NPCC
National Police Chiefs' Council

Issued by the National Policing DCG Futures Group
Version 2016_07
27 July 2016

Stay Secure Online 2016

A review of the privacy options currently available to users

TRMG

Produced by The Risk Management Group

This document only describes the privacy options available to users.

Contents

Foreword 03
Hacker Girl; The Naïve Banker 04
Secure Social Media 08
- Facebook 13
- LinkedIn 20
- Twitter 28
- Google+ 37

The Case of the Facebook Friends 43
Browsers 53
- Opera 54
- Chrome 60
- Firefox 68
- Internet Explorer 71

Smartphones 78
- Android 79
- Blackberry 87
- iOS 91
- Windows 100

Hacker Girl; Will you be my friend? 108
Secure Gmail 115
Secure Snapchat 120
Credits 124

Foreword

By ACC Richard Berry, Assistant Chief Constable, Gloucestershire Constabulary

We live in the age of the digital, with information readily accessible to all who seek to find it, including those who we wish to keep it safe from. With every tweet, like or share, our digital footprint grows. It is our responsibility, as individuals, to keep our data safe.

This book provides tips and guidance on protecting your online data across a range of social media platforms, browsers and devices. This guide has been written with sharing in mind so please feel free to share it with family and friends, as in some cases it is they who may be putting information about you online when you would rather they did not.

Richard Berry, January 2016

Richard Berry is the National Policing lead for Communications Data and Chair of the Data Communications Group. He is a core member of the NPCC Capability Management Group for digital investigations and has specific responsibility for the People strand. Richard has been engaged in developing a range of leading edge digital capabilities and cyber-crime projects both locally and nationally.

NPCC
National Police Chiefs' Council

Important note: This book contains a summary of the common body of knowledge with respect to online security for social media, browsers and smartphones as at end December 2015. It is not an operational guide and merely sets out the security options available. Online sites and services change all the time and readers should consult other sources, or new releases of this document, for updated information. See the disclaimer on the final page for further information.

Hacker Girl Episode One

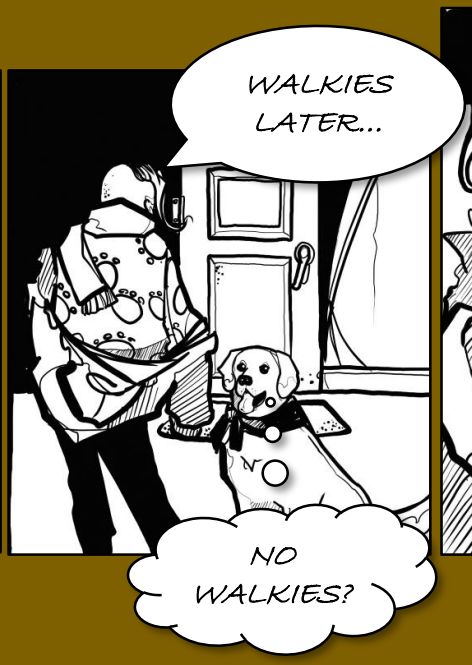
The Case of the Naïve Banker

Copyright: The Risk Management Group
January 2016

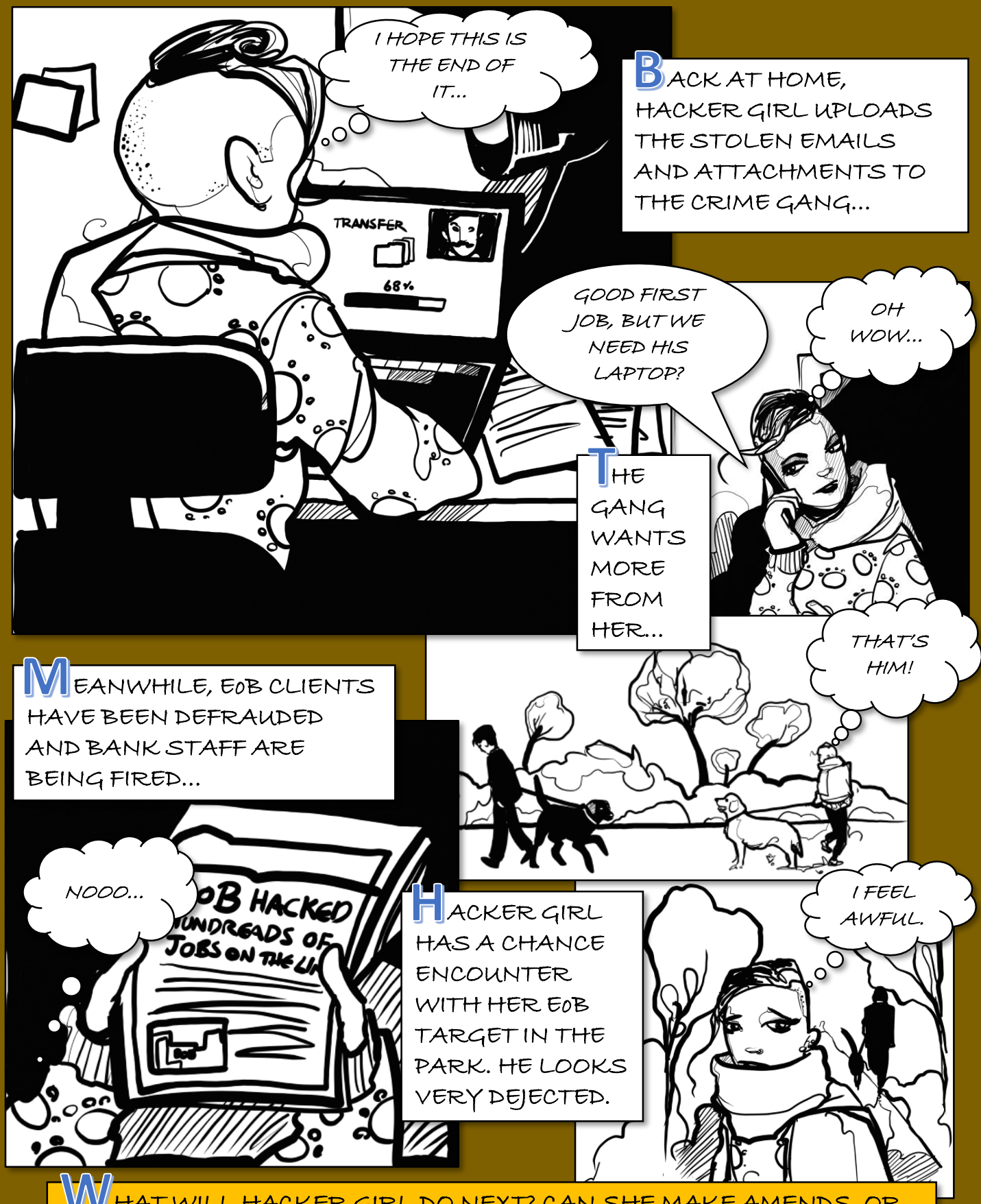
Criminals regularly use social media as a reconnaissance tool.

HACKER GIRL IS IN DEBT TO A CRIME GANG. UNFORTUNATELY, THEY HAVE LEARNED OF HER HACKING SKILLS AND NOW SHE HAS TO WORK OFF WHAT SHE OWES...

SHE DOESN'T WANT TO DO IT, BUT SHE HAS NO WAY OUT. SHE'S CONVINCED THE GANG WILL KILL HER IF SHE DOESN'T HELP THEM. TIME TO GET TO IT, SHE DECIDES. SHE WILL START BY SEARCHING LINKEDIN AND THEN SHE'LL TRY SOME OLD FASHIONED SURVEILLANCE.



AFTER SEVERAL TRIES, SHE FINALLY SPOTS HER MAN.
THERE HE IS!
I'LL USE THIS WIFI HIJACKING TOOLKIT...
HACKER GIRL USES A SPECIALIST TOOLKIT TO HIJACK THE BANKER'S WIFI CONNECTION.
THE BANKER'S IS USING A PUBLIC WIFI HOTSPOT DURING HIS BREAK TO SEND UNECRYPTED EMAILS TO CLIENTS.
Zap!
BINGO!!!

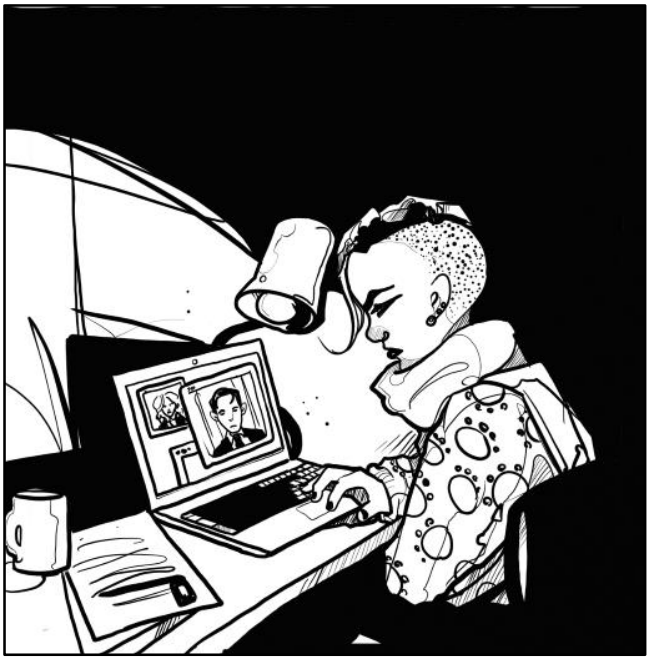


WHAT WILL HACKER GIRL DO NEXT? CAN SHE MAKE AMENDS, OR WILL SHE CONTINUE TO WORK FOR THE CRIME GANG? CATCH UP WITH HER LATER IN THIS BOOK...

Secure Social Media

IN THE HACKER GIRL STORY, WE SAW HOW SHE USED LINKEDIN AS A TOOL TO IDENTIFY A LIKELY TARGET.

POOR SOCIAL MEDIA HABITS CAN BE A MAJOR RISK TO BOTH INVESTIGATORS AND VICTIMS OF CRIME.



Social media tools such as Facebook, LinkedIn and Twitter have become increasingly popular over the past decade.

In parallel, the use of social media by police officers and policing organisations, both as a means of communication and as an investigative resource, has also increased dramatically.

However, poor social media practices can lead to security breaches that might be exploited by criminals. This risk can be offset in large part by the wise utilisation of the security options provided by social media sites for their users. Unfortunately, many users are unaware of the scope of these controls and where to find them.

This section of the guide provides some high level advice about secure social media practices, as well as details on how you can adjust your security settings to better protect yourself and your colleagues online.

