



# 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.

- 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

- 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

# Who cares about privacy anyway?



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?

## *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?

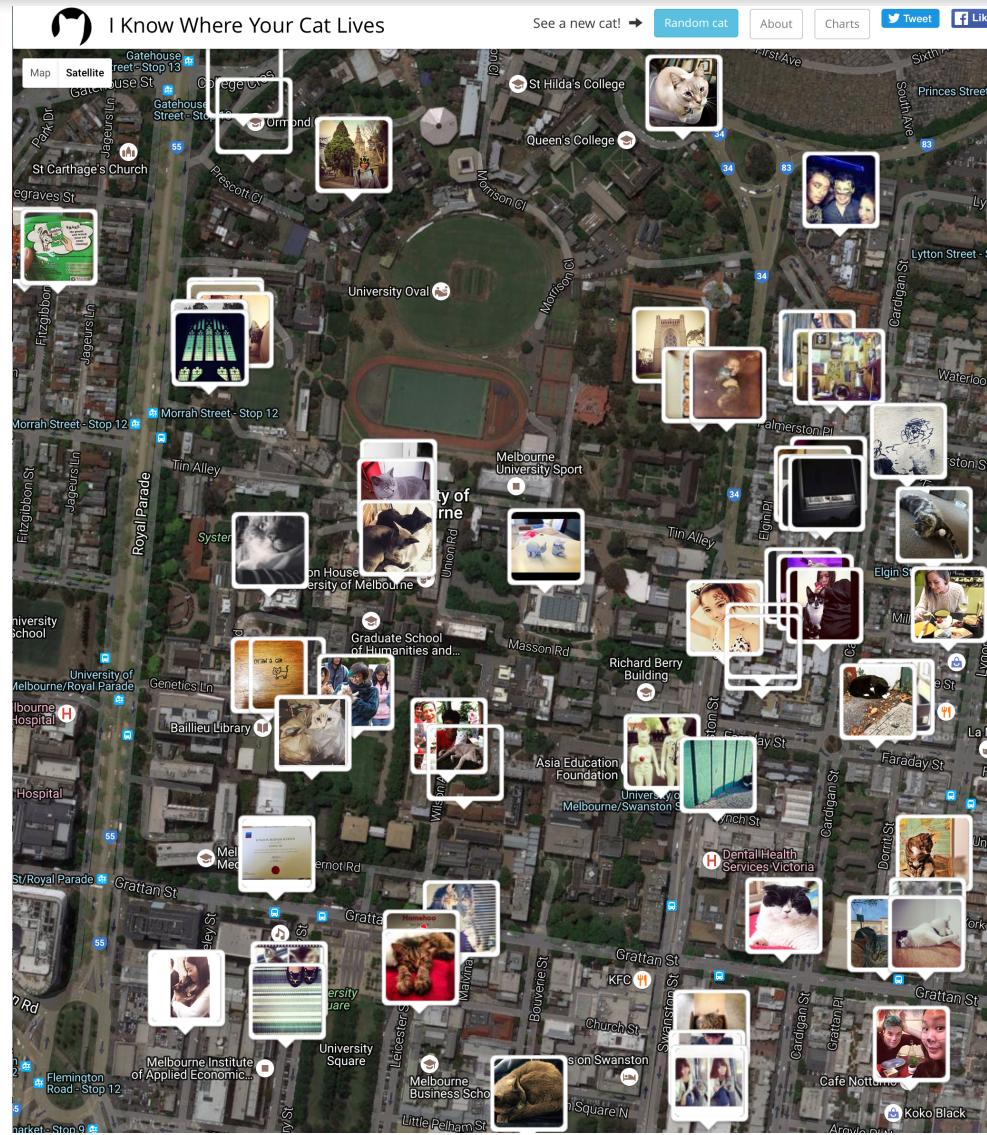
Nearby strangers: You could be in the background of someone else's photo – which might be geo-tagged. Then face-recognised by software.

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

Who here loves cat pics?

## *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*



I'm at  
161 collins st



I'm talking to  
Hubert James

I'm pinning  
doilies on  
the pinterest  
app

I'm visiting  
the bronies  
website

I took photos  
in the botanic  
gardens

Chatterbox..



### Inside TAO: Documents Reveal Top NSA Hacking Unit

By SPIEGEL Staff

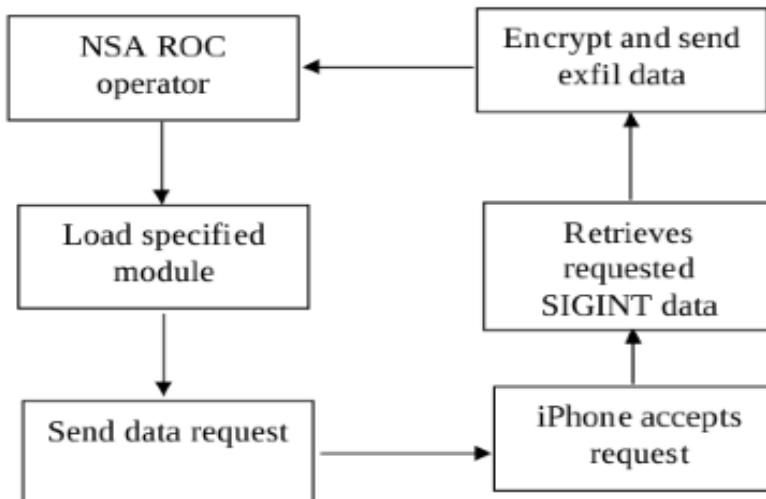


Google Earth

**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.**

# 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.”

**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

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



TOP SECRET//COMINT//REL TO USA, FVEY//20320108

(U//FOUO) PREFER

Identification & Extraction April 2011

(S//SI//REL) 194 Million Messages Collected by DISHFIRE per Day,  
Including

- (S//SI//REL) VCARDS → names+; (113,672 average extracted daily)  
sometimes DNI link (email) to DNR (telephony) as well as images
- (S//SI//REL) Geocoordinates (76,142 daily avg; hex-encoded 10.432)
  - Requests by people for route info
  - Setting up meetings at a location
  - Tracking information: e.g., [REDACTED] (12,809)
  - Comma Separated Formats (33,020)
- (S//SI//REL) Missed Calls → contact chaining (5,058,114)
- (S//SI//REL) SIM Card Changes → IMSI/IMEI links (6,017,901)
- (S//SI//REL) Roaming information → border crossings (1,658,025)
- (S//SI//REL) Travel (5,314)
  - Itinerary including multiple flights
  - Changes: cancellations, reschedules, delays
- (S//SI//REL) Financial Transactions:
  - Credit card transactions: correlate credit cards to individuals (61,488)
  - Money transfers (social networks) – Phone to Phone (630,846)
  - Track financial information (account activity – bank transaction) (115,480)
- (S//SI//REL) Passwords (pending); Other Requests?



## 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 browser's 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 Yamieh 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.

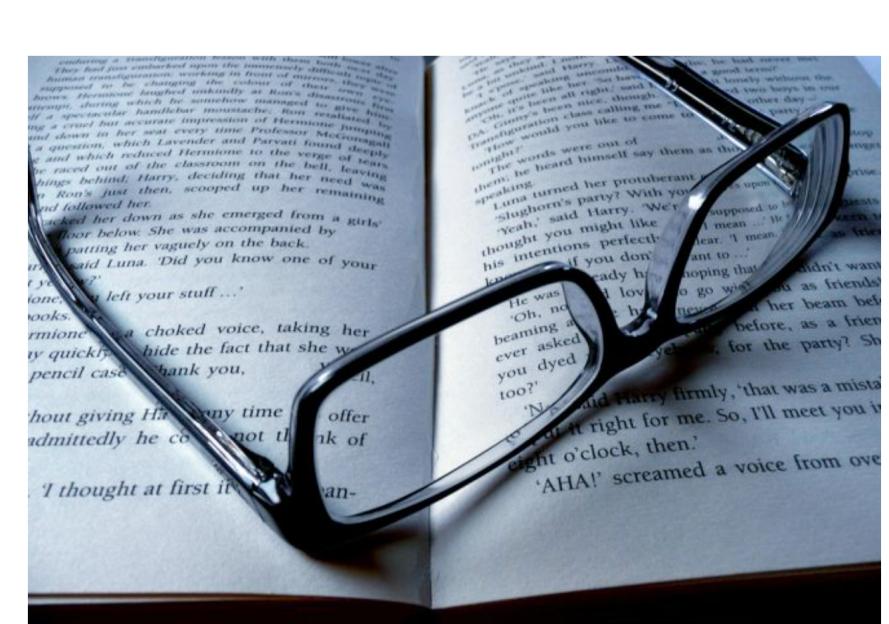
Source: Leger, DL, & Alcindor, Y 2012. 'Petraeus and Broadwell used common email trick', *USA Today*, 13 Nov.  
See: <http://www.usatoday.com/story/tech/2012/11/13/petraeus-broadwell-email/1702057/>

## It's difficult to be truly anonymous

### Technical (Cont)

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

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/>



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)**

## 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**

### 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

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 screenshot shows a news article from The Hacker News. The title is "Facebook CEO Zuckerberg's Twitter, Pinterest accounts Hacked! And the Password was...". The date is Sunday, June 05, 2016, by Mohit Kumar. The article features a large photo of Mark Zuckerberg. On the right side of the image, there are two social media posts. The top post is from Mark Zuckerberg (@finkd) saying: "Hey, @finkd You were in Linkedin Database with the password "dadada" ! DM for proof..". Below it is a post from "Hacked By OurMine Team - Read" (@zuck) with the text "ZUCK GET PWNED!". A caption below the image states: "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." The text at the bottom of the article says: "Yes, I'm talking about Facebook CEO [Mark Zuckerberg](#), who had his Twitter and Pinterest accounts compromised on Sunday." Another note at the bottom says: "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.

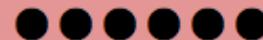
- Don't reuse passwords
- Choose secure passwords (not 'dadada'!)
- Consider a password manager



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



# HOW SECURE IS MY PASSWORD?



It would take a computer about

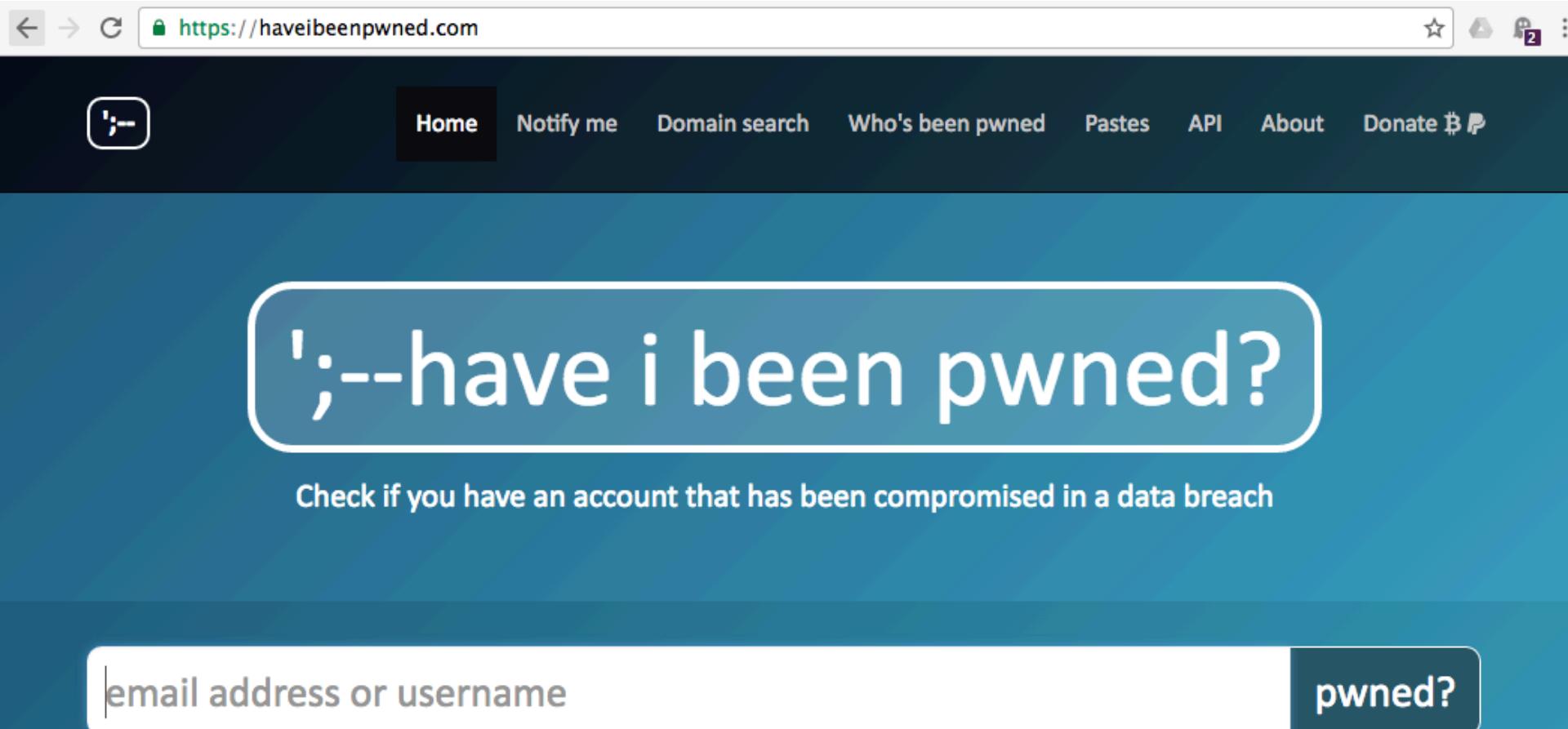
**8 MILLISECONDS**

to crack your password

Why not try **Dashlane** to create and remember stronger passwords? It's free!

[Tweet Your Result](#)

Well, you might have been pwned. Test it.



