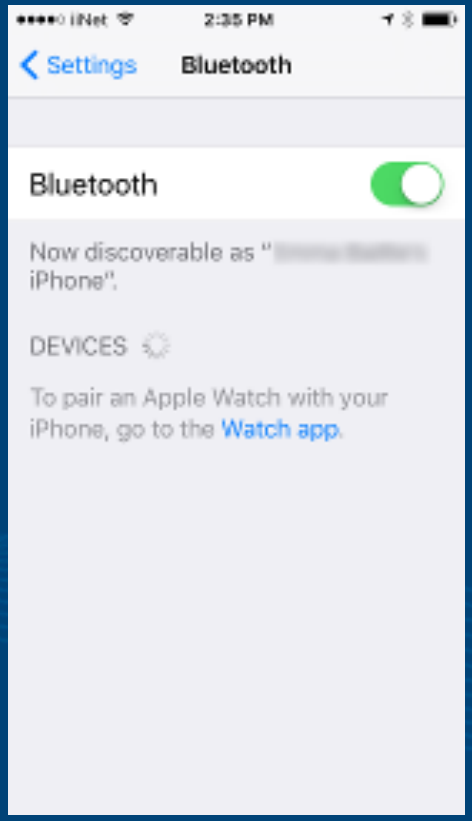


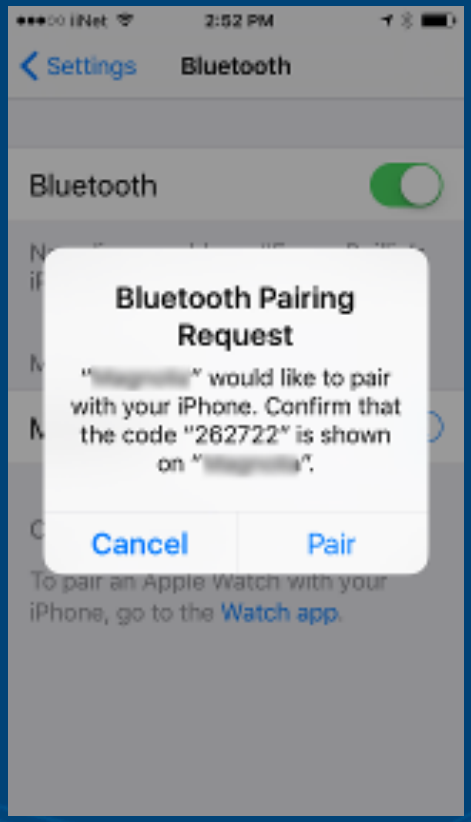


Bonus Track: Turn off Bluetooth

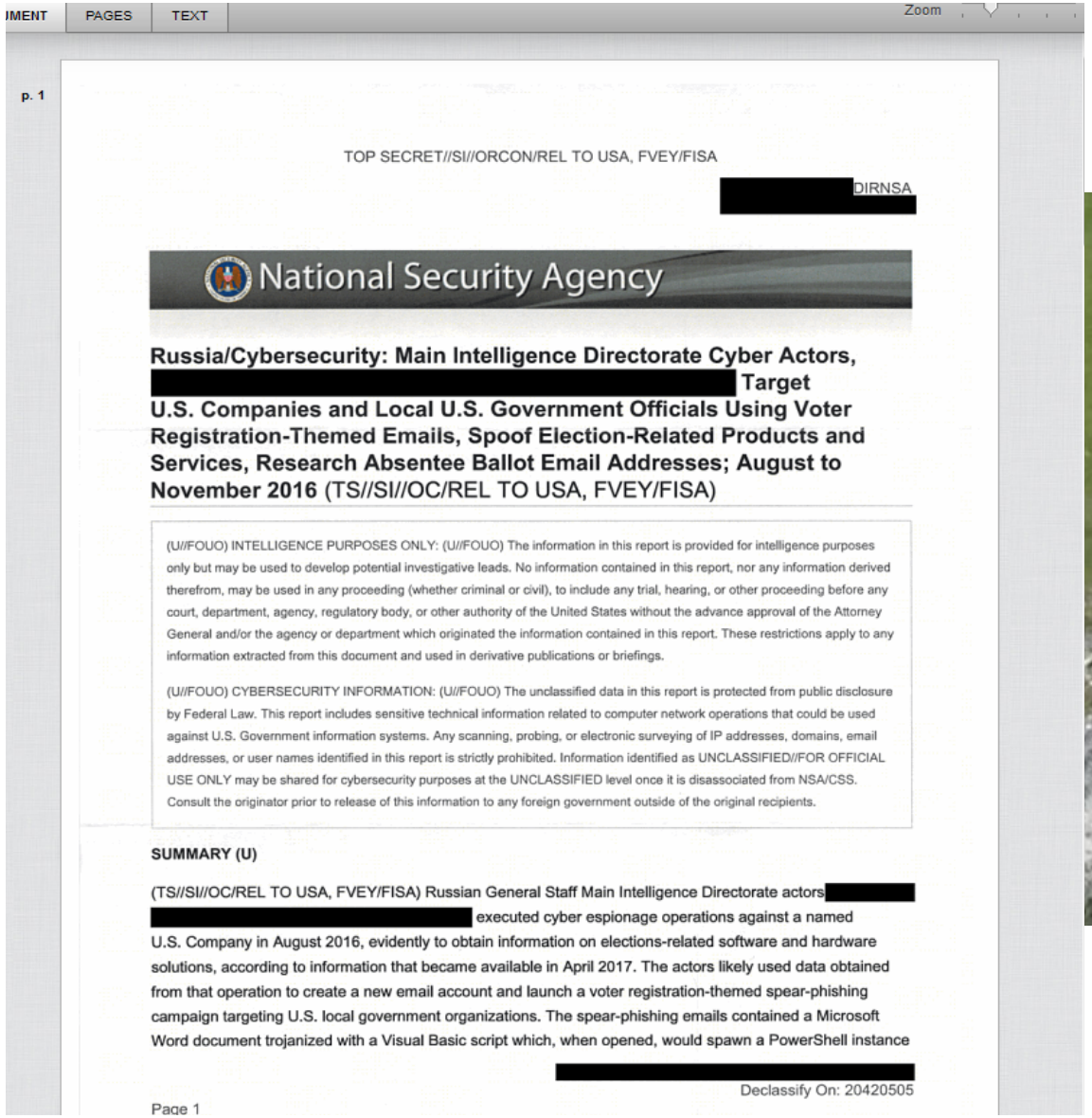
Bluetooth in your phone's settings







Printers Don’t always provide Privacy



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)