Social Media Risks

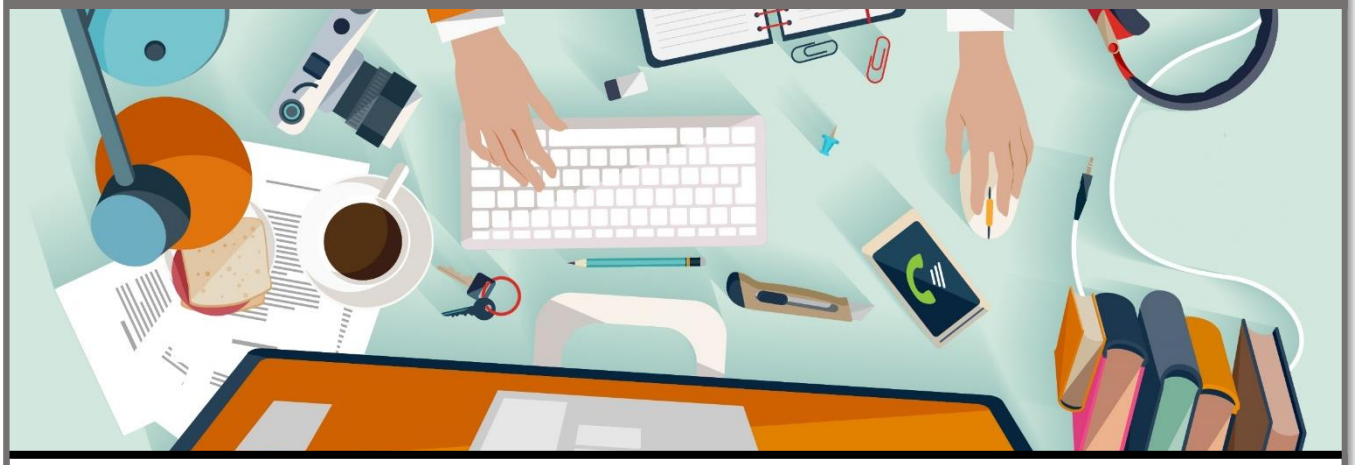
Fake or malicious social media accounts have become a major risk facing social media users and organisations. In 2013 Facebook reported that between 5.5% and 11.2% of its user accounts were fakes or duplicates.

This seems to indicate that more than **100 million** fake Facebook accounts are being used daily worldwide, based on other statistics from the company. Sites such as LinkedIn are also experiencing problems of this nature.

Malicious fake accounts in various social media platforms can be used to commit a range of offences or deceptions, as shown below.

Be wary about accepting social media invitations from people you don't know. Search online to see if the image that person is using actually belongs to someone else; this happens frequently. And never post sensitive work or personal data online.

10 key social media “Do’s and Don’ts”



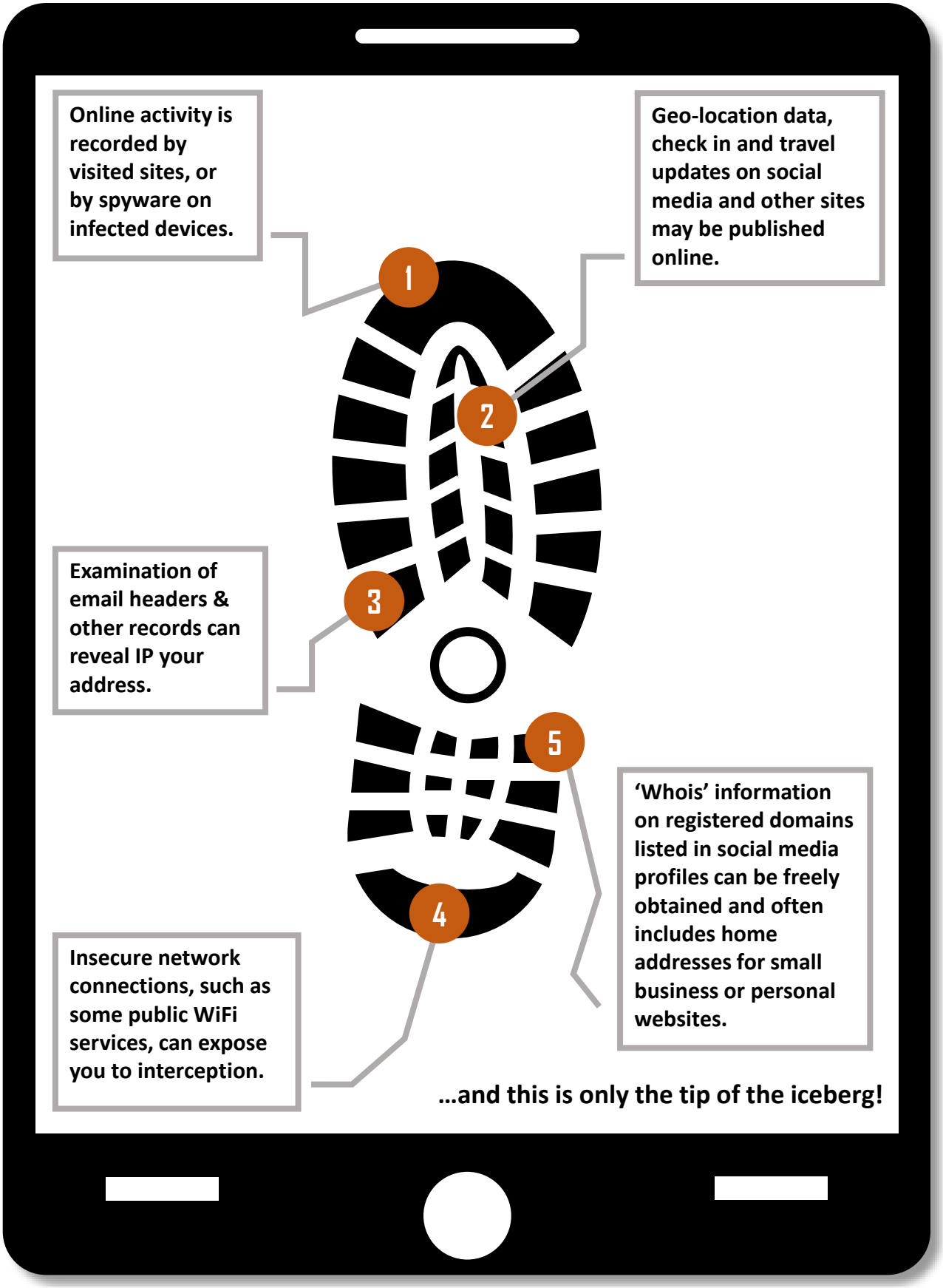
Do

1. Use social media security settings.
2. Turn off location services.
3. Secure your profile data.
4. Limit your search ‘footprint’.
5. Use private browsing.
6. Create a strong password.
7. Change your passwords regularly.
8. Use secure encrypted connections.
9. Use only approved devices and networks.
10. Search using a range of search engines, social feeds and languages.

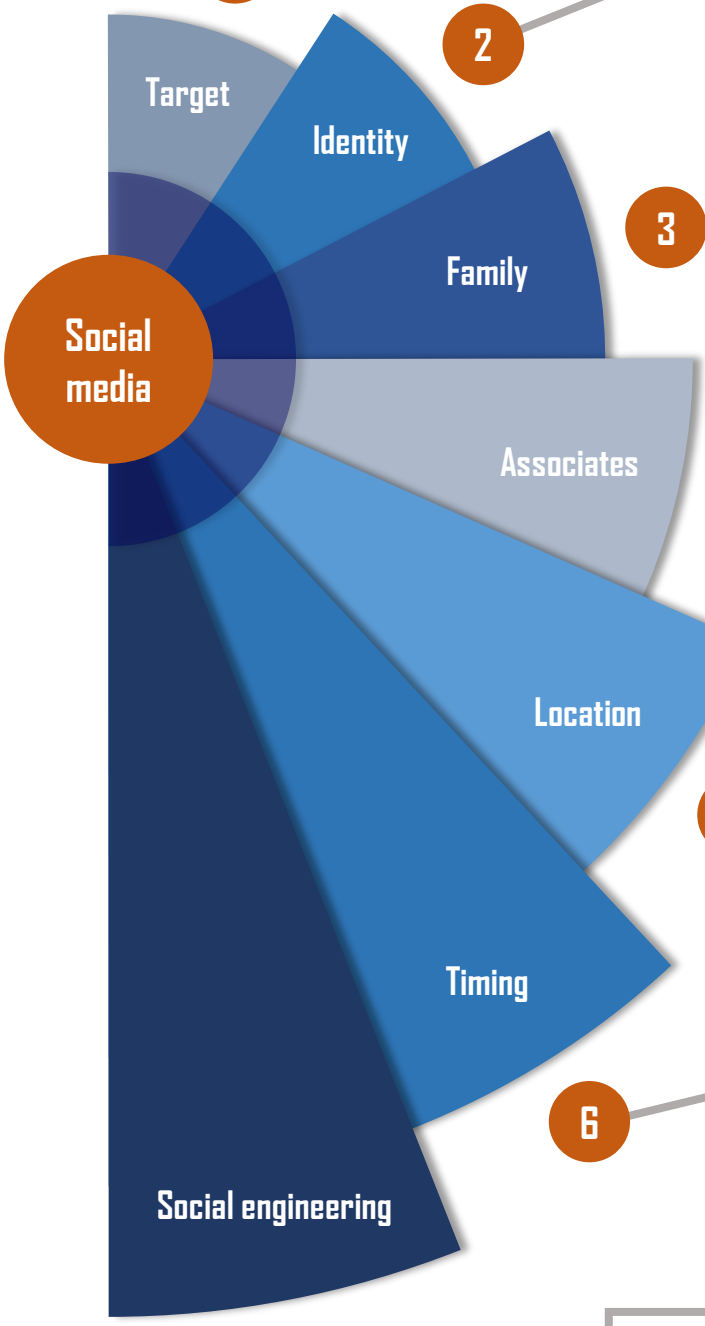
Don’t

1. Post personal details.
2. Use easily identified photos.
3. Allow Apps to access your contacts or your location.
4. Install non-approved Apps.
5. Save payment information.
6. Share your passwords.
7. Leave devices logged on and unattended.
8. Use public WiFi for sensitive tasks.
9. Auto ‘check-in’ to hotspots or social feeds.
10. Visit the profiles of persons of interest using insecure or personal accounts.