A screenshot of a web browser displaying the homepage of [haveibeenpwned.com](https://haveibeenpwned.com). The page features a large, stylized question mark icon with the text '';--have i been pwned?'. Below it, a subtext reads 'Check if you have an account that has been compromised in a data breach'. At the bottom, there is a search bar with the placeholder 'email address or username' and a blue button labeled 'pwned?'.

https://haveibeenpwned.com

Home Notify me Domain search Who's been pwned Pastes API About Donate Ⓜ

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address or username

pwned?

Think you  
are too  
smart?  
Can't get  
owned?  
Think  
again.

# ';--have i been pwned?

Check if you have an account that has been compromised in a data breach

suelette@unimelb.edu.au

pwned?

Oh no — pwned!

Pwned on 1 breached site and found no pastes (subscribe to search sensitive breaches)

 Notify me when I get pwned

  Donate



## Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.



**LinkedIn:** In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

**Compromised data:** Email addresses, Passwords

125  
pwned websites

1,314,990,097  
pwned accounts

38,810  
pastes

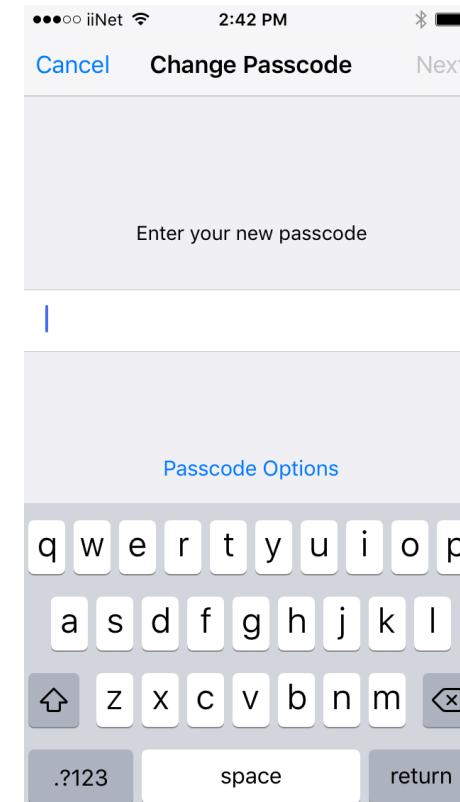
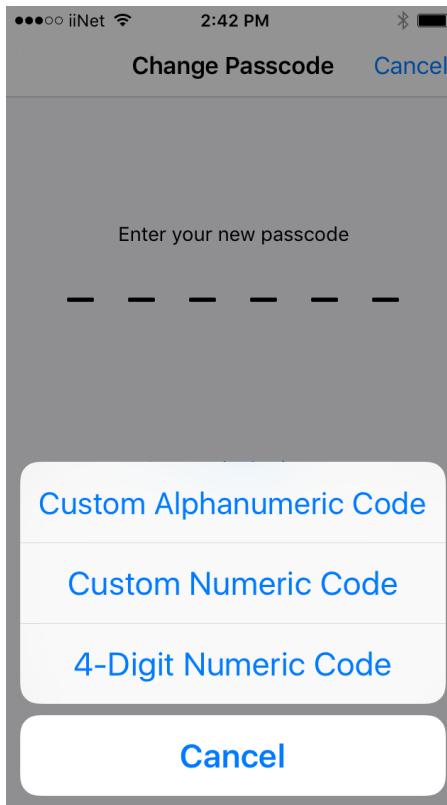
30,284,538  
paste accounts