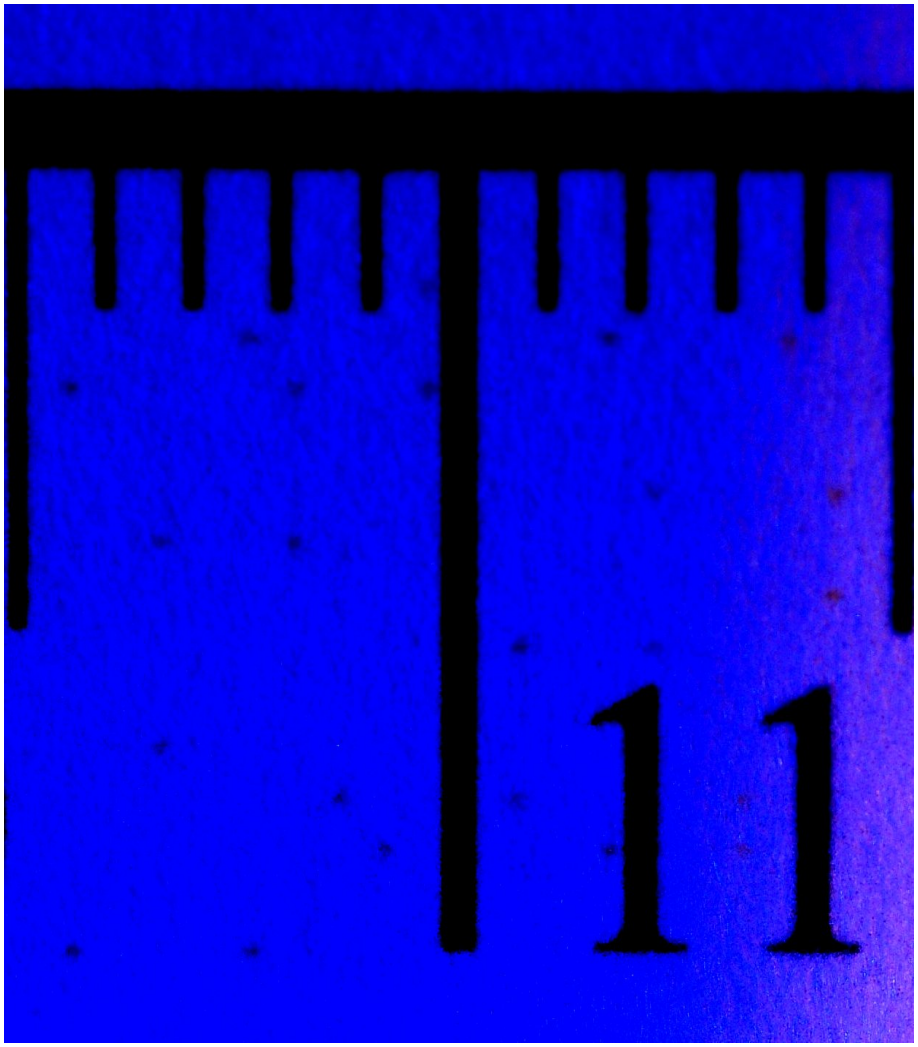
(TS//SI//OC/REL TO USA, FVEY/FISA) Russian General Staff Main Intelligence Directorate actors [redacted] executed cyber espionage operations against a named U.S. Company in August 2016, evidently to obtain information on elections-related software and hardware solutions, according to information that 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