Understanding your online footprint



How a criminal might investigate you…



1. Criminals search LinkedIn for anyone whose job title includes the words 'intelligence' or 'investigator'.

2. They then search other sites for the same name, photo and personal data.

3. Having located you on another site, they search for family details, images and other intel.

4. They also connect with your connections in order to gain trust or to gather further background.

5. If the you have location services turned on, criminals might find your geo-tagged Tweets, images or posts.

6. Based on your posts and geo-location data, criminals can guess when you are likely to be at certain locations.

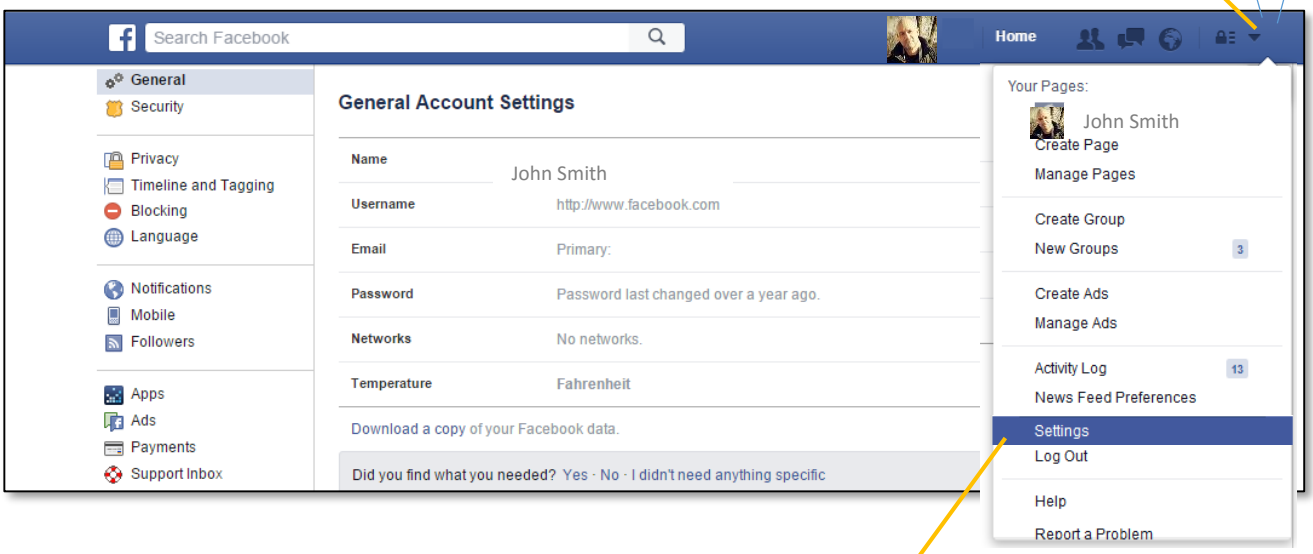
7. Criminals might also attempt to trick you into revealing sensitive information by friending you online, often by offering romance.

Secure Facebook

Note: all screenshots taken from the Facebook.com site. Mobile apps will have differing features.

General account settings

1 *First click here…*



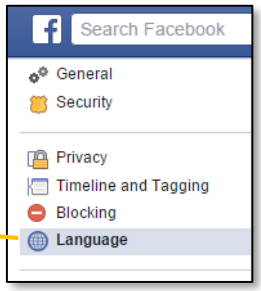
2 *…then click here…*

3

- Select the user name that other users will see.
- Assign an email address – not your work email!
- Change your password frequently.
- **Note**; creating a fake account is a breach of Facebook's T&Cs

4

- Set 'Language' to '**US English**' to exploit all FB search tools



Security: access & edit

Click here to access Security 1

2 *Then click to edit each setting*

General
Security

Privacy
Timeline and Tagging
Blocking
Language

Notifications
Mobile
Followers

Apps
Ads
Payments
Support Inbox

Security Settings

Login Alerts	Get an alert when anyone logs into your account from a new device or browser.	Edit
Login Approvals	Use your phone as an extra layer of security to keep other people from logging into your account.	Edit
Code Generator	Use your Facebook app to get security codes when you need them.	Edit
App Passwords	Use special passwords to log into your apps instead of using your Facebook password or Login Approvals codes.	Edit
Trusted Contacts	Pick friends you can call to help you get back into your account if you get locked out.	Edit
Your Browsers and Apps	Review which browsers you saved as ones you often use.	Edit
Where You're Logged In	Review and manage where you're currently logged into Facebook.	Edit
Legacy Contact	Choose a family member or close friend to care for your account if something happens to you.	Edit
Deactivate Your Account	Choose whether you want to keep your account active or deactivate it.	Edit

So, I've decided to give you a few discrete pointers.

Make sure you check your settings if you don't want me to track you!

The settings you choose are all optional and may be subject to specific operational guidance or best practice standards within your organisation. Check before making changes.

Security: Login alerts

Security Settings

Login Alerts

Get an alert when anyone logs into your account from a new device or browser.

Notifications

- (•) Get notifications
- ( ) Don't get notifications

Email

- (•) Email login alerts to (your email address will appear here)
- ( ) Don't get email alerts

Text messages

- (•) Text login alerts to (your mobile number will appear here, if assigned)
- ( ) Don't get text alerts

Save Changes | Cancel

Get notified if someone else logs into your account from a new device or browser.

Security: Login approvals

Login Approvals

☐ Require a security code to access my account from unknown browsers [?]

Save Changes | Cancel

You have the option to use mobile number linked to your profile to approve logins from browsers or devices that have not been used before. This is a second layer of security.

Note that some browser settings (e.g. Cookie settings or private browser mode) may prevent you from activating this feature.

Security: where you're logged in

Where You're Logged In

Current Session End All Activity

Location Unknown

Device Type Firefox on Windows 7

If you notice any unfamiliar devices or locations, click 'End Activity' to end the session.

Desktop (1)

Last Accessed **August 7 at 10:43am** End Activity

Location Amsterdam, Netherlands (Approximate)

Device Type Firefox on Windows 8

Facebook for iPhone (1)

Messenger (2)

Facebook for iPad (1)

Close

1

Review all sessions that Facebook regards as active.

2

Click to end any active sessions

3

Check your active mobile device and Messenger sessions as well.

These are normally just sessions I didn't fully log out of, but if I do see a suspicious session, I investigate it (if possible) end it, and then change my password right away.

Security: Your browsers & apps

Your Browsers and Apps

You won't get notified or have to confirm your identity when logging in from these devices:

Facebook for iPhone	April 12, 2015 · Remove
Facebook for iPhone	November 29, 2014 · Remove
Firefox on Windows	March 20, 2014 · Remove

Save Changes | Cancel

This is a list of the browsers & apps Facebook trusts for your account. Remove any that you DO want to receive Login Alerts for. No alerts will be raised for browsers or apps remaining on this list.

Security: deactivate your account

Deactivate Your Account

Deactivating your account will disable your profile and remove your name and photo from most things you've shared on Facebook. Some information may still be visible to others, such as your name in their friends list and messages you sent. Learn more.

Deactivate your account.

Close

*Click to **temporarily** deactivate your account if you need to do so.*

Never leave an unwanted and unused account lying dormant. If it is hacked and misused, you might not notice the fact. Such misuse could continue for years in some cases. ***To permanently delete an account visit*** https://www.facebook.com/help/delete_account

Privacy

1 *Make sure only your friends can see what you have posted.*

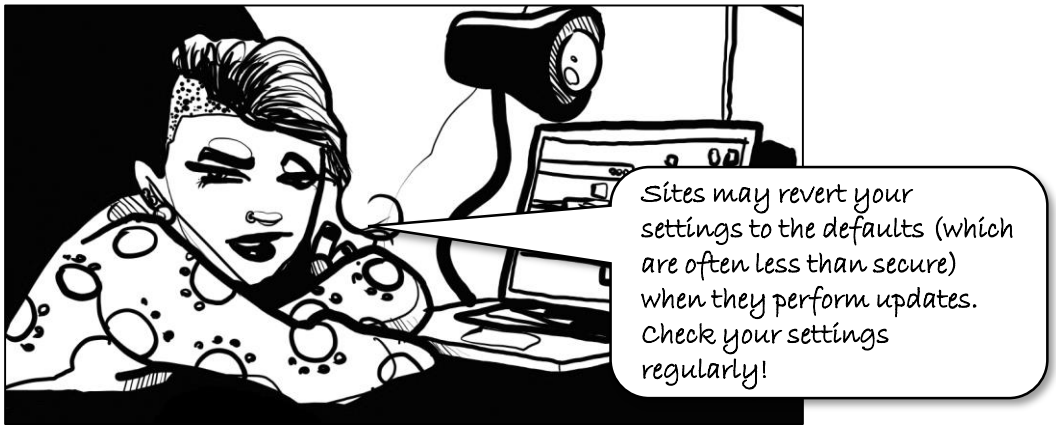
Privacy Settings and Tools

Who can see my stuff?	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
Who can contact me?	Who can send you friend requests?	Friends of Friends	Edit
Who can look me up?	Who can look you up using the email address you provided?	Friends	Edit
	Who can look you up using the phone number you provided?	Friends	Edit
	Do you want search engines outside of Facebook to link to your profile?	No	Edit

2 *Limit who can contact you.*

3 *Limit who can search for you and how.*

Timeline | About | **Friends** 456 | Photos | More ▾



Timeline & Tagging

1 *Make sure that only you can add posts. Approve posts friends tag you in.*

Timeline and Tagging Settings

Who can add things to my timeline?	Who can post on your timeline?	Only Me	Edit
	Review posts friends tag you in before they appear on your timeline?	On	Edit
Who can see things on my timeline?	Review what other people see on your timeline		View As
	Who can see posts you've been tagged in on your timeline?	Only Me	Edit
	Who can see what others post on your timeline?	Only Me	Edit
How can I manage tags people add and tagging suggestions?	Review tags people add to your own posts before the tags appear on Facebook?	On	Edit
	When you're tagged in a post, who do you want to add to the audience if they aren't already in it?	Only Me	Edit