## Top 10 breaches

 359,420,698 MySpace accounts

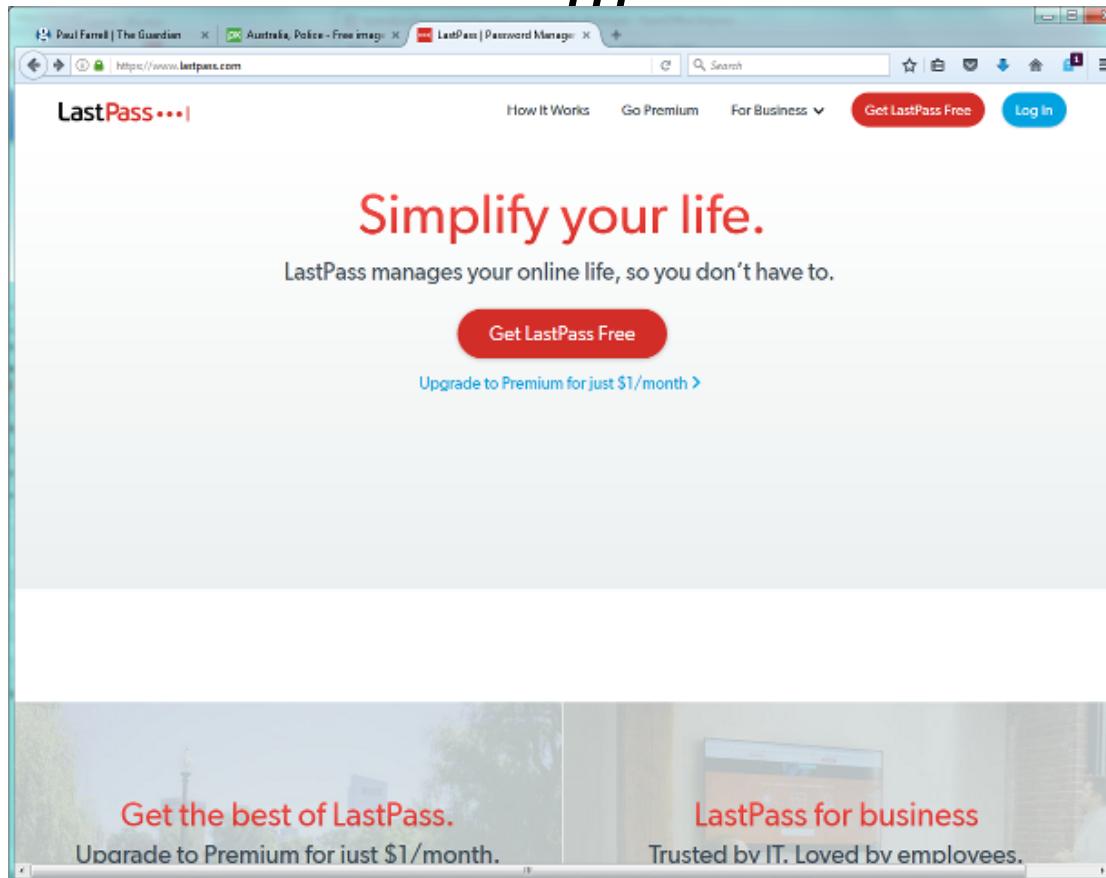
 164,611,595 LinkedIn accounts

# Password protect iPhone: use alphanumeric

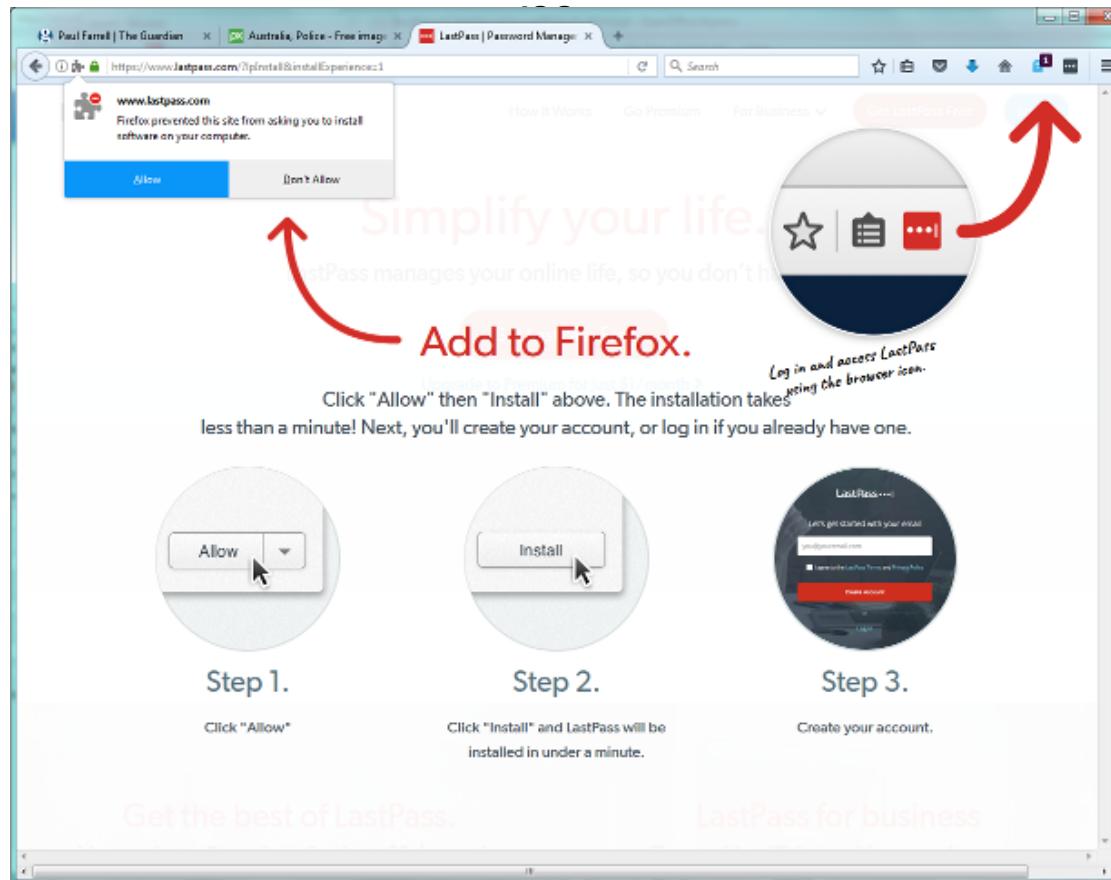


*www.lastpass.co*

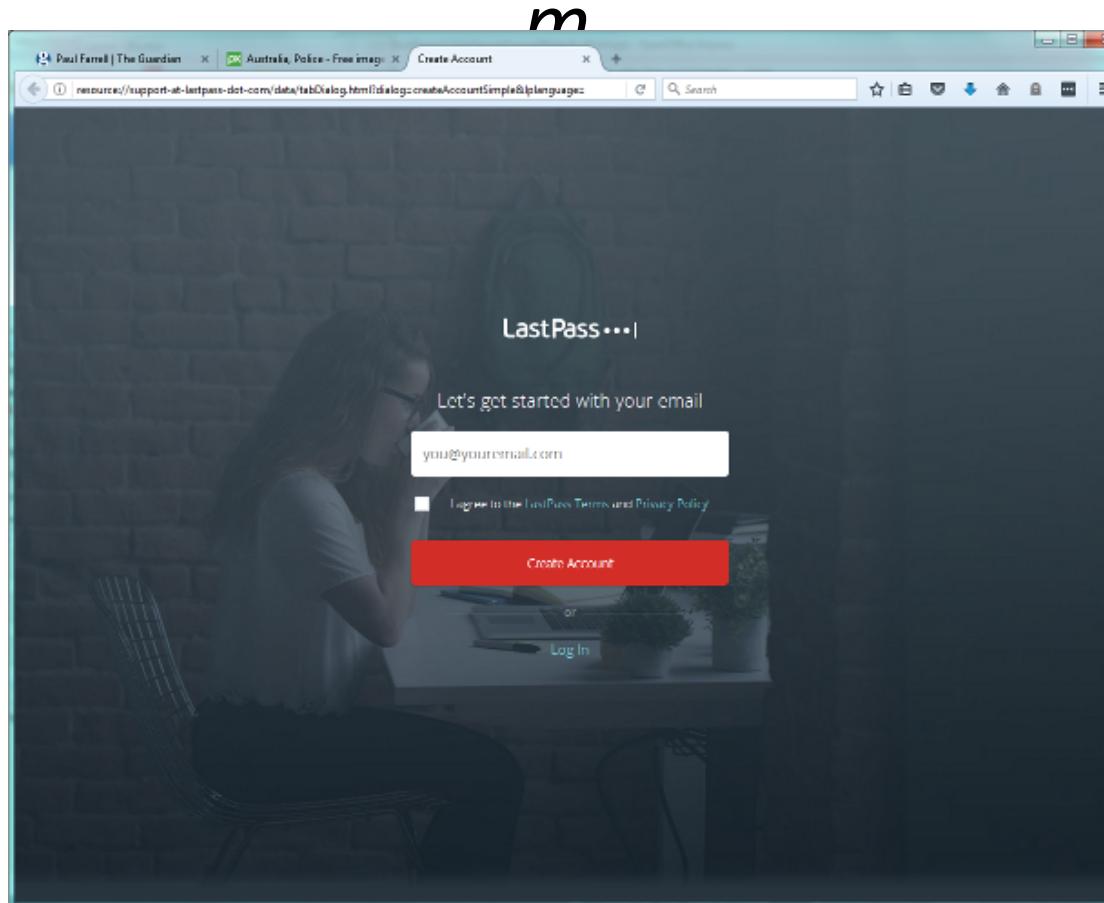
*m*



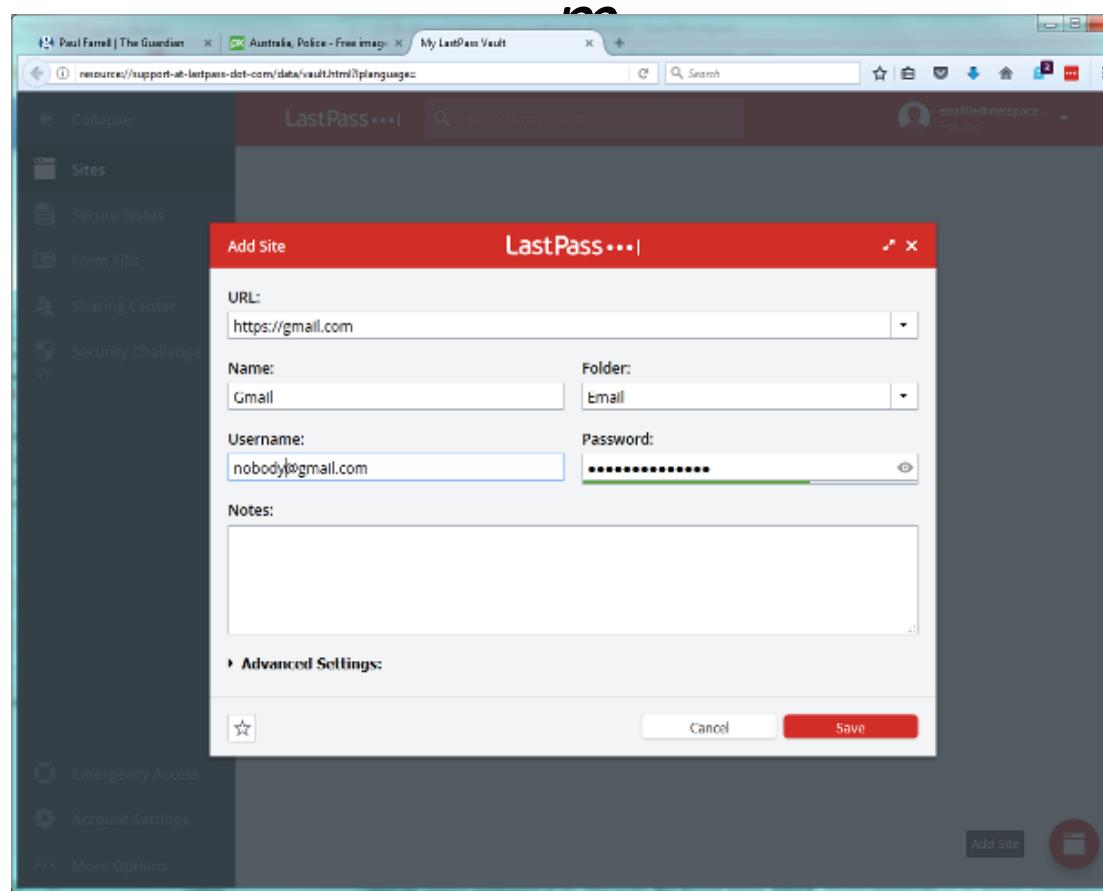
*www.lastpass.co*



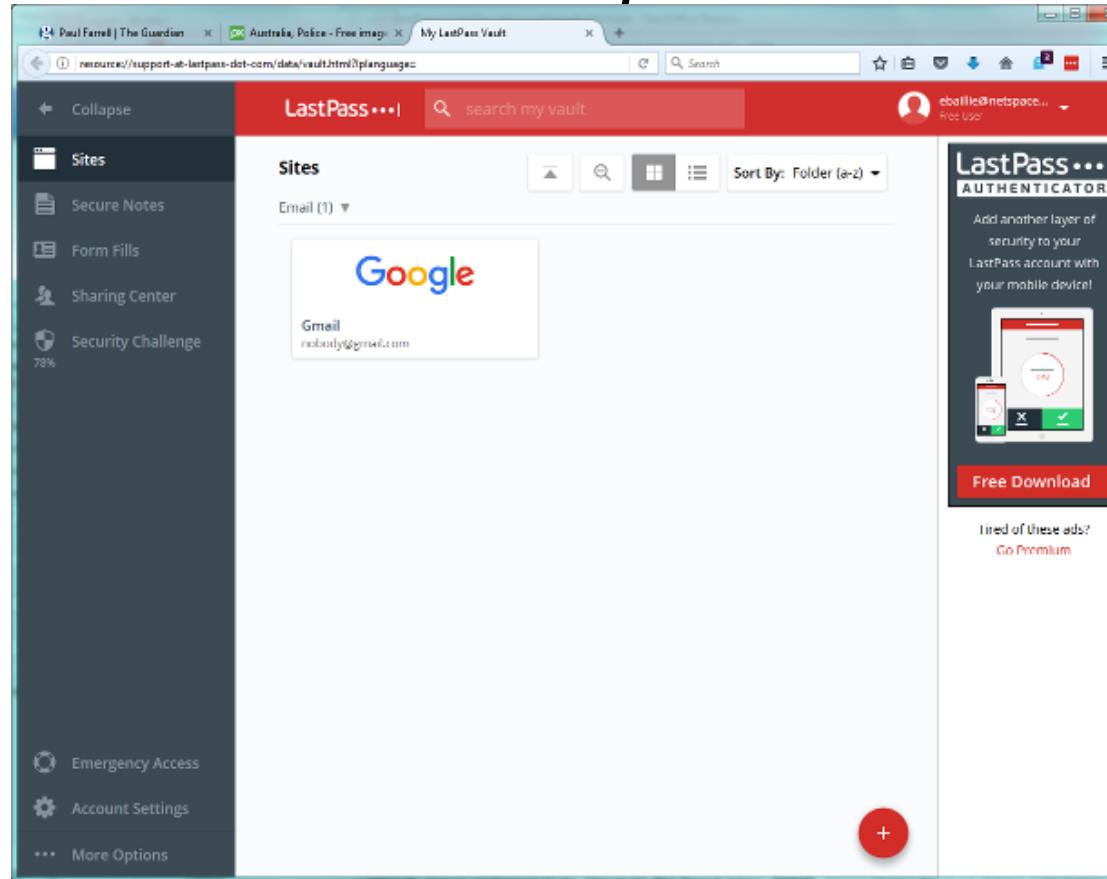
*www.lastpass.co*



*www.lastpass.co*



*www.lastpass.com*



# LastPass Password Strength Tester

passwdTesterLastpass.jpeg

LastPass...| Security Challenge

75% Top 19% 100%

Your Security Score Your LastPass Standing Master Password Score

Challenge your friends [f](#) [t](#)

 Improve Your Score

- Step 1 - Change Compromised Passwords +
- Step 2 - Change Weak Passwords +
- Step 3 - Change Reused Passwords +
- Step 4 - Change Old Passwords +

 Detailed Stats

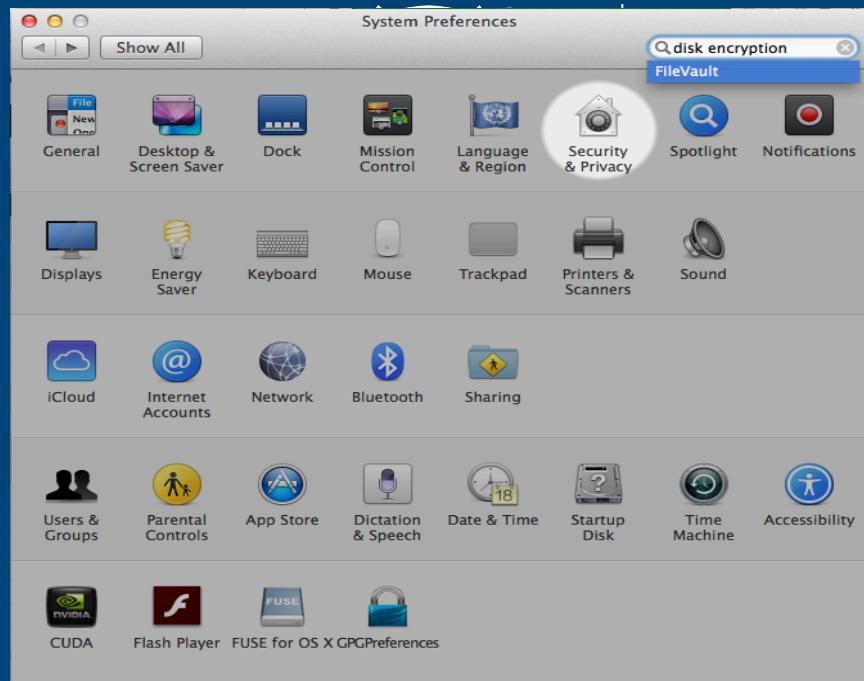
Click each below to see a full report of all the logins and passwords stored in your LastPass vault. On supported websites you can change the password in one click, and you can check more than one to change multiple passwords at once. For other website, use the 'Launch' option to go to the website, login, and use the LastPass Password Generator to replace the account's password.

All (0)  Duplicate (0)  Compromised (0)  Weak (0)  Old (0)  Blank (0)

 [X.com.au](#) 94% -  11 minutes ago [Launch Site](#)

Want to know if your email addresses were leaked in known security breaches? [Check now!](#)

# Encrypt data at rest



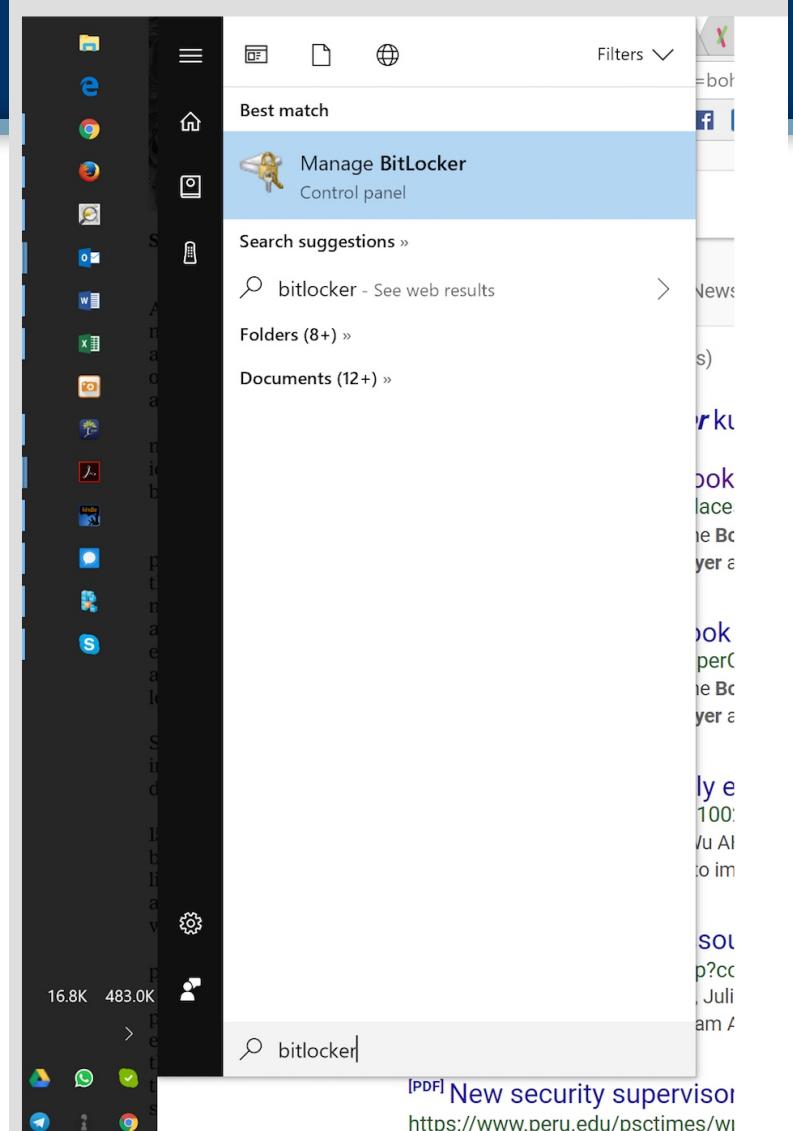
Bitlocker; FileVault.  
You need Win 10 Pro to get Bitlocker included.

## 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.



- 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
- 



## 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 Everywhere](#)

[FAQ](#)

[Report Bugs / Hack On The Code](#)

[Creating HTTPS Everywhere Rulesets](#)

[How to Deploy HTTPS Correctly](#)

[HTTPS Everywhere Atlas](#)

HTTPS Everywhere is a Firefox, Chrome, and Opera extension that encrypts your communications with many major websites, making your browsing more secure. [Encrypt the web: Install HTTPS Everywhere today.](#)



[Install in Firefox](#)



[Install in Firefox for Android](#)



[Install in Chrome](#)



[Install in Opera](#)

HTTPS Everywhere is produced as a collaboration between [The Tor Project](#) and the [Electronic Frontier Foundation](#). Many sites on the web offer some limited support for encryption over [HTTPS](#), but make it difficult to use. For instance, they may default to unencrypted HTTP,

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

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.**

Steps:



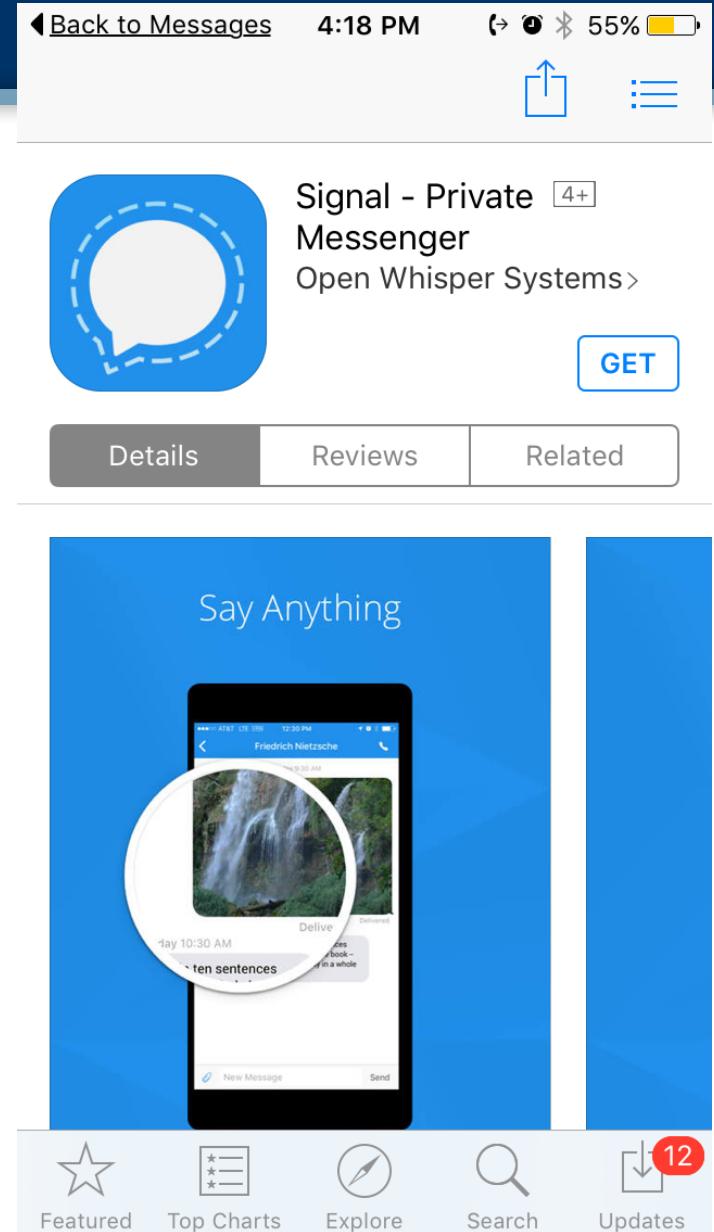
Find a buddy: share phone numbers

Open your App store in your smartphone

Search: Signal Private Messenger (by Whisper Open Systems)

Be sure you get the right App!