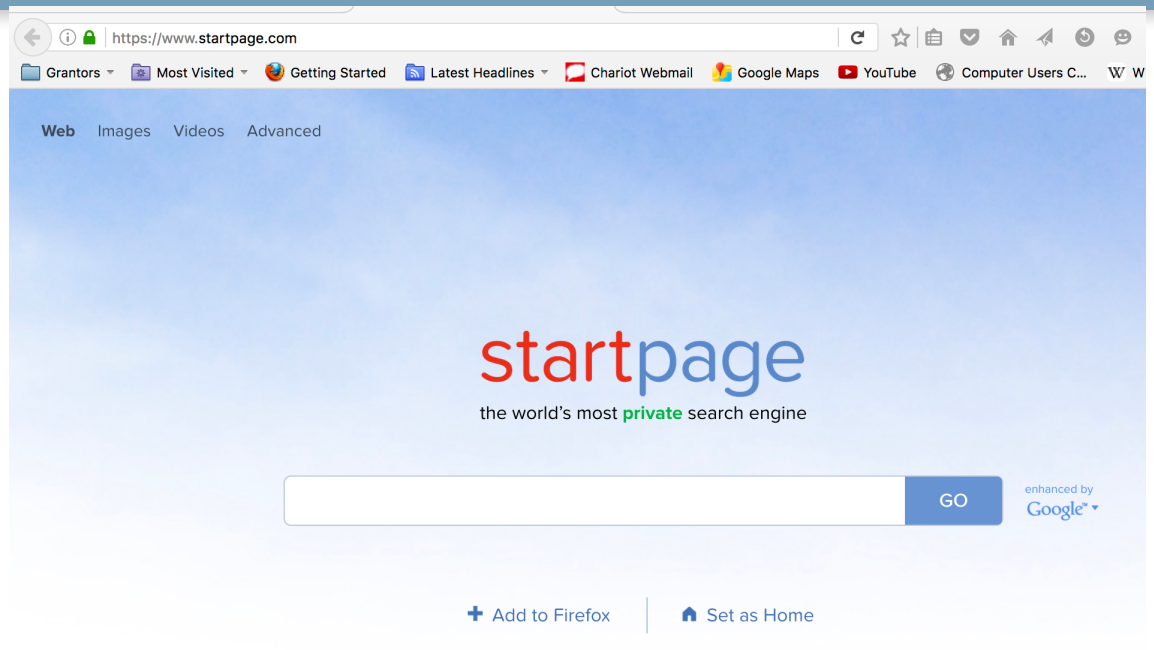
Page 1

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.



Ways to Browse with more anonymity



Set it as your default search engine in your browser

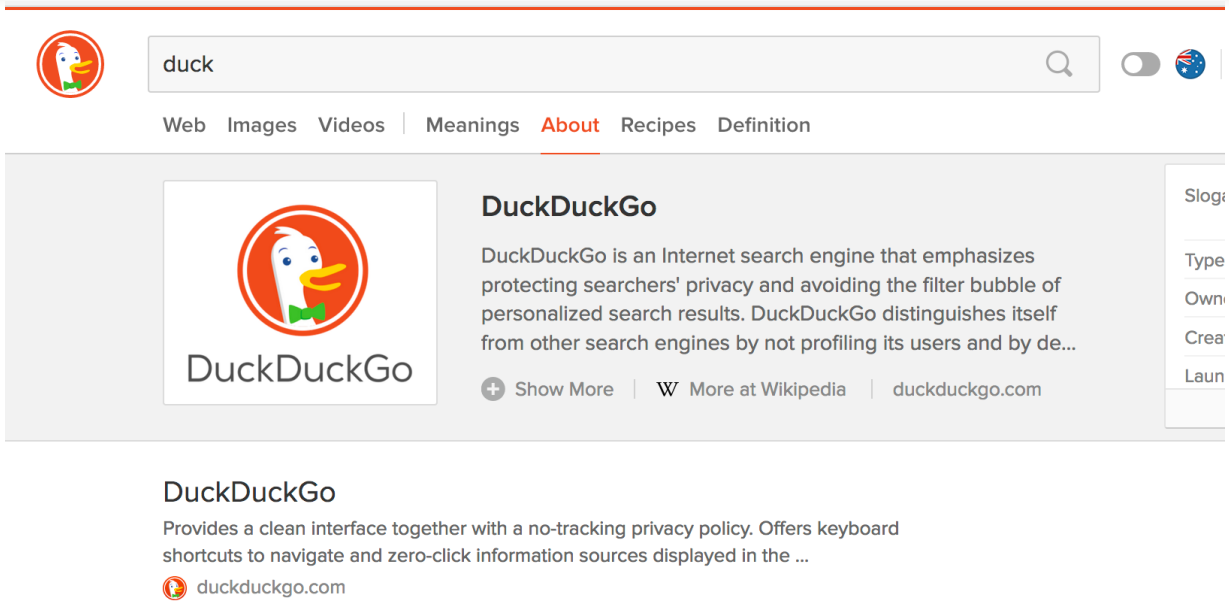
Option 1 https://startpage.com

Similar quality search results to Google. Your searches are proxied to Google – it looks like Startpage is making the search.

No metadata from you is kept.