2 *Limit who can see your timeline.*

3 *Review and manage tags posted by others that mention you.*

Timeline	About	Friends 456	Photos	More ▾

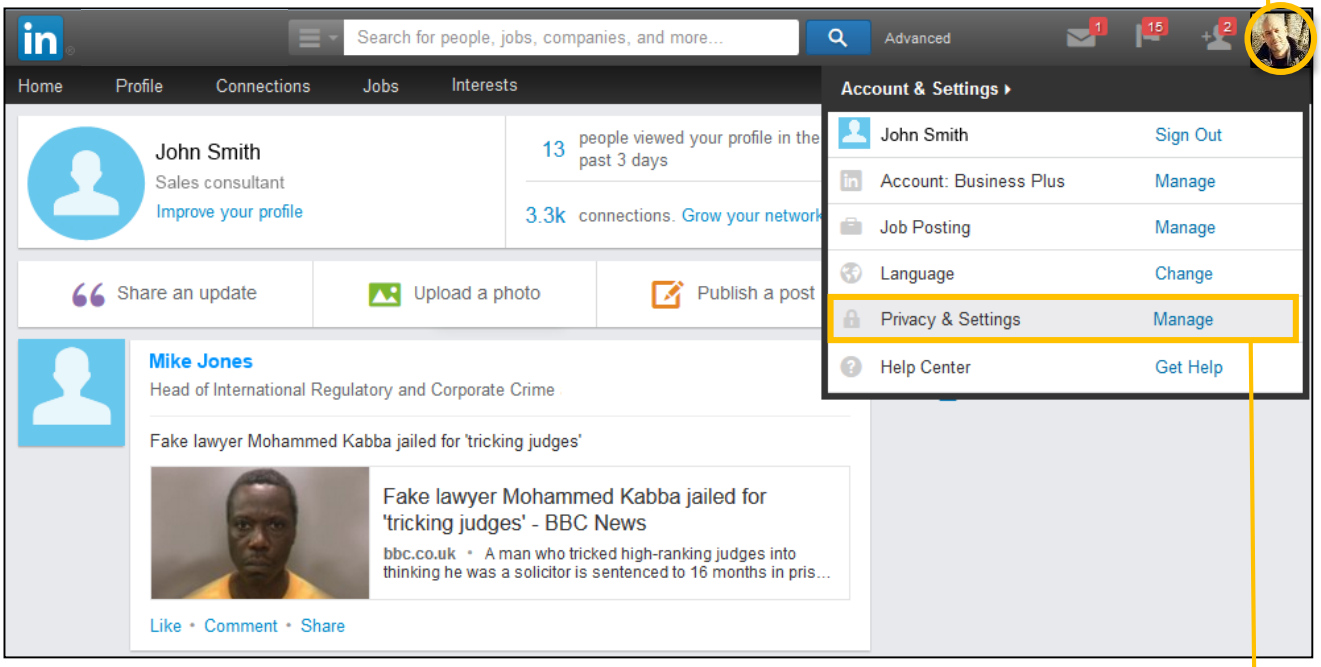
Social Media settings and options change all the time. Please check with the issuer (DCGFutures@met.police.uk) for the latest version of this guide.

Secure LinkedIn

Note: all screenshots taken from the LinkedIn.com site. Mobile apps will have differing features.

Privacy & settings

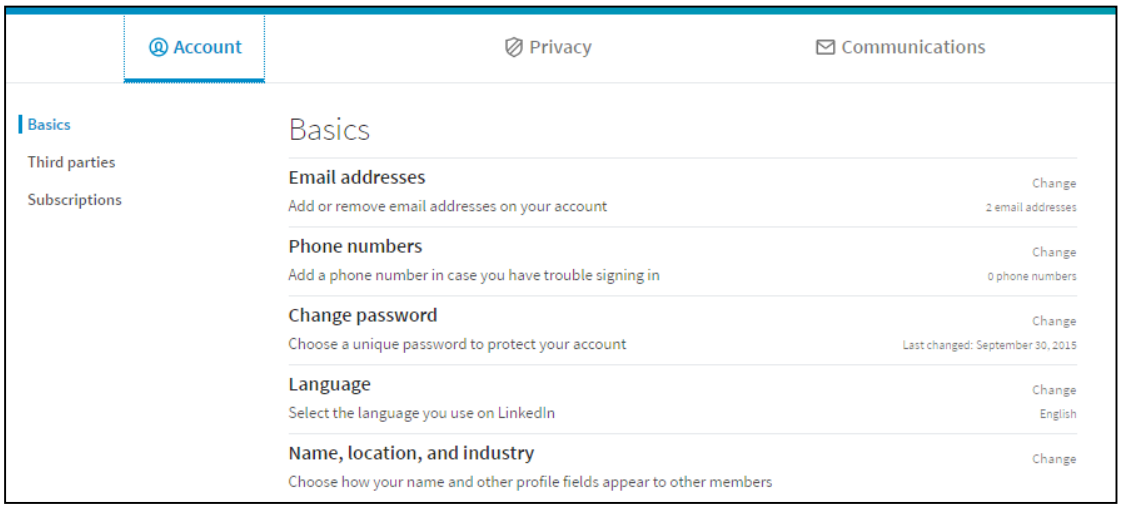
1 *First hover your mouse **here**…*



2 *…then click here…*

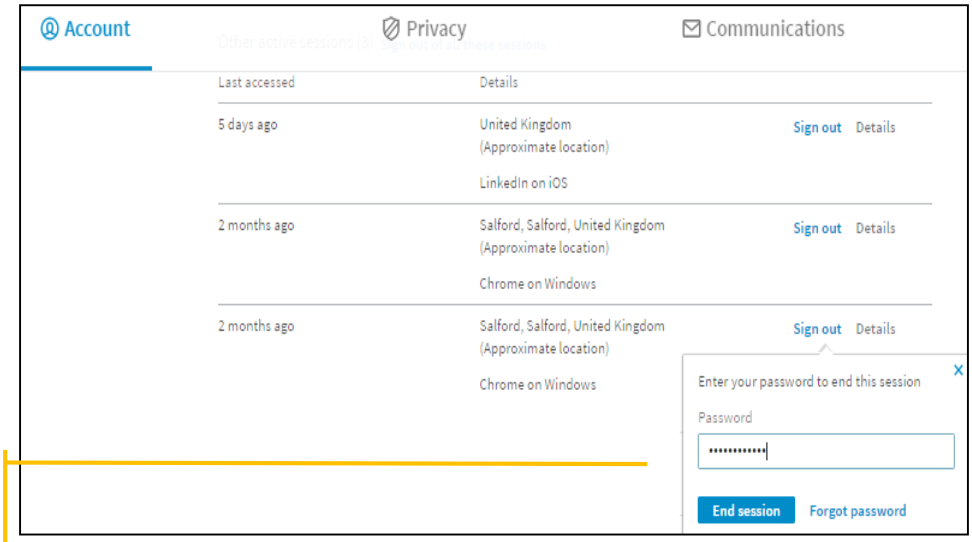
Security: Access & edit

1. *Set a strong password & change it regularly*
2. *Edit your email address - no work email*
3. *Avoid using a phone number*



Security: Active sessions

1. *Review all sessions that LinkedIn regards as current.*
2. *Click to end any active sessions*



Security: Profile photo & visibility

Account | Privacy | Communications

Basics
Third parties
Subscriptions

Showing profile photos
Choose whether to show or hide profile photos of other members
Select whose photos you would like to see.
Your connections

Close
Connections

Restrict who can see your photo by selecting 'Your connections'

Security: Archive of your data

Getting an archive of your data
Download an archive of your account data, posts, connections, and more
Change

Request your data archive

Download your LinkedIn data

Did you know you can request an archive of your activity and data on LinkedIn anytime?

Within minutes, you'll get the archived information that's fastest to compile including things like your messages, connections and imported contacts. We'll send you an email with a link where you can download it right away.

You'll get an email with a link where you can download the second part of your data archive in about 24 hours. You'll also be able to access your archive by going to your settings, selecting the Account tab, and clicking **Request an archive of your data**. Want more details? Just visit our Help Center.

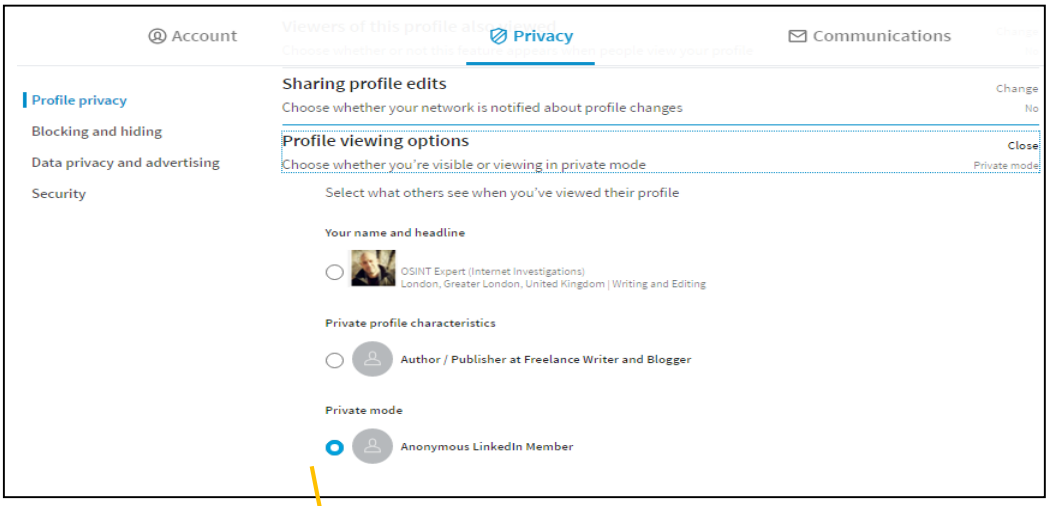
Here's what's included

Your data archive will contain the information LinkedIn has stored for you including your activity and account history, from who invited you to join, to the time of your latest login. For the full list, visit our Help Center.

Request archive

Backup your data regularly, using the archive feature.