Download  
Open



# Signal



**Signal - Private Messenger**  
Open Whisper Sy... [OPEN](#)

**Stay Private**  
Everything is always end-to-end encrypted

**Voice or Video Calls**  
Make crystal-clear voice or video calls from anywhere

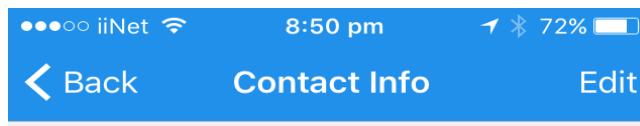


- 
- A list of Signal contacts in the inbox:
- Wilhelm Reich
  - Clement Oval
  - Jules Bonnot
  - Valentine de Chêvre
  - Book Club
  - Chairman Meow
  - Stephen Stills
  - Wengenmünster
  - Nautilus & Journeys

Lois Lane 19/7/16



New Message



57750 43898 33516 16781  
12257 77586 79790 18300  
50354 02060 28620 82214

If you wish to verify the security of your end-to-end encryption with Lois Lane, compare the numbers above with the numbers on their device.

Alternatively, you can scan the code on their phone, or ask them to scan your code.

[Learn More](#)

✓ [Mark as Verified](#)

# Whatsapp – removing cloud backup

••○○○ iiNet WiFi 2:46 pm 75% 🔋

**Settings**

 **Emma** >  
Hey there! I am u...

 **Starred Messages** >

 **WhatsApp Web/Desktop** >

 **Account** >

 **Chats** >

 **Notifications** >

 Status    Calls    Camera    Chats    Settings

••○○○ iiNet WiFi 4:53 pm 60% 🔋

< **Settings**   **Chats**

**Chat Wallpaper** >

**Save to Camera Roll** 

Automatically save photos and videos you receive to your iPhone's Camera Roll.

**Chat Backup** >

[Archive All Chats](#)

[Clear All Chats](#)

 Status    Calls    Camera    Chats    Settings

••○○○ iiNet WiFi 4:54 pm 60% 🔋

< **Chats**   **Chat Backup**

 Last Backup: Never  
Total Size: -

Back up your chat history and media to iCloud so if you lose your iPhone or switch to a new one, your chat history is safe. You can restore your chat history and media when you reinstall WhatsApp. Media and messages you back up are not protected by WhatsApp end-to-end encryption while in iCloud.

[Back Up Now](#)

**Auto Backup** 

# Whatsapp – checking chat security

●●●○ iiNet ⌂ 2:50 pm ↳ 74% 🔋

< Suelette Dreyfus last seen today at 2:12 pm

Today

**🔒 Messages to this chat and calls are now secured with end-to-end encryption. Tap for more info.**

+ |  | | |

I Yes I'm

Q W E R T Y U I O P  
A S D F G H J K L  
Z X C V B N M ↲  
123 ⌂ ⌘ space ↵ return

●●●○ iiNet ⌂ 2:51 pm ↳ 73% 🔋

< Suelette Contact Info Edit

Suelette Dreyfus   
+61 419 879 350

Media, Links and D... None >  
 Starred Messages None >  
 Mute No >  
 Custom... Default (Note) >  
 Save Media to C... Default >

**Encryption**  
Messages to this chat and calls are secured with end-to-end encryption. Tap to verify.

●●●○ iiNet ⌂ 2:52 pm ↳ 73% 🔋

< Info Verify Security Code You, Suelette

38999 30091 38982 77599  
62249 56887 77978 48721  
02204 93396 65223 40920

Scan the code on your contact's phone, or ask them to scan your code, to verify that the messages and calls with them are end-to-end encrypted. You can also compare the number above to verify. This is optional. [Learn more.](#)

Scan Code

# Whatsapp – security notifications

••••• iiNet WiFi 2:46 pm 75% 🔋

## Settings

Emma Hey there! I am u... >

Starred Messages >

WhatsApp Web/Desktop >

Account >

Chats >

Notifications >

Status Calls Camera Chats Settings

••••• iiNet WiFi 2:46 pm 75% 🔋

< Settings Account

Privacy >

Security >

Two-Step Verification >

Change Number >

Delete My Account >

Status Calls Camera Chats Settings

••••• iiNet WiFi 2:47 pm 75% 🔋

< Account Security

Your messages and calls are secured with end-to-end encryption, which means WhatsApp and third parties can't read or listen to them. [Learn more about WhatsApp security.](#)

Show Security Notifications

Turn on this setting to receive notifications when a contact's security code has changed. Your messages and calls are encrypted regardless of this setting.

Status Calls Camera Chats Settings

IMENT PAGES TEXT Zoom

p. 1

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

DIRNSA [REDACTED]

 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]

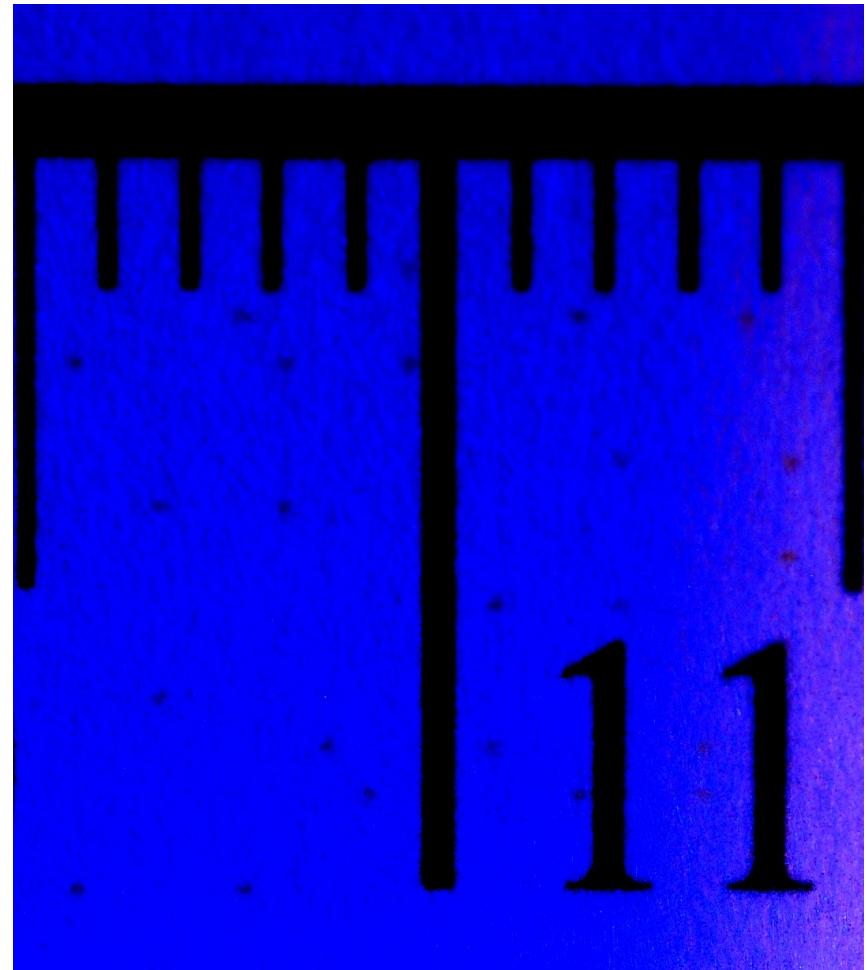
Declassify On: 20420505

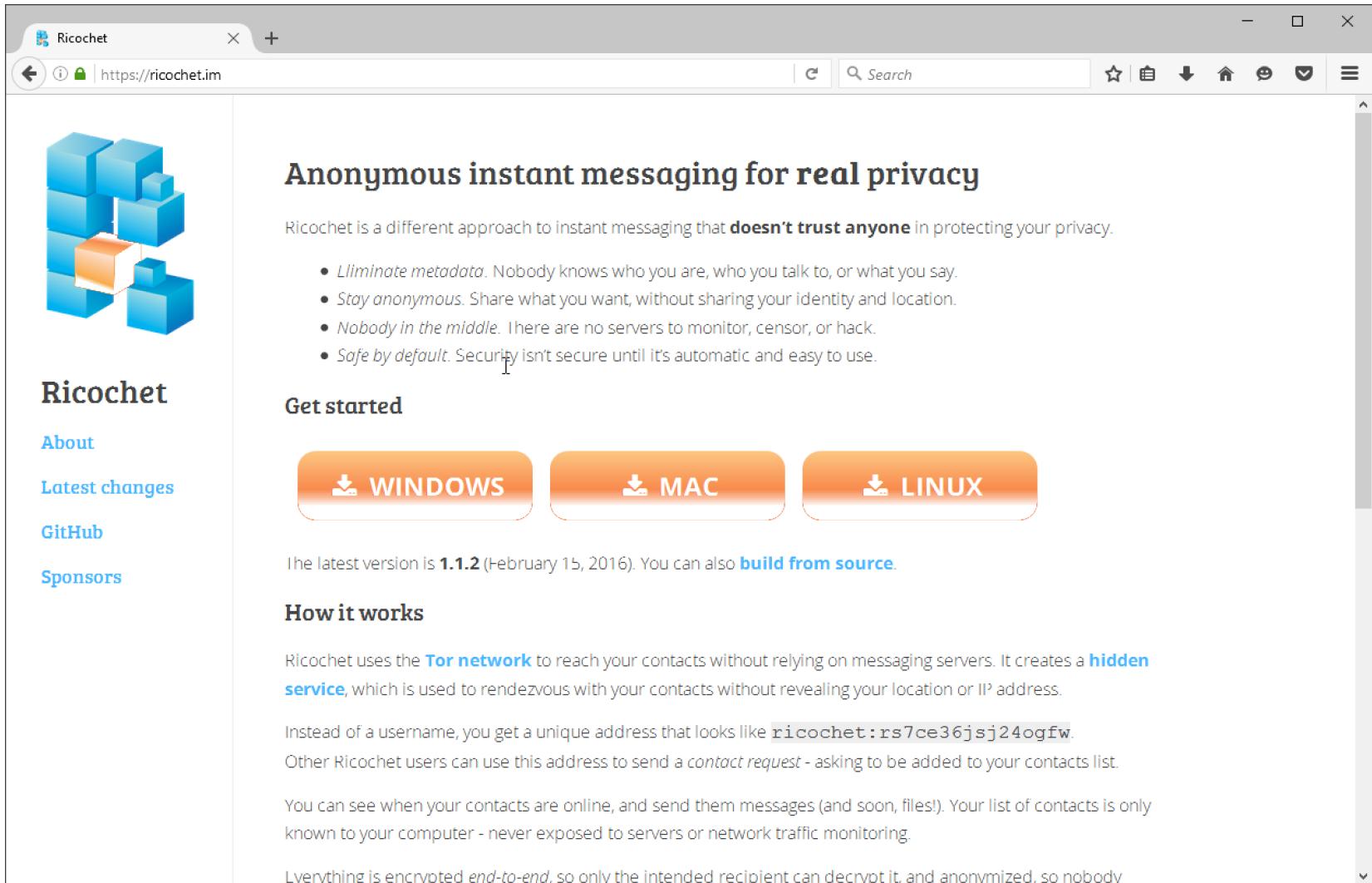


FROM FACEBOOK

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

- 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.





The screenshot shows a web browser displaying the Ricochet website at <https://ricochet.im>. The page has a dark blue header with the Ricochet logo and title. The main content area features a large blue 3D cube icon on the left, followed by text and download links for Windows, Mac, and Linux. The page describes Ricochet as anonymous instant messaging for real privacy, mentioning its focus on metadata elimination, anonymity, no middleman, and being safe by default.

**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.

- *Llimate 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**

[!\[\]\(4e3e717ab100d922ed16b4f67c0941ee\_img.jpg\) WINDOWS](#)

[!\[\]\(eb688e7697c23b01443b634af381fa38\_img.jpg\) MAC](#)

[!\[\]\(831ec440f411c9caa717c4dbbc32e3e2\_img.jpg\) LINUX](#)

The latest version is **1.1.2** (February 15, 2016). You can also [build from source](#).