Reasonable anonymity (not perfect) unless searching something unique to you (great-grandfather's name etc)

Browsing with more anonymity



Set it as your default search engine in your browser

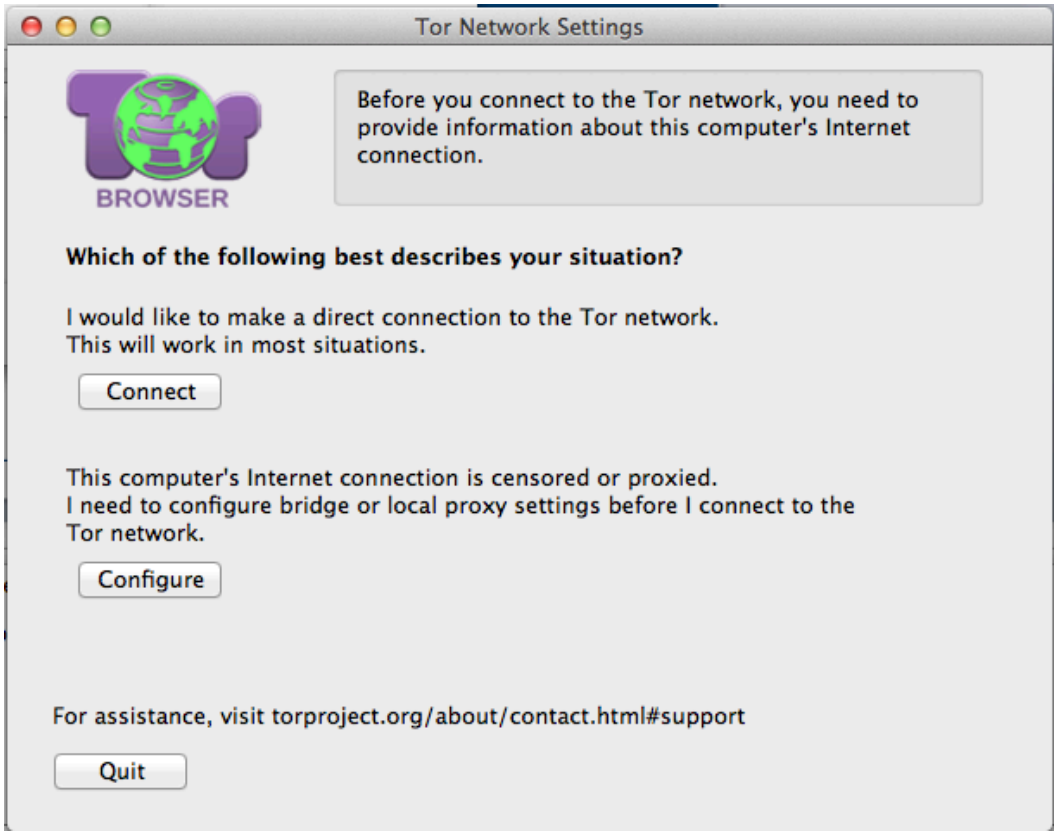
Option 2 https://duckduckgo.com

Will turn up different search results than Google, because they index the web themselves. They don't send your request onto anyone.

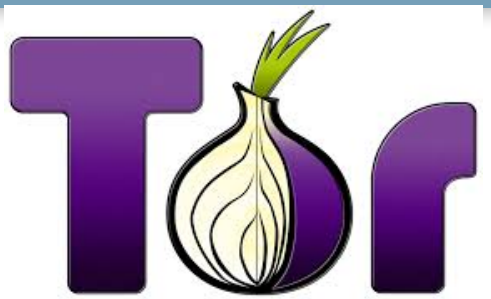
Their privacy policy says: metadata and searches are are not kept.

TOR Browser

https://www.torproject.org/



TOR Browser



https://www.torproject.org/

https://check.torproject.org/

TOR Principles

- Use the TOR Browser
- Don't torrent over TOR
- Don't open downloaded documents when online

How Unique is your browser?

https://panopticlick.eff.org/

Your browser fingerprint **appears to be unique** among the 129,323 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 16.98 bits of identifying information.**

The measurements we used to obtain this result are listed below. You can read more about our methodology, statistical results, and some defenses against fingerprinting here.

Test	Result
Is your browser blocking tracking ads?	⚠ partial protection
Is your browser blocking invisible trackers?	⚠ partial protection
Does your browser unblock 3rd parties that promise to honor Do Not Track?	✗ no
Does your browser protect from fingerprinting?	✗ your browser has a unique fingerprint

Class hands on: run it now – share the answer

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