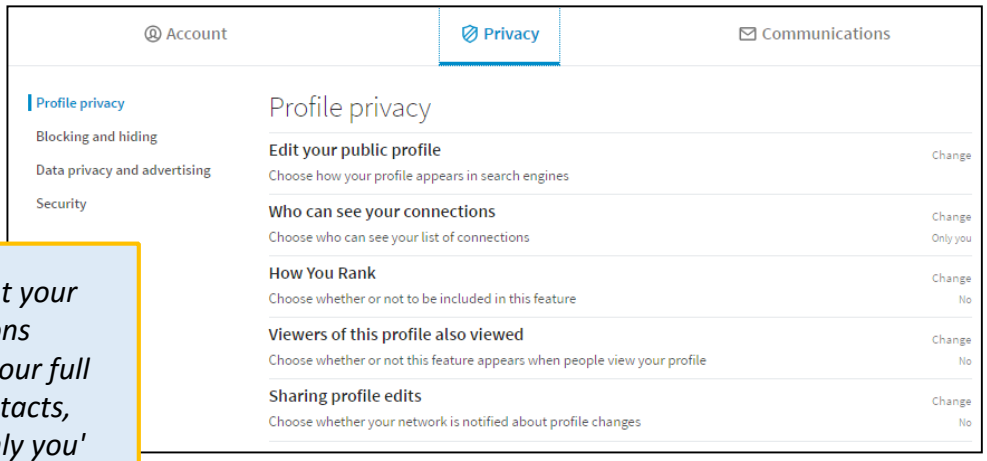
Security: Profile viewing options



Select the 3rd option to be totally anonymous, then click 'Save changes'

***Note**: if you do select this option, you will not see the details of anyone who views your profile…*

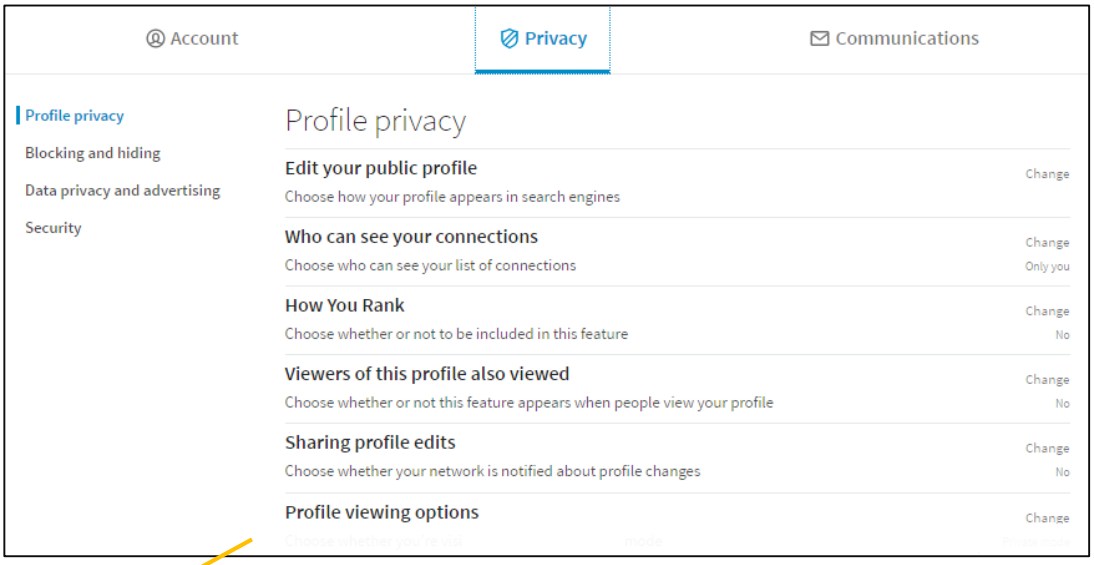
Security: Sharing profile edits



1. *To prevent your connections viewing your full list of contacts, select 'Only you'*

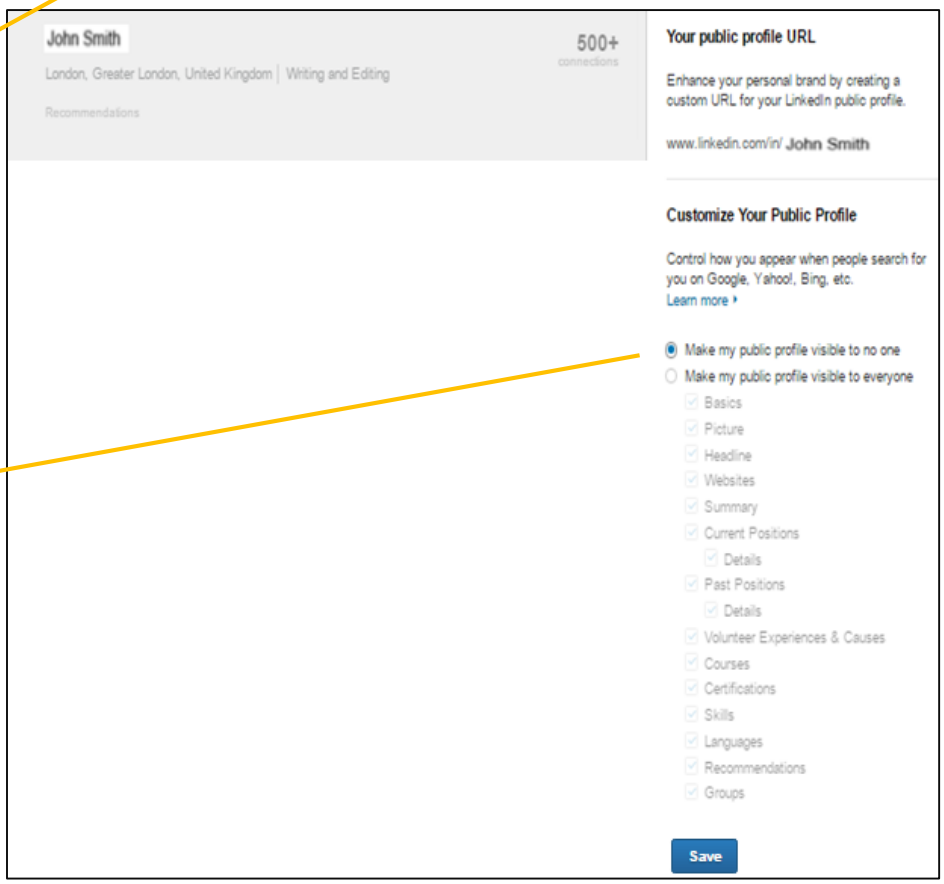
2. *Based on your role choose either 'Yes' or 'No' to Sharing your profile edits.*

Security: Hiding your public profile



1

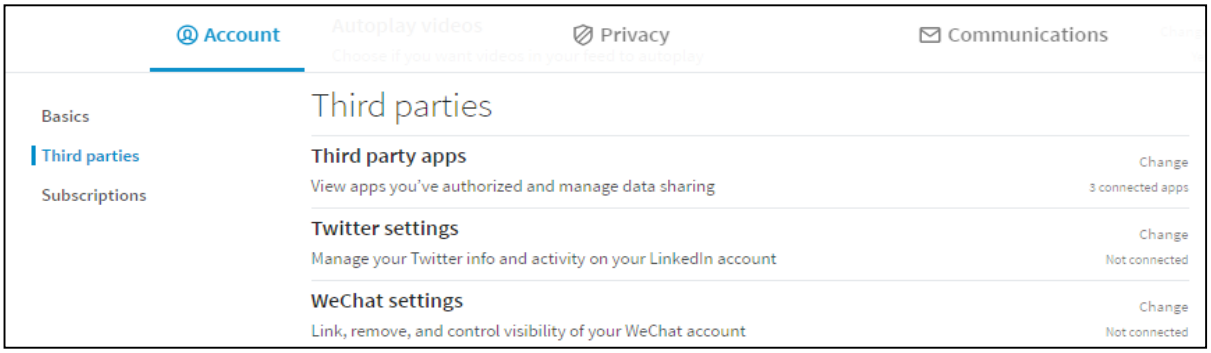
*Return to **Privacy** and choose the **Profile Privacy** tab. Then click **Profile viewing options.***



2

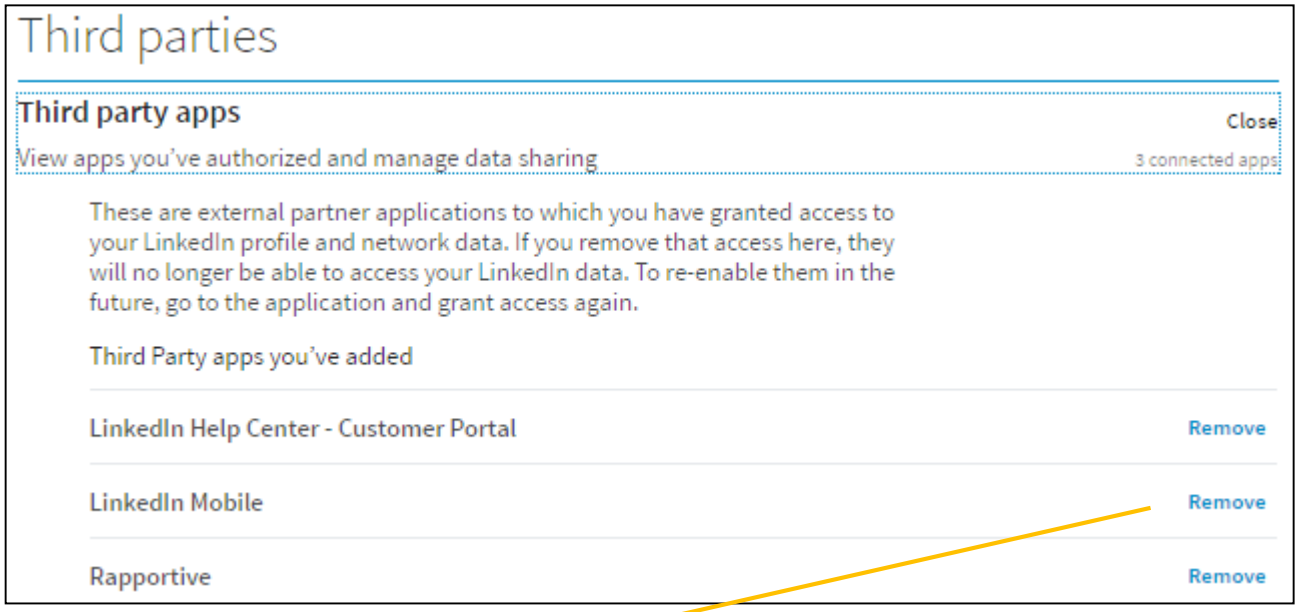
Hide the access to your profile by selecting 'Make my public profile visible to no one'

Security: View your applications



1 *In 'Account' 'Third Party' section, you can view the apps you have authorised.*

2 *You will see a list of the **external** apps that currently have permission to access your LinkedIn account. These apps can see your feed, your connections and your contact details.*



3 *Select those apps you did not authorize or wish to block and then click 'Remove'.*

Security: Data sharing with 3rd party apps

Data privacy and advertising

Suggesting you as a connection based on your email address Choose who can see you as a suggested connection if they have your email address	Change Nobody
Suggesting you as a connection based on your phone number Choose who can see you as a suggested connection if they have your phone number	Change Nobody
Representing your organization Choose if we can show your profile information on your employer's pages	Change No
Sharing data with third parties Choose if we can share your basic profile data with third parties	Change No
Advertising preferences Choose whether LinkedIn can use cookies to personalize ads	Change No

Apply your settings as shown in the above image.