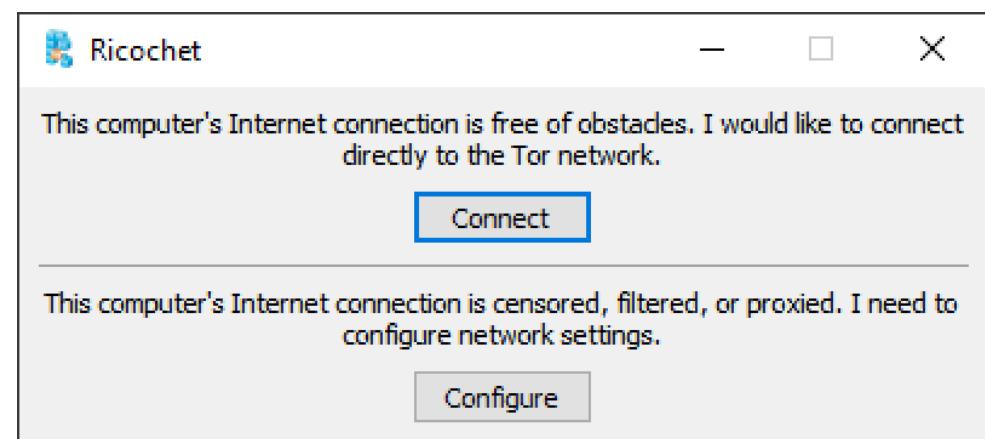
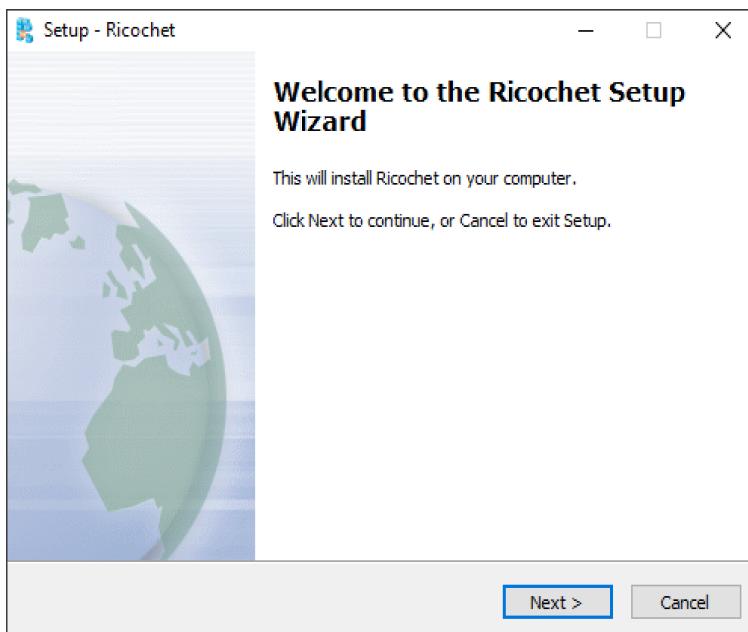
**How it works**

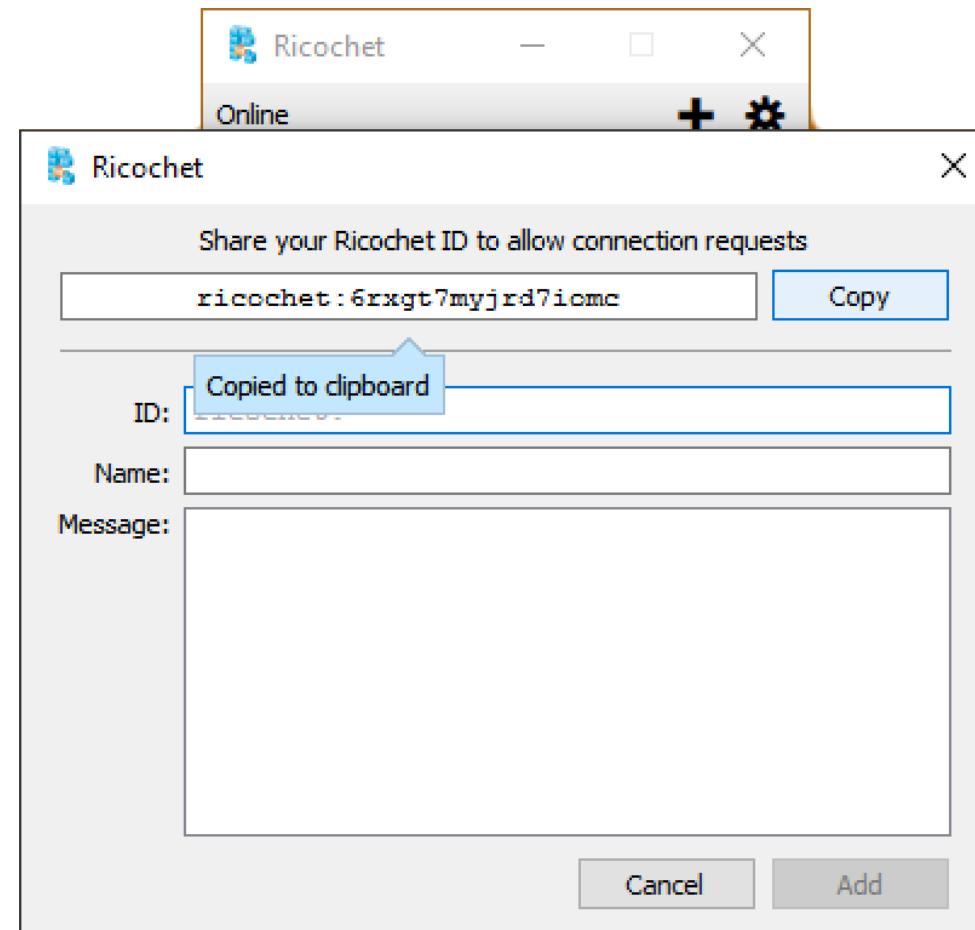
Ricochet uses the **Tor network** to reach your contacts without relying on messaging servers. It creates a **hidden service**, which is used to rendezvous with your contacts without revealing your location or IP address.

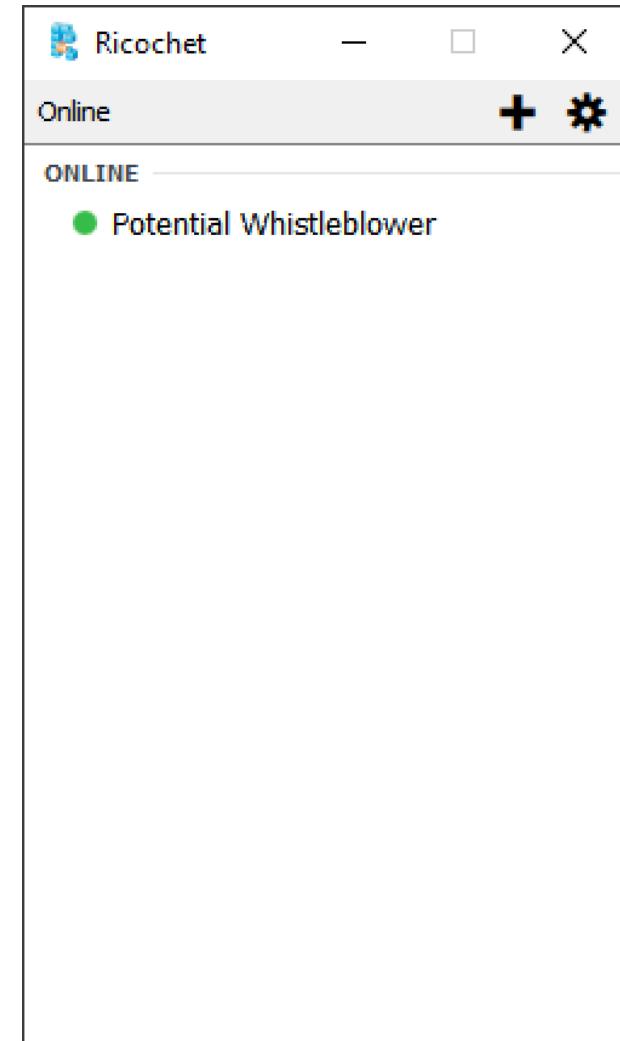
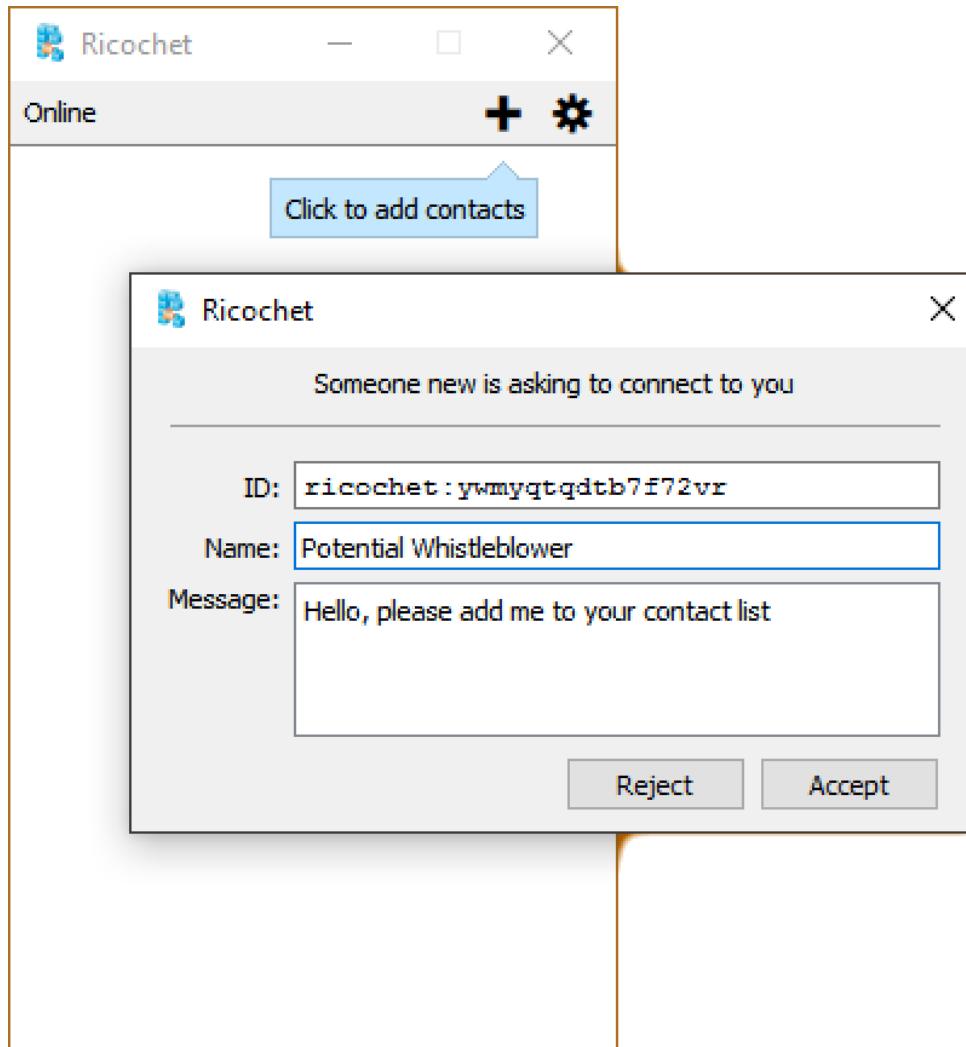
Instead of a username, you get a unique address that looks like `ricochet:rs7ce36jsj24ogEw`. Other Ricochet users can use this address to send a *contact request* - asking to be added to your contacts list.

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

Online

ONLINE

Potential Whistleblower

+

Potential Whistleblower

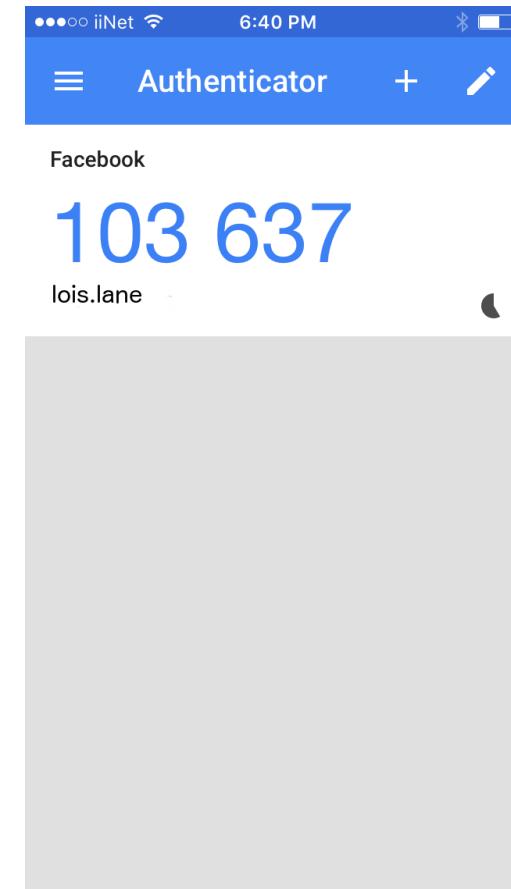
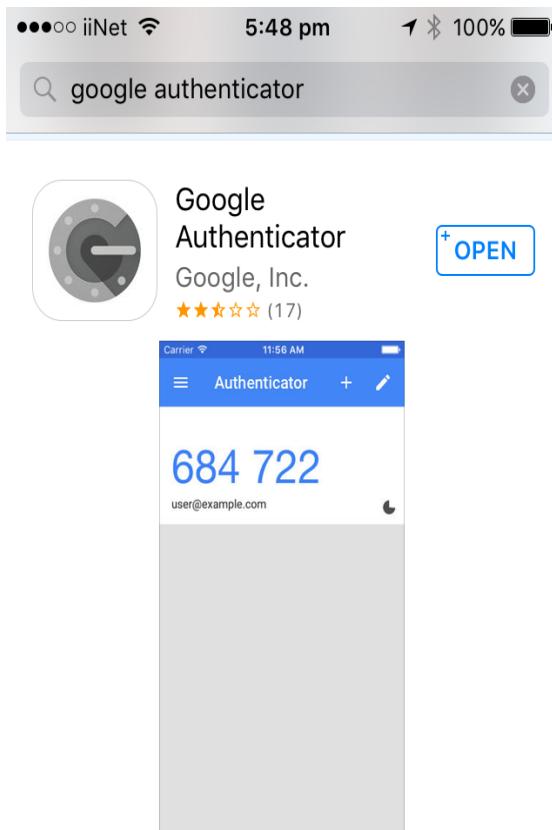
Potential Whistleblower