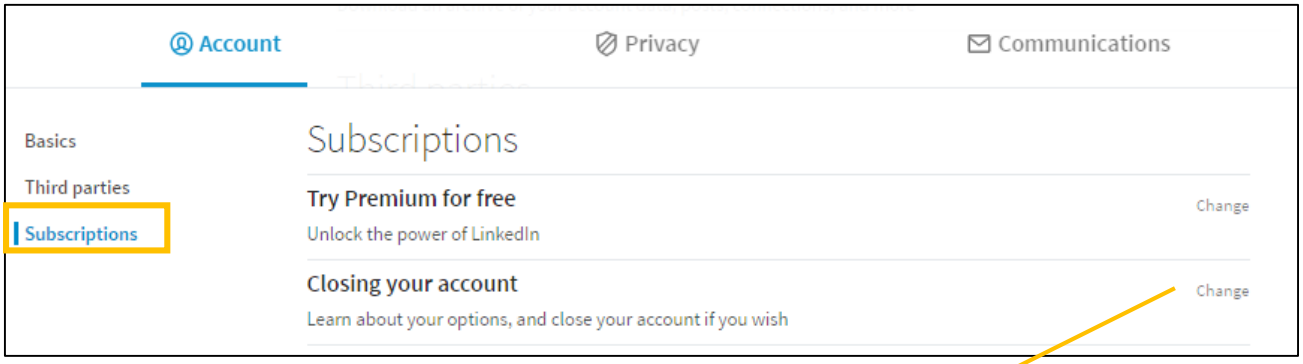
Choose the 'No' option for data sharing, advertising and representing your organisation.

Select 'Nobody' to suggest you as a connection based on your personal details.

DO NOT DATA SHARE

Remember, Social Media settings and options change all the time. Please check with the issuer (DCGFutures@met.police.uk) for the latest version of this guide.

Security: Closing your account



*Always close your account **when it is no longer needed**. This prevents it from being hacked and misused.*

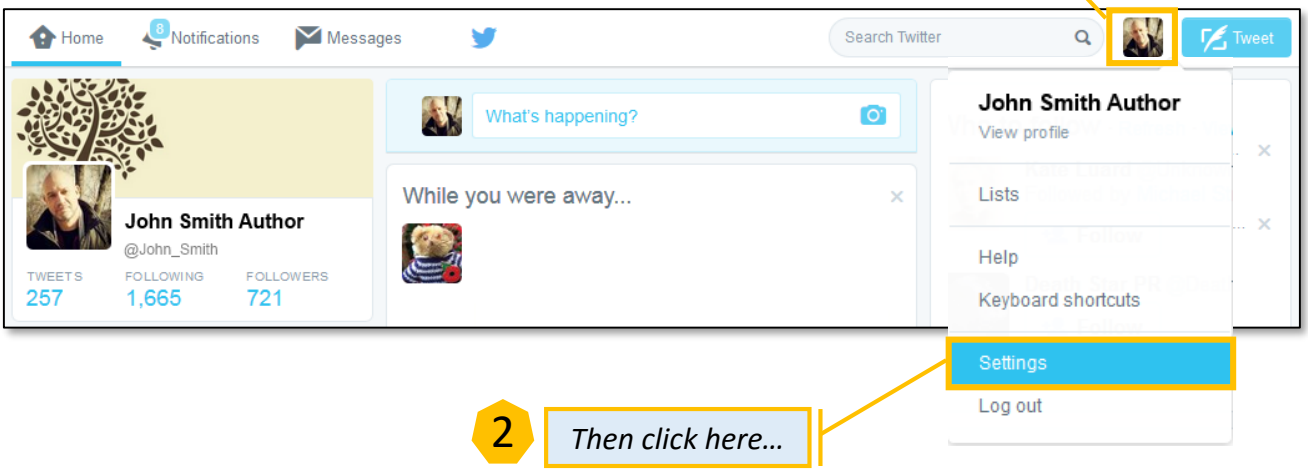
ONLY WHEN NO LONGER NEEDED

Secure Twitter

Note: all screenshots taken from the Twitter.com site. Twitter mobile apps will have differing features

To access Settings

1 *First click here…*



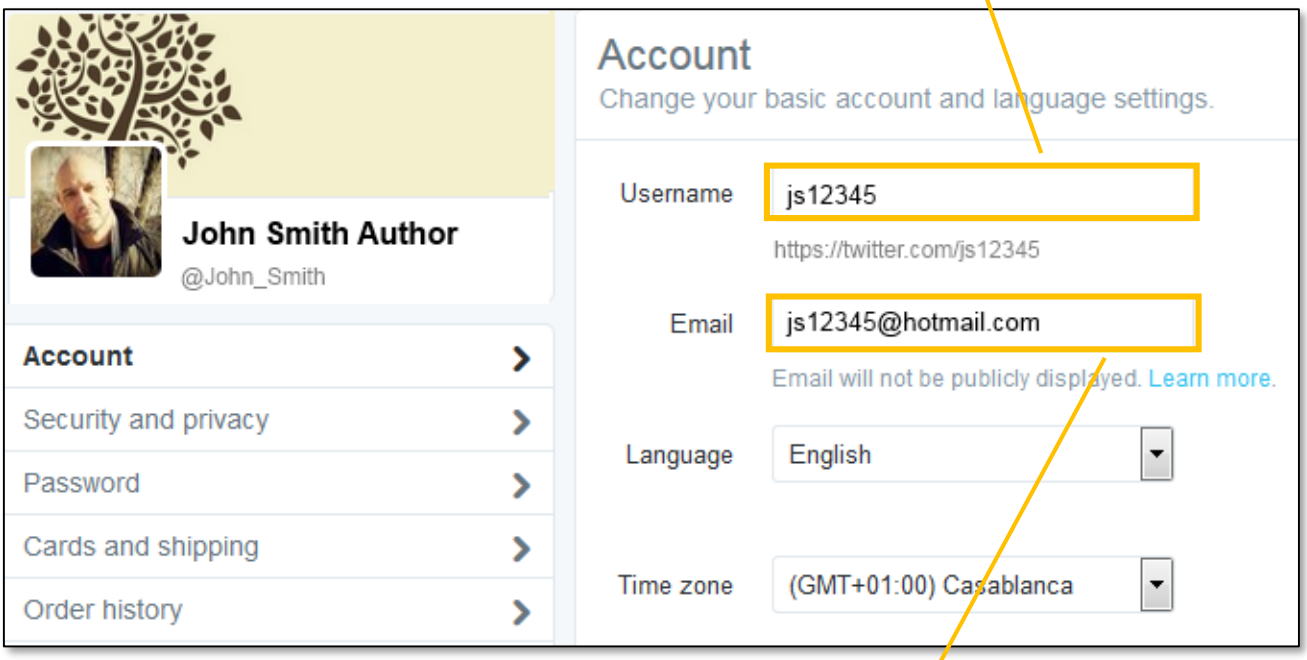
2 *Then click here…*

That woman tweeted my whole life's story to the whole world!

Unless you restrict your posts, Twitter is a broadcast medium; once you Tweet it you've set it free for the whole wide world to see!

Account settings

1 *You can edit the user name visible to other users*

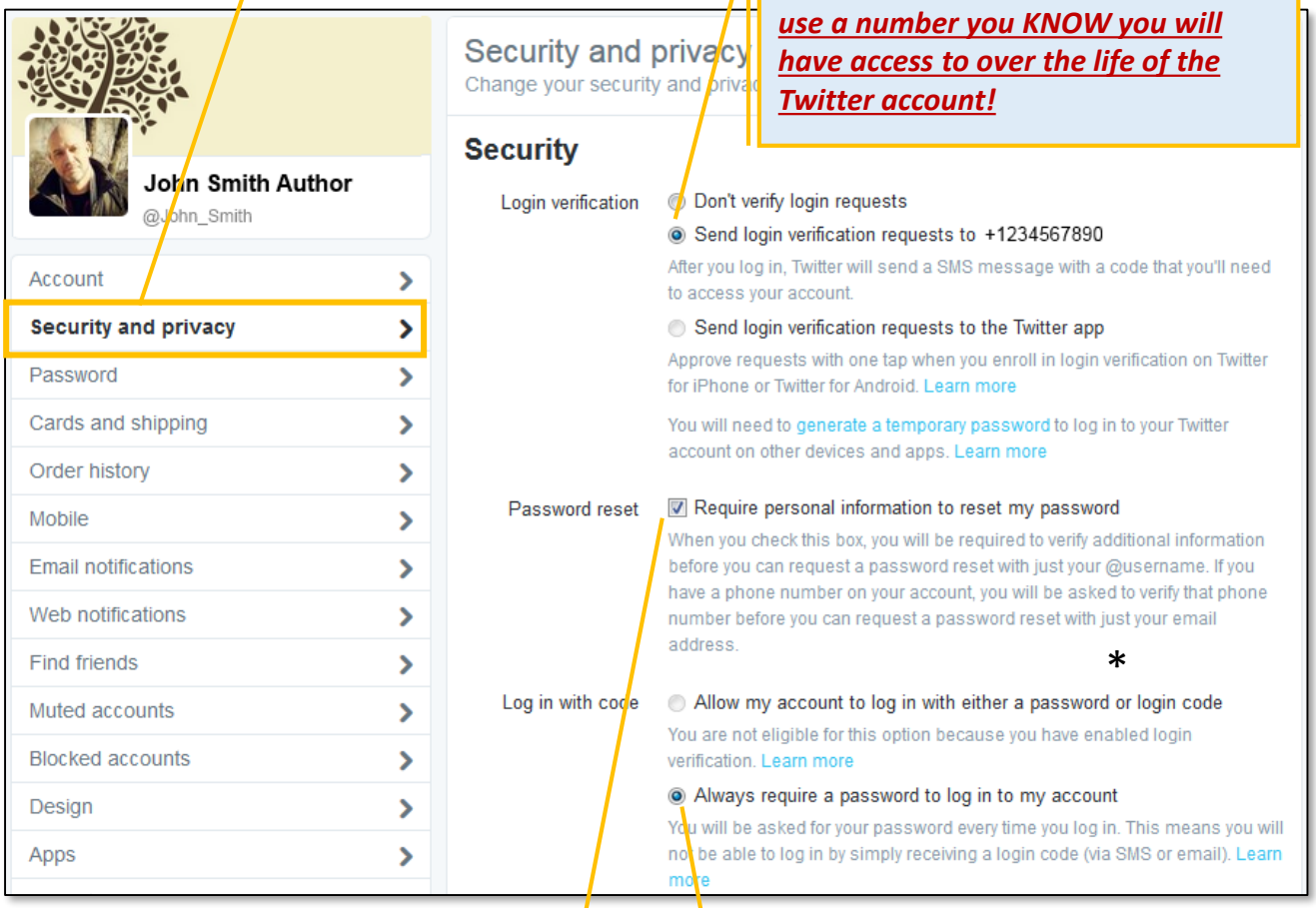


2 *Do not use a work email address. Edit as necessary.*

Security

1 *Next click here…*

2 ***Optionally**, you can use a mobile number to validate each login. **Only use a number you KNOW you will have access to over the life of the Twitter account!***



3 *Make sure that others cannot easily change your password and take over your account.*

4 *Enhance your login security by always requiring a password to login.*

** **Note**: using the Twitter App on a mobile device might expose you to being geo-located if your geo-location settings are left on, or turned back on by you or another person.*

Privacy

1

Apply the Privacy settings as shown…

Privacy

Photo tagging
- Allow anyone to tag me in photos
- Only allow people I follow to tag me in photos
- Do not allow anyone to tag me in photos

Tweet privacy
- Protect my Tweets

Optional

If selected, only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places. Learn more.