28/06/2016 2:21 PM

Hello, I have something interesting for you

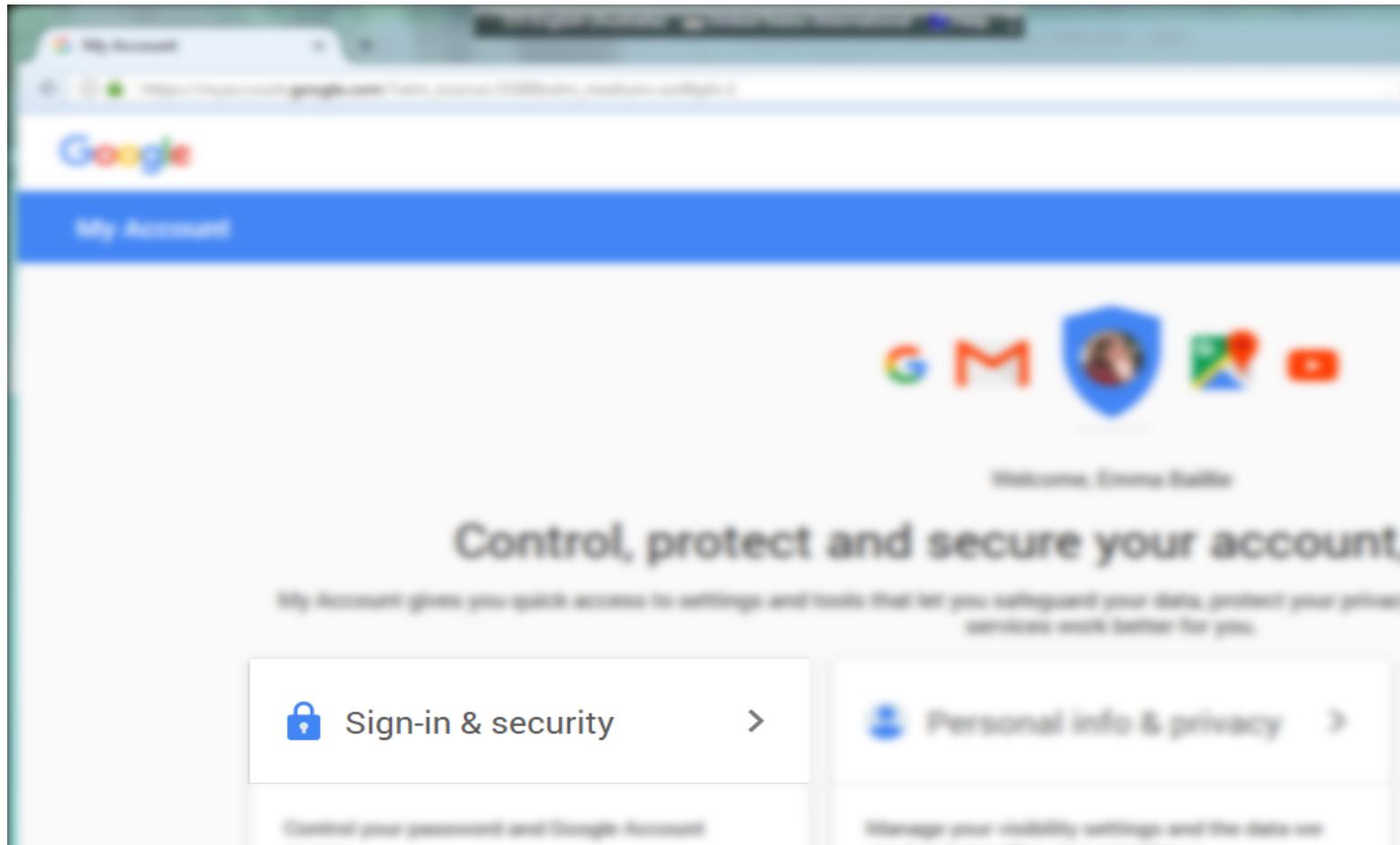
Cool, thanks for contacting me

# Google Authenticator

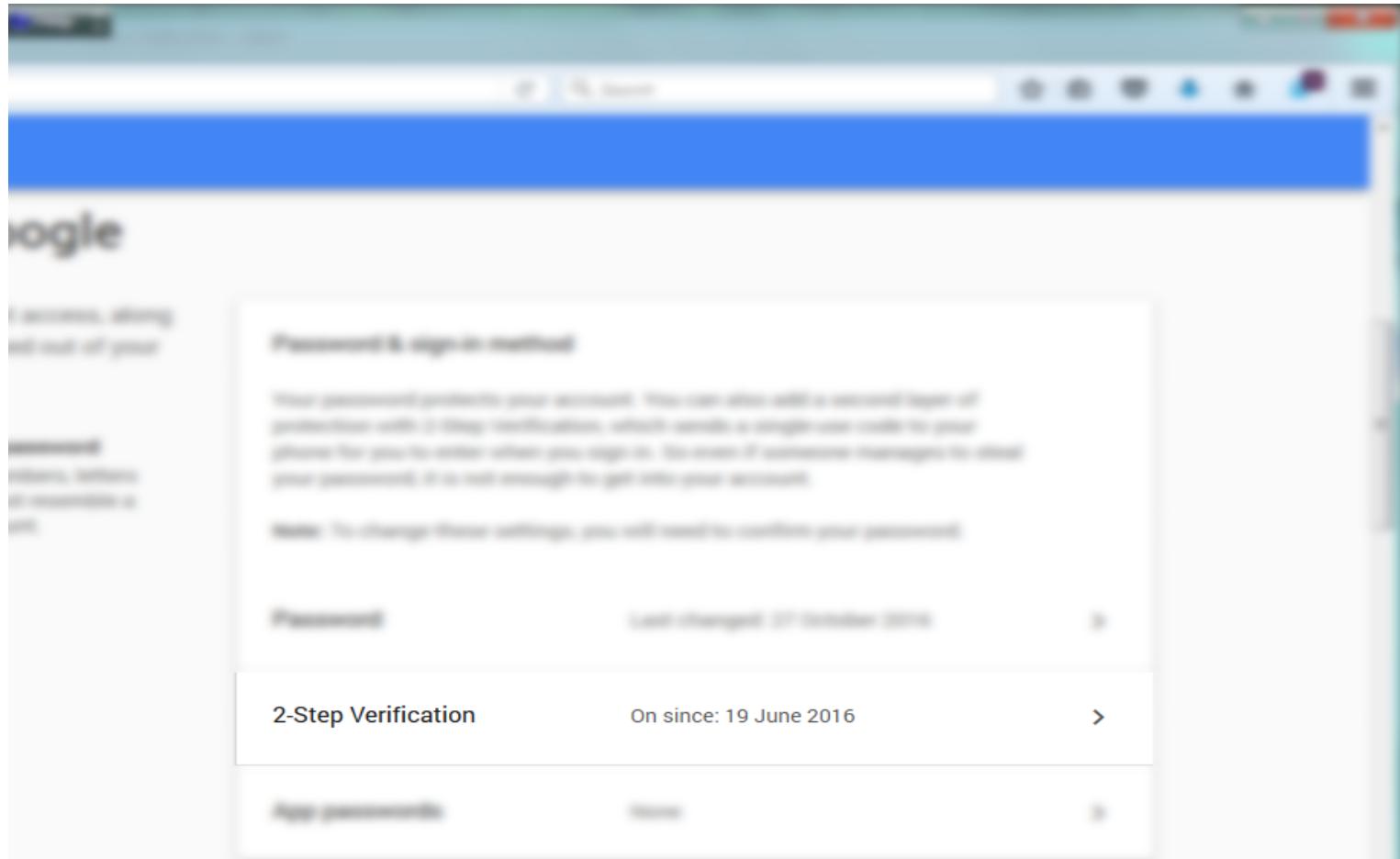


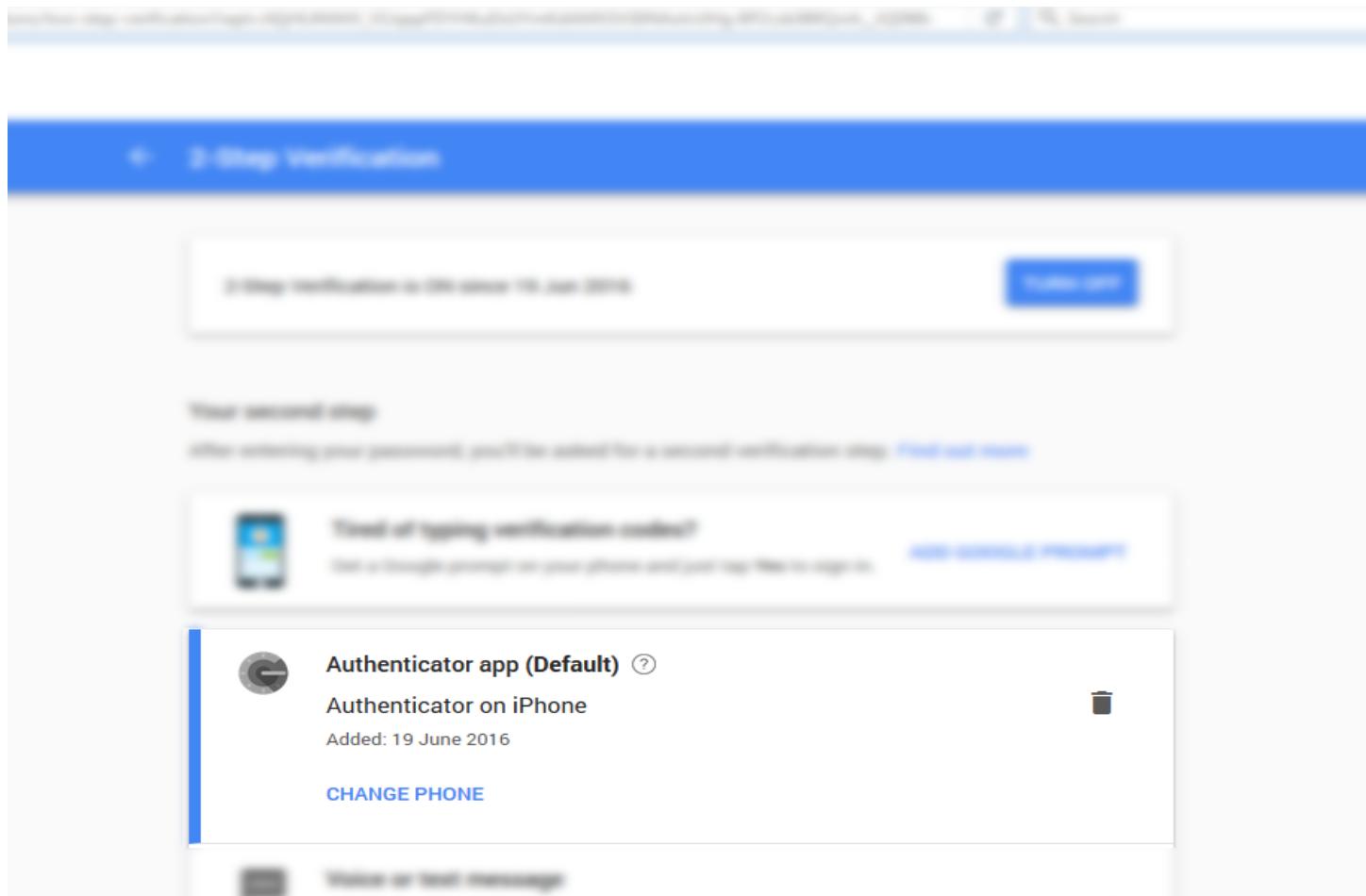


## 2 Factor Authentication - gmail



The screenshot shows the Google My Account interface. At the top, there's a blurred header bar with tabs like "My Account" and "Google". Below that is a blue navigation bar with icons for "Gmail" (with a shield and profile picture), "Google Photos", "Google Sheets", and "Google Slides". The main content area is titled "Welcome, Emma Ballie" and features a large heading "Control, protect and secure your account.". A sub-section below it says "My Account gives you quick access to settings and tools that let you safeguard your data, protect your privacy, and make Google work better for you." There are two main buttons: "Sign-in & security" (with a lock icon) and "Personal info & privacy" (with a person icon). Below each button is a small explanatory text: "Control your password and Google Account" under Sign-in & security, and "Manage your visibility settings and the data we" under Personal info & privacy.





A screenshot of the Google Two-Step Verification settings page. At the top, there's a blue header bar with the text "2-Step Verification". Below it, a white card displays a QR code with the text "Scan me" and "Barcode verification is valid until 19 June 2019". A blue "VERIFY" button is to the right. Under "Your second step", it says "After entering your password, you'll be asked for a second verification step" with a "Read more" link. Below that, a section titled "How do I get my verification codes?" shows an icon of a smartphone and a "Get started" button. The main list shows an entry for "Authenticator app (Default)". This entry includes a circular icon with a minus sign, the text "Authenticator app (Default)", a question mark icon, "Authenticator on iPhone", and "Added: 19 June 2016". There's also a blue "CHANGE PHONE" button and a small trash can icon. At the bottom of the card, there's a "Scan me" button and a "Verify an email message" link.

2-Step Verification

Scan me

Barcode verification is valid until 19 June 2019

VERIFY

Your second step

After entering your password, you'll be asked for a second verification step [Read more](#)

How do I get my verification codes?

Authenticator app (Default)

Authenticator on iPhone

Added: 19 June 2016

CHANGE PHONE

Scan me

Verify an email message

## 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.

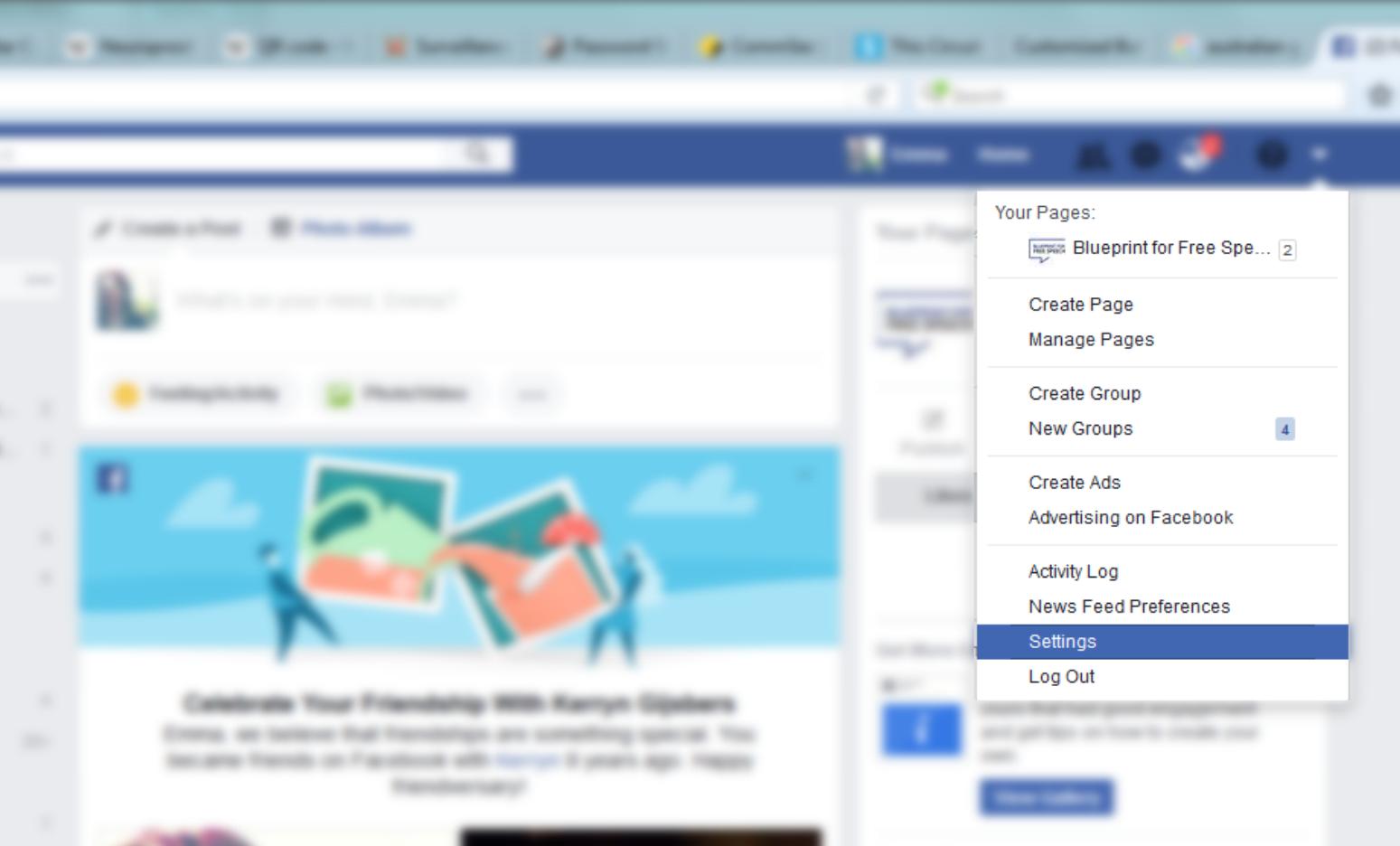
[ADD PHONE](#)



### 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](#)



Your Pages:

Blueprint for Free Spe... [2]

---

Create Page

Manage Pages

---

Create Group

New Groups [4]

---

Create Ads

Advertising on Facebook

---

Activity Log

News Feed Preferences

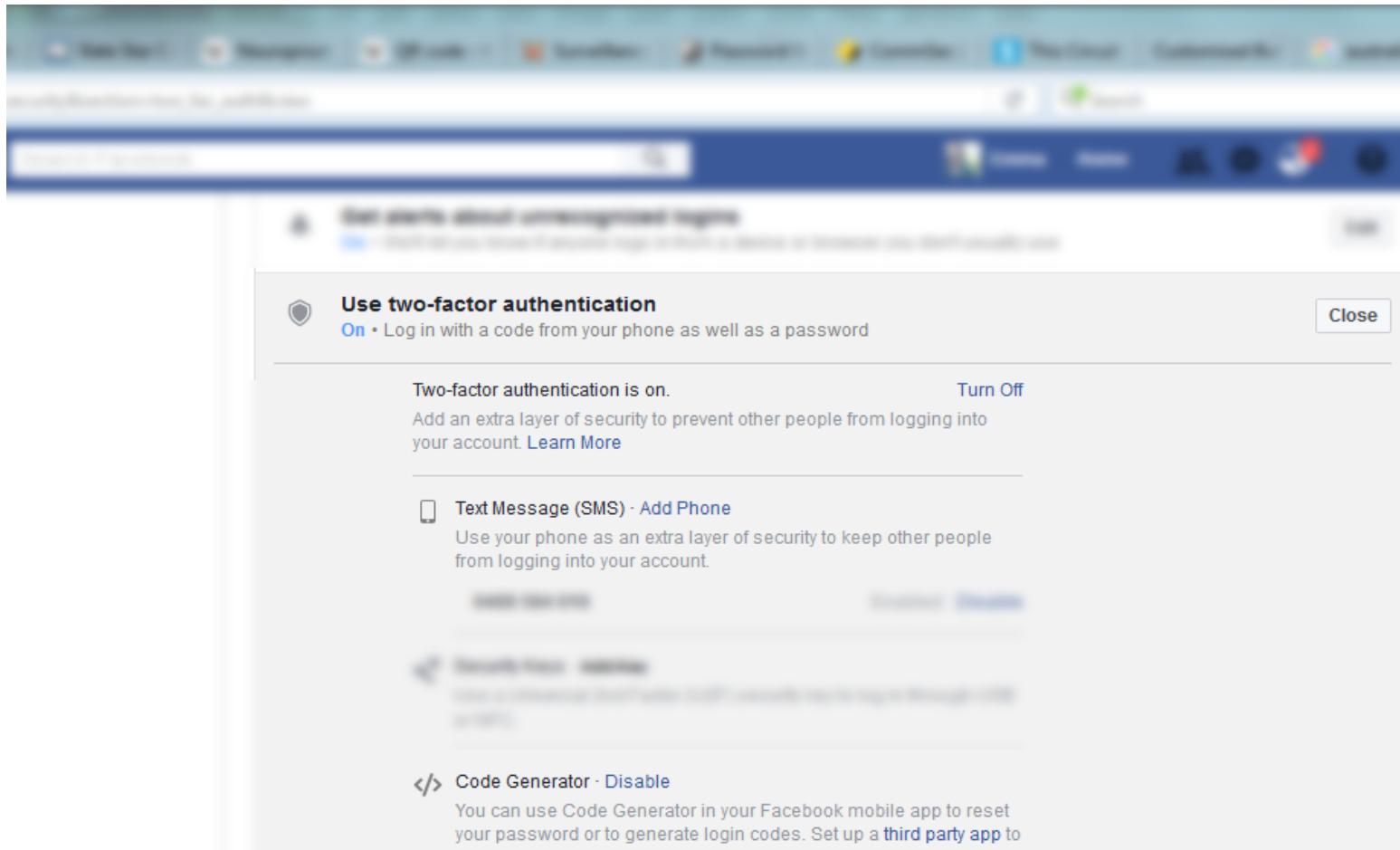
**Settings**

Log Out



2fa - Facebook

The screenshot shows the 'Security and Login' section of the Facebook settings. The left sidebar lists various categories: General, Security and Login (selected), Privacy, Timeline and Tagging, Blocking, Language, Notifications, Mobile, Public Posts, Apps, Ads, Payments, Support Inbox, and Videos. The main content area displays the 'Security and Login' settings, which include sections for 'Recent logins', 'Device Logins', and 'Logins from Friends'. It also shows a list of devices connected to the account, including a Windows PC, a mobile phone, and a laptop.



**Use two-factor authentication**

**On** • Log in with a code from your phone as well as a password Close

---

Two-factor authentication is on. Turn Off

Add an extra layer of security to prevent other people from logging into your account. [Learn More](#)

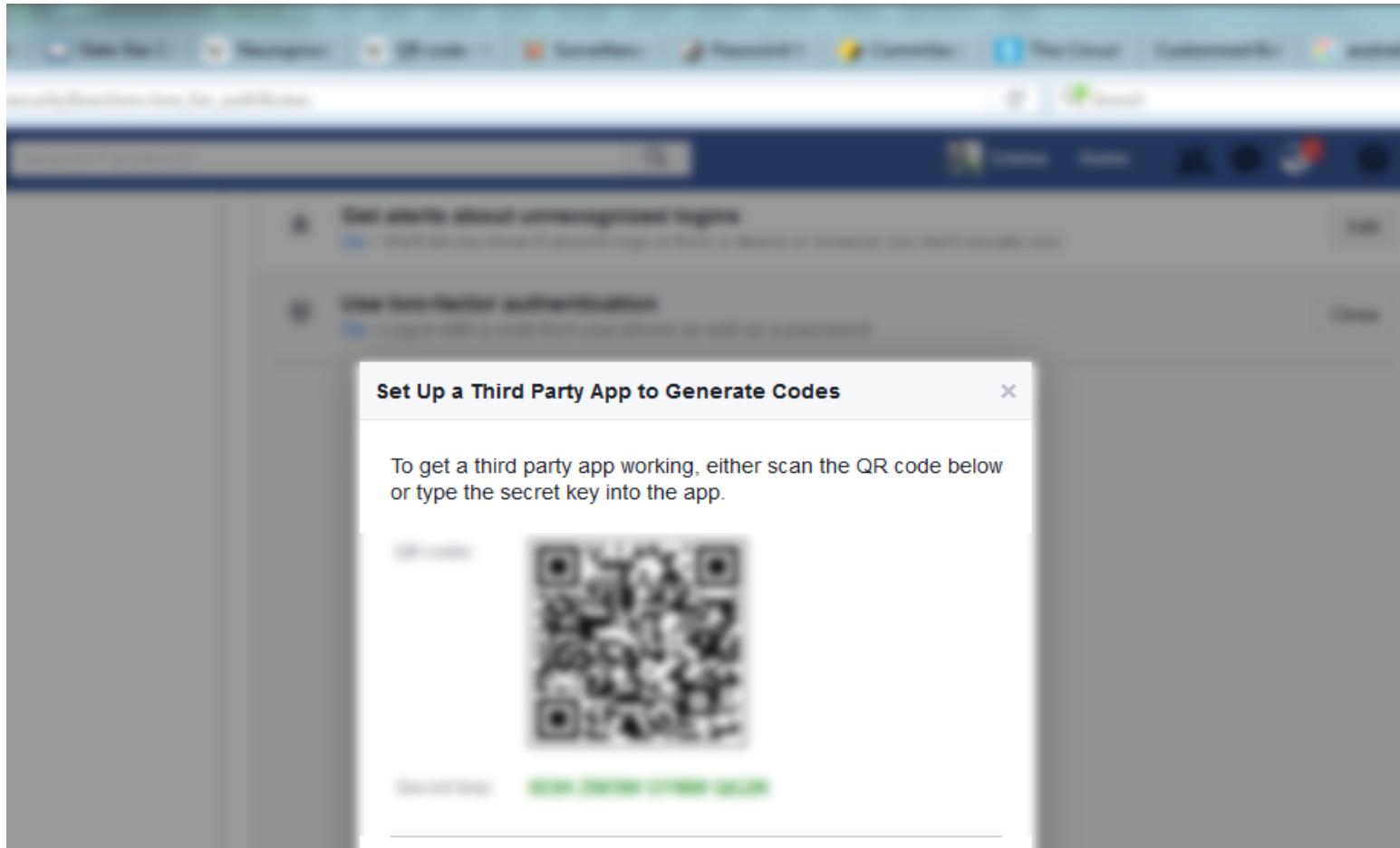
---

 **Text Message (SMS) · Add Phone**

Use your phone as an extra layer of security to keep other people from logging into your account.

 **Code Generator · Disable**

You can use Code Generator in your Facebook mobile app to reset your password or to generate login codes. Set up a [third party app](#) to



# 2fa

# Facebook

## Use two-factor authentication

On • Log in using a code from your phone as well as a password

[Close](#)

Two-factor authentication is on.

[Turn off](#)

Add an extra layer of security to prevent other people from logging in to your account. [Learn more](#)



[Text message \(SMS\)](#) · [Add phone number](#)

Use your phone as an extra layer of security to keep other people from logging in to your account.

0419 879 350

[Enabled](#) · [Disable](#)



[Security keys](#) · [Add key](#)

Use a Universal 2nd Factor (U2F) security key to log in via USB or NFC.



[Code generator](#) · [Disable](#)

You can use Code Generator in your Facebook mobile app to reset your password or generate login codes. Set up a [third-party app](#) to generate codes.



[Recovery codes](#) · [Get codes](#)

Use these codes when you don't have your phone with you, such as when you're travelling.