Off

Tweet location
- Add a location to my Tweets

When you tweet with a location, Twitter stores that location. You can switch location on/off before each Tweet. Learn more

Click this

Delete all location information

This will delete all location information from past Tweets. This may take up to 30 minutes.

Off

Discoverability
- Let others find me by my email address
- Let others find me by my phone number

Address book

Manage your contacts

Review

Contacts you've uploaded to Twitter from your address book.

Personalization

The feature to tailor Twitter based on your recent website visits is not available to you.

Do Not Track ✔

While you have Do Not Track turned on, your visits to sites that feature Twitter are not available to personalize your experience.

Off

Promoted content
- Tailor ads based on information shared by ad partners.

This lets Twitter display ads about things you've already shown interest in. Learn more about how this works and your additional privacy controls.

Do Not Track ✔

While you have Do Not Track turned on, Twitter will not receive browser-related information from our ads partners for tailoring ads.

Twitter for teams
- Allow anyone to add me to their team
- Only allow people I follow to add me to their team
- Do not allow anyone to add me to their team

Organizations can invite anyone to Tweet from their account using the teams feature in TweetDeck. Learn more.

Off

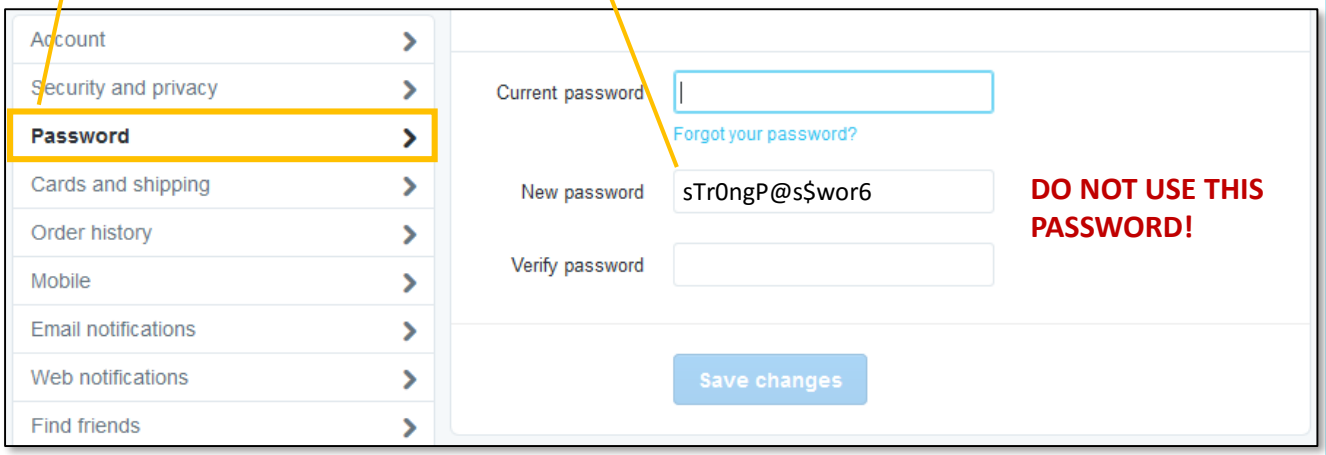
Direct Messages
- Receive Direct Messages from anyone

If selected, you will be able to receive messages from any Twitter user even if you do not follow them.

Password management

Now click here… 1

2 *Choose a strong password* & change it frequently.*



DO NOT USE THIS PASSWORD!

** A strong password contains **at least** 9 characters, includes no names, dates or common words, no repeating characters, and has a mix of lower case characters, upper case characters and numbers. Special characters (e.g. &,%,£,^,$,%, etc.) can sometimes be used as well.*

Notifications

- Account
- Security and privacy
- Password
- Cards and shipping
- Order history
- Mobile
- **Email notifications**
- Web notifications *

1 *Optional… not recommended.*

Email notifications

Control when and how often Twitter sends emails to you. Learn more.

Email is enabled. Turn off

Activity related to you and your Tweets

Email me when

- My Tweets are marked as favorites — Tailored for you
- Tweets I'm mentioned in are marked as favorites — Tailored for you
- My Tweets are retweeted — Tailored for you
- Tweets I'm mentioned in are retweeted — Tailored for you
- My Tweets get a reply or I'm mentioned in a Tweet — Tailored for you
- I'm followed by someone new
- I'm sent a direct message
- Someone emails a Tweet to me
- Someone from my address book joins Twitter

Activity related to your Retweets

Email me when

- My Retweets are marked as favorites — Tailored for you
- My Retweets are retweeted — Tailored for you

2

*You can opt to receive alerts about all retweets, mentions, follows, etc. (**recommended**).*

** The **Web notifications** page provides similar options, but with fewer choices.*

Blocked accounts

Blocked accounts

Account
Security and privacy
Blocked accounts
Design
Apps

1 *You can export a list of blocked accounts, or import a list of those you want to block.*

Accounts you're blocking

You've blocked these accounts. You will not see their Tweets in your timeline. Additionally, blocked accounts cannot follow you or view your profile while logged in to Twitter. Learn more about blocking.

All / Imported

Advanced options
Export your list
Import a list

Silly Man 1
@sillyman1

Silly Man 2
@sillyman2
Blocked
Unblock
Report

Silly Man 3
@sillyman3
Blocked

2 *You can also unblock a blocked account, or report it to Twitter.*

Manage your Apps

Apps

Design
Apps
Widgets
Your Twitter data

1 *Revoke the access of any unwanted or unknown Apps.*

Applications

These are the apps that can access your Twitter account. Learn more.

You will need to generate a temporary password to log in to your Twitter account on other devices and apps. Learn more.

Cloze by Cloze Inc.
Relationship Management, Inbox, and Contacts in One App
Permissions: read, write, and direct messages
Approved: Friday, December 13, 2013 at 3:59:57 AM

Undo Revoke Access

Report application

2 *If you believe that an App has obtained access without your consent, you can report it to Twitter…*

Twitter Data

Widgets >
Your Twitter data >

1

Check your Twitter history. If you spot anything that seriously concerns you, consider changing your password or even deleting your account.

2

You can download and backup your entire Tweet history for evidential purposes.

Your Twitter data

A snapshot of your account information.

Account history

Account creation	**Sep 18, 2011 at 6:58 AM**
Username	**@js12345** Edit
Email	**js12345@hotmail.com** Edit
Phone	**+123456789000** Edit Activation date: Aug 11, 2013 Country: United Kingdom Carrier: vodafone_uk

Device history

These are the devices you have used to access your Twitter account.

Phones	**Twitter for iPhone** Activated on May 19, 2015

Login history

If you see any suspicious activity from an app, go to the Apps tab to revoke its access. In some cases the IP location may differ from your physical location. Learn more

APP	DATE & TIME	IP LOCATION
Twitter.com	Aug 14, 2015 12:52 PM	81.156.37.108 United Kingdom
Twitter for iPhone	Aug 11, 2015 7:56 PM	81.156.37.108 United Kingdom
Twitter.com	Aug 6, 2015 1:44 PM	217.195.248.66 Netherlands

Other data

Contacts	Manage the contacts imported from your address book.
Twitter Archive	Download your entire Tweet history.
Connected apps	Review the apps that you have given access to your Twitter account.
Muted accounts	Review the accounts you've muted.
Blocked accounts	Review the accounts you've blocked.

Deactivation

- Account
- Security and privacy
- Password
- Cards and shipping
- Order history
- Mobile
- **Email notifications**
- Web notifications

Account

Change your basic account and language settings.

Username: MarkJ_Books
https://twitter.com/MarkJ_Books

Email: mark.johnson@trmg.biz
Email will not be publicly displayed. Learn more.

Language: English
Interested in helping translate Twitter? Check out the Translation Center.

Time zone: (GMT+01:00) Casablanca

Content

Country: United Kingdom
Select your country. This setting is saved to this browser.

Tweet media
☐ Do not inform me before showing media that may be sensitive
You will see all photos or videos even if they contain sensitive media.
☐ Mark media I tweet as containing material that may be sensitive
Please check this box if your Tweets contain sensitive media so that users can be informed prior to viewing.

Video Tweets
☑ Video autoplay
Videos will automatically play across the Twitter website.

Your Twitter archive: Request your archive
You can request a file containing your information, starting with your first Tweet. A link will be emailed to you when the file is ready to be downloaded.

Save changes

Deactivate my account

DO NOT CLICK UNLESS SURE!

1

Click here and carefully read the text on the page that appears.

At the time of writing, deactivated accounts remain in suspense for 30 days before Twitter permanently deletes them.

Secure Google+

Note: all screenshots taken from the Google.com site. Mobile apps may have differing features.

Google+ 'Settings'

Google+ Search Google+

Settings

Settings

Who can interact with you and your posts

Who can send you notifications? Learn more

Who can comment on your public posts? Learn more

Your circles

Shared Endorsements Off Edit

Notification delivery

Email: mjohnson.trmg@gmail.com

Add email address

Phone: Add phone number

Manage subscriptions

Occasional updates about Google+ activity and friend suggestions

Occasional updates from people outside your circles

Receive notifications

Be notified by email or phone when someone...