[App passwords](#) · [Generate](#)

Get a unique, one-off password for apps that don't support two-factor authentication (e.g. Xbox, Spotify) [Learn more](#)



[Authorised logins](#) · [Close](#)

Review a list of devices on which you won't have to use a login code

## Advanced



### Encrypted notification emails

Add extra security to notification emails from Facebook (only you can decrypt these emails)

[Close](#)

#### Your OpenPGP public key

Enter your OpenPGP public key here:

Enter a PGP public key

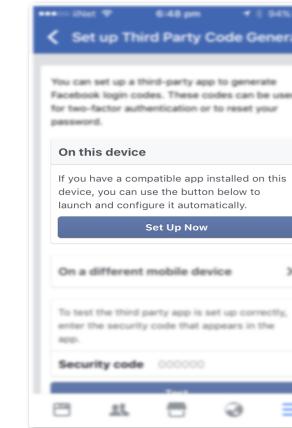
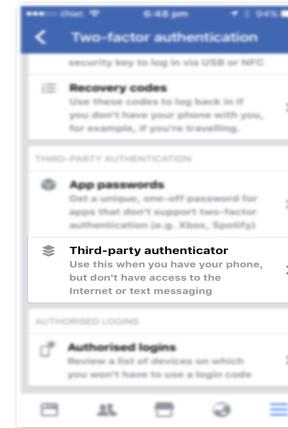
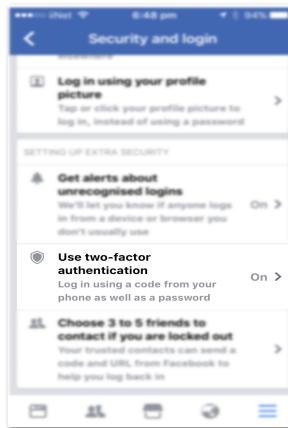
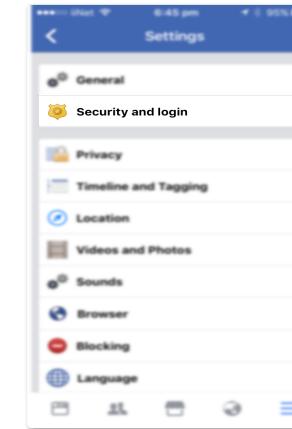
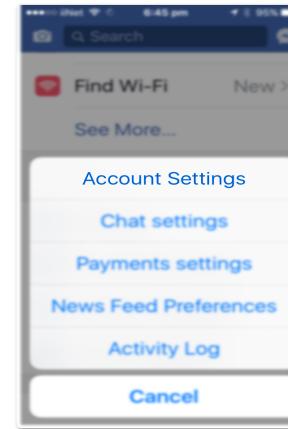
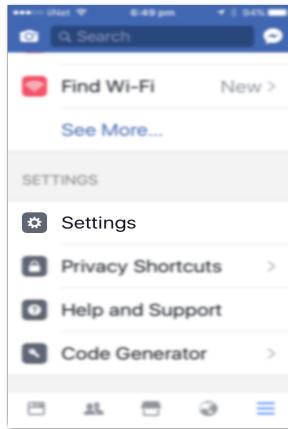
Use this public key to encrypt notification emails that Facebook sends you? [\[?\]](#)

If you wish to share your public key, you can change who can see it in your profile's [Contact and basic info about page](#).

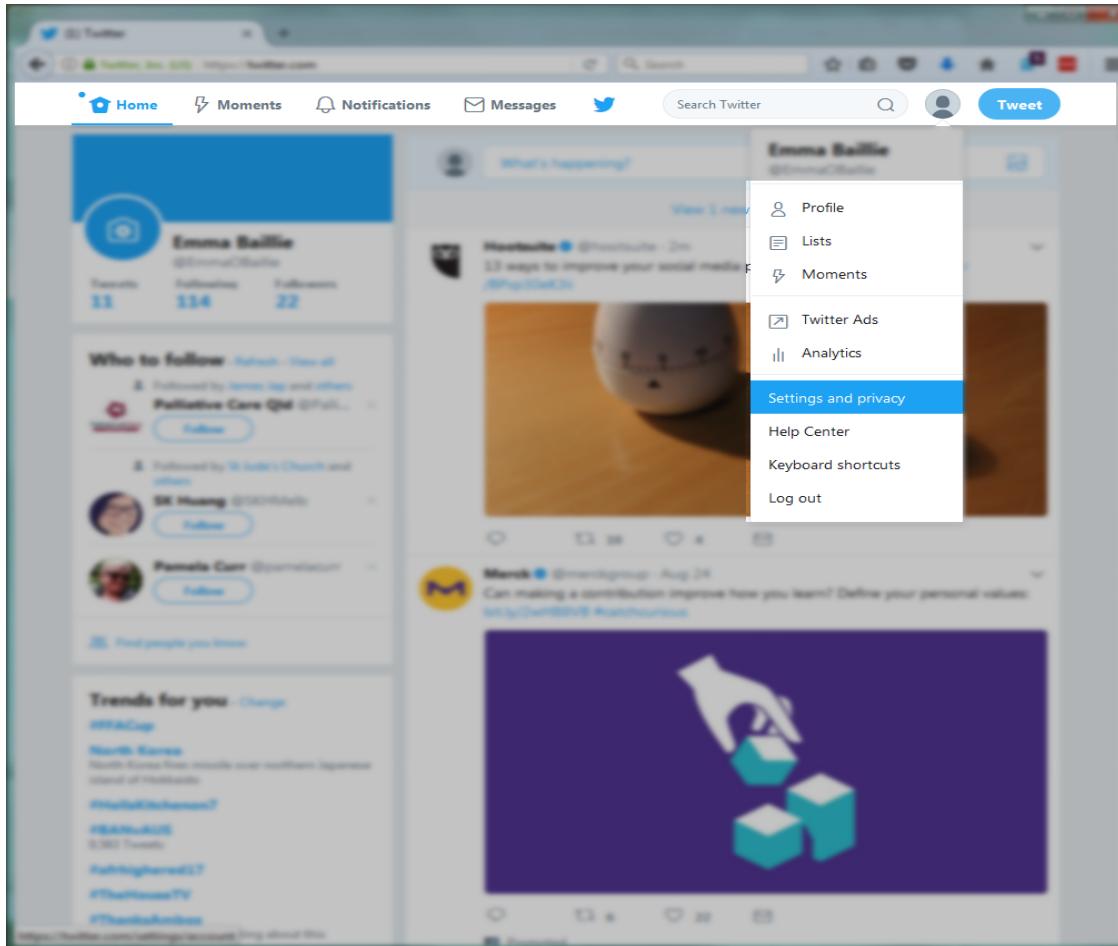
You can download Facebook's public key [here](#).

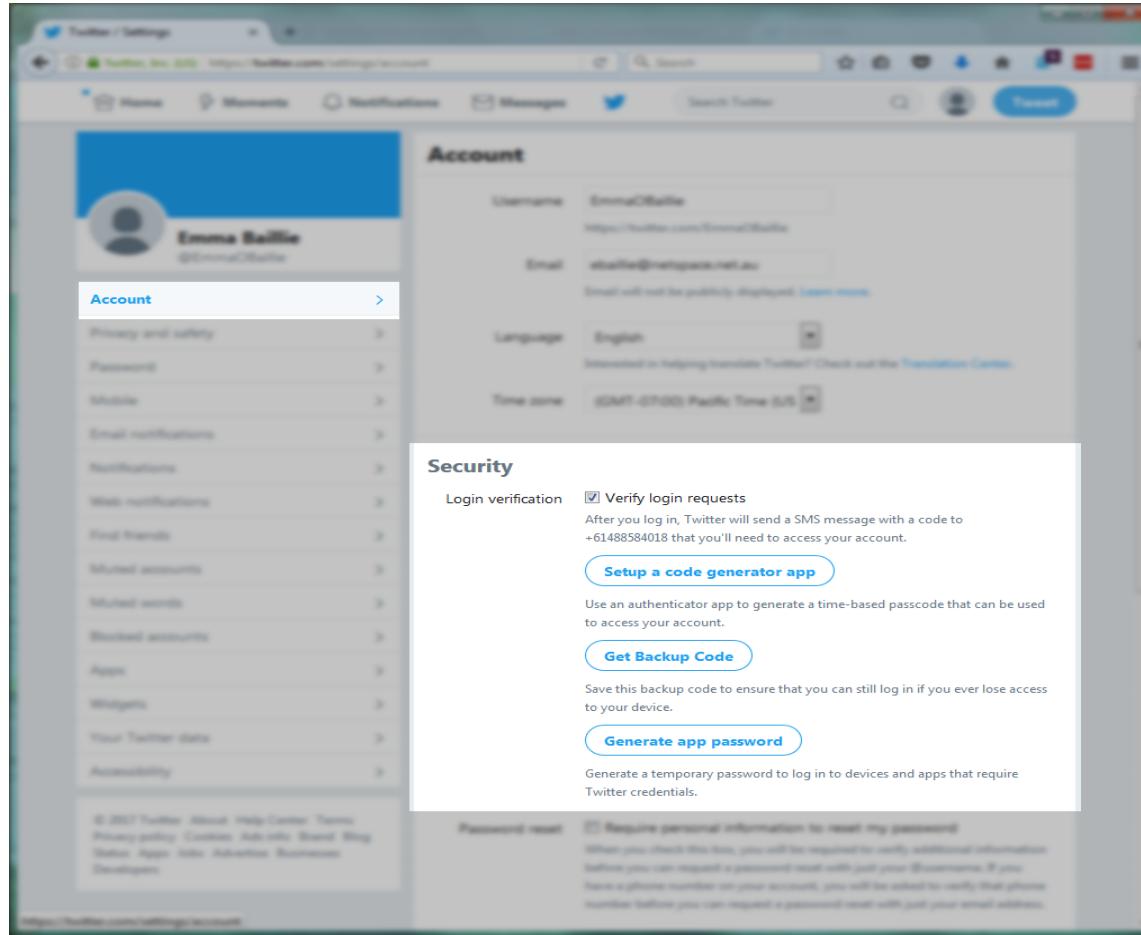
[Save Changes](#)

# 2fa – Facebook setup on Phones



## 2fa - Twitter





The screenshot shows the Twitter account settings page for a user named Emma Baillie (@EmmaOBaillie). The main account information is displayed, including the username (EmmaOBaillie), email (emmaobaille@metaspaces.net.au), language (English), and time zone (EDT-07:00 Pacific Time (US)). A sidebar on the left lists various account management options such as Privacy and safety, Password, Mobile, Email notifications, Notifications, Web notifications, Friend friends, Muted accounts, Muted words, Blocked accounts, Apps, Widgets, Your Twitter data, and Accessibility.

**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.

[Password Reset](#)  Require personal information to reset my password

When you check this box, you will be required to verify additional information before you can request a password reset with just your @username. If you have a phone number on your account, you will be asked to verify that phone number before you can request a password reset with just your email address.

•••• 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% 

•••• iiNet ⌘ 3:01 pm 72% 

< **Settings and privacy** < **Account**  
@EmmaOBaillie @EmmaOBaillie

---

**@EmmaOBaillie**

Account >

Privacy and safety >

Notifications >

Content preferences >

---

**General**

Display and sound >

Data usage >

Accessibility >

About Twitter >

---

**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%

••••• iiNet 3:02 pm 72%

••••• iiNet 3:13 pm 69%

**Security**  
@EmmaOBaillie

**Login verification** 

**Login code generator** >

**Backup code** >

**Temporary password** >

**Login code generator**  
@EmmaOBaillie

Enter this code to complete login to your Twitter account.

**545 096 C**

This code will update every 30 seconds.

You can also use a third party authenticator app to generate login verification codes. [Learn more](#)

**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

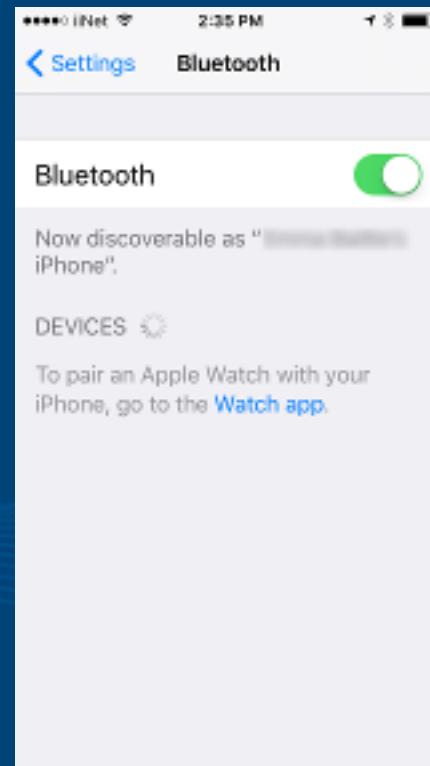
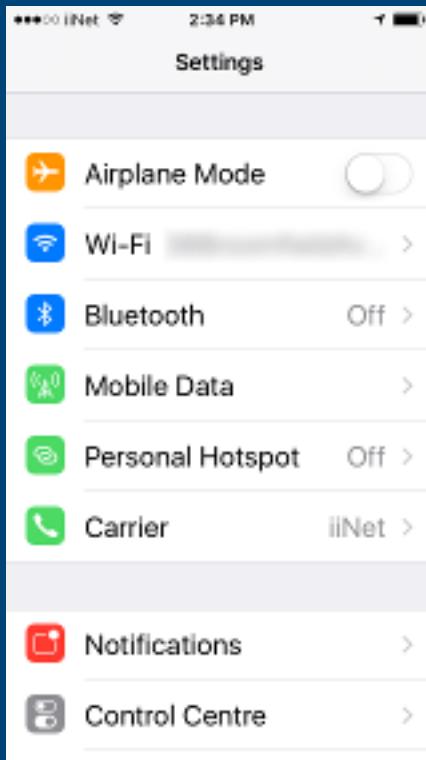
**Submit**

You can also [use a saved backup code](#) to log in.

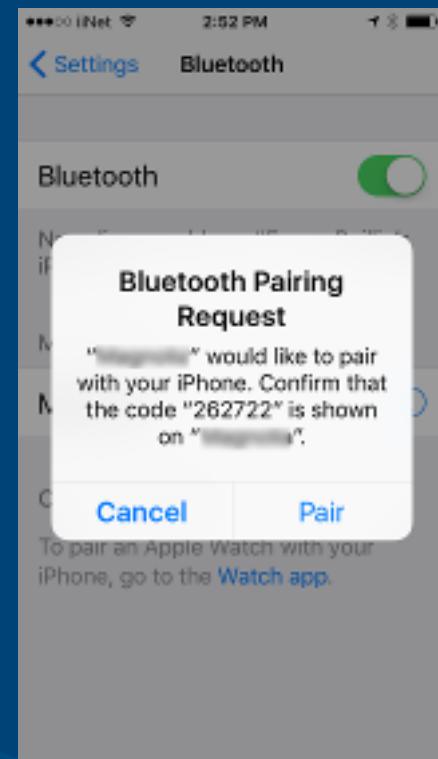
Need help? Please contact [Twitter Support](#).



## 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.

Licensed by the International Computer Science Institute under a Creative Commons Attribution 4.0 License (CC-BY)

Thoughtworks workshop training CryptoParty Melbourne trainers