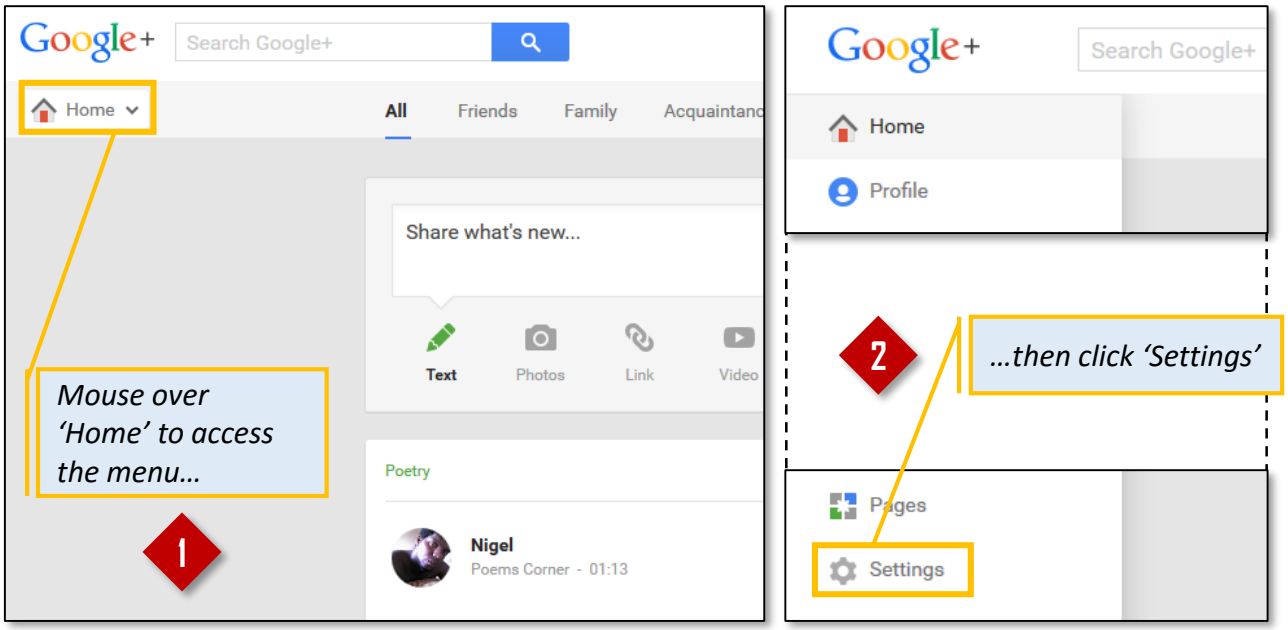
- **Posts**
- **Circles**
- **Photos**
- **Hangouts**
- **Events**
- **Communications about Google+ Pages**
- **Communities**
- **Polls**

***Note**: This guide only covers Google+. Gmail has its own settings area. Please see the separate Gmail guide for pointers on securing your Google email account.*

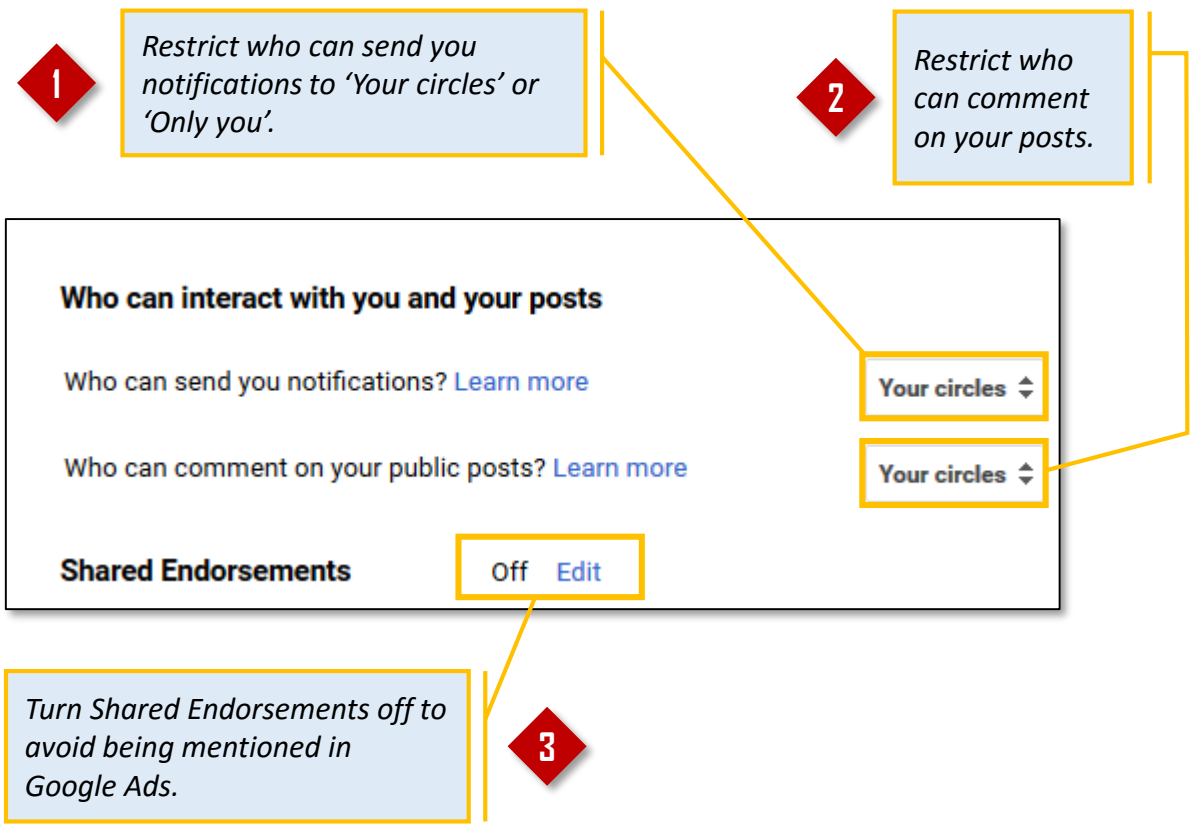
All Google+ settings are accessed via a single page which is quite lengthy.

Scroll down the page for more settings options…

To access 'Settings'



Posts and Endorsements



Notifications and Subscriptions

1

Toggle email notifications On or Off ('On' is recommended). Pick your email address with care.

2

***DO NOT** add a phone number unless essential.*

Notification delivery

Email: js123456@gmail.com

Add email address

Phone: Add phone number

Manage subscriptions

- [ ] Occasional updates about Google+ activity and friend suggestions
- [ ] Occasional updates from people outside your circles

3

Turn off subscriptions.

Receive notifications

Be notified by email or phone when someone...

- **Posts**
- **Circles**
- **Photos**

4

*Set your notification options to suit your preferences, but **DO** consider receiving photo tagging notifications, as these can be useful personal security warnings.*

	Email
Tags you in a photo	☑
Tags one of your photos	☑
Suggests a profile photo for you	☑
Comments on a photo that you're tagged in	☑

- **Hangouts**
- **Events**

Apps & activities

1

Click to manage your apps and your activities log.

Apps & activities

Manage your apps and Activity Log, including who can see your Google and third-party activities.

Manage apps & activities

This is the most secure scenario.

2

Apps Google Log

Manage apps

You've signed in to these apps with Google. You control who can see your signed-in apps and activities on Google services. Learn more

You have not connected with any apps using Google+ Sign-In. Learn more

3

This setting prevents others from identifying posts you have commented on.

Apps Google Log

Google+
+1s on posts activity

Extended circles edit

Who can see your "+1s on posts" activity?

Extended circles
Public
Your circles
Only you
Custom

iends find cool people and posts. People you select future Google+ activity. You can view your past ways, activity updates from private posts will only be ared with. Learn more

Cancel Save

Customise "Your circles"

Click here.

1

Your circles

When you share posts, photos, profile data and other things with "Your circles", you're sharing to all of your circles ones you're just following.

Customise

Accessibility

Change the pr

Photos and Vide

Show geo loca

Allow viewers

Don't feature r

Upload my ph

Storage used:

Buy more stor

Turning on full

Google Drive

Customise "Your circles"

When you share posts, photos, profile data and other things with "Your circles", you're sharing with all of your circles, except the ones you're just following (they're unchecked in this list). Learn more

Choose who to include in "Your circles":

- [ ] Friends
- [x] Family
- [ ] Acquaintances
- [ ] Following
- [ ] Book Reviewers
- [ ] Authors

Think carefully about how widely you want to share your posts, photos and profile data.

2

Cancel | Save

1

*Turn **OFF** automatic geolocation tagging and download permissions.*

2

*Turn **ON** to prevent Google from using your photos in ads.*

Photos and Videos

- [ ] Show geo location by default on newly shared albums. You can change the setting for each album. Learn more
- [ ] Allow viewers to download my photos and videos.
- [x] Don't feature my publicly shared Google+ photos as background images on Google products & services. Learn more
- [ ] Upload my photos at full size.

Profile

Profile

Show your Google+ communities posts on the Posts tab of your Google+ profile. Learn more.

Show these profile tabs to visitors (they're always visible to you): Learn more

- Photos
- YouTube / Videos
- +1
- Reviews

Allow people to send you a message from your profile — Only you

Help others discover my profile in search results. Learn more

Unticking this box prevents most search engines from indexing your profile. It does not prevent them from indexing any public posts or comments.

Show how many times your profile and content have been viewed.

*Consider turning all of these options off. Preventing search engine indexing should be set to **OFF**. Read the small print!*

Location Settings

Location Settings

Enable Location Sharing

Location Sharing allows you to share your current location with people you choose, from Location Reporting on your devices. People you share your location with can see your current location across Google products, including Google+ and Google Now. They can also see your places, such as home and work. Learn more

*Set Location Sharing to **OFF**.*

Disable Google

Disable Google+

Delete your entire Google profile here.

*Click to delete your Google+ profile. Note that **previously indexed search engine results will not be deleted**.*

Cyber Cops Episode One

The Case of the Facebook Friends

A CAR IS REPORTED ON FIRE IN A REMOTE LANE...
IT IS BURNING!
THE POLICE WILL TRACK THE OWNER...
THE CAR IS BADLY DAMAGED BUT THE NUMBER PLATE IS STILL LEGIBLE...
DIALLING 999!
THE FOLLOWING MORNING, 50 MILES AWAY, A PAIR OF WALKERS GET A TERRIBLE SHOCK!

THE BURNT OUT CAR BELONGS TO THE DECEASED; ONE PAUL SMITH...
PAUL SMITH
DS MIKE EVANS HAS A NEW MYSTERY ON HIS HANDS...
THE LOCATIONS ARE 50 MILES APART BUT A SHOT WAS REPORTEDLY HEARD IN THE WOODS AT THE SAME TIME THE CAR WAS SPOTTED ON FIRE.
BANG!
THE KILLER CAN'T HAVE ACTED ALONE. EVANS KNOWS HE NEEDS SOME EXPERT HELP.

DC ALISON KRAMER IS EVANS' TOP INVESTIGATOR.

FIRST, I WANT TO SEE THE CRIME SCENE.

KRAMER IS AN INTERNET AND COMMUNICATIONS SPECIALIST, BUT SHE KNOWS THE IMPORTANCE OF PHYSICAL EVIDENCE TOO.

WE'RE DEFINITELY LOOKING FOR TWO PEOPLE...

LOOK AT THIS!

KRAMER IS THE FIRST DETECTIVE ON THE SCENE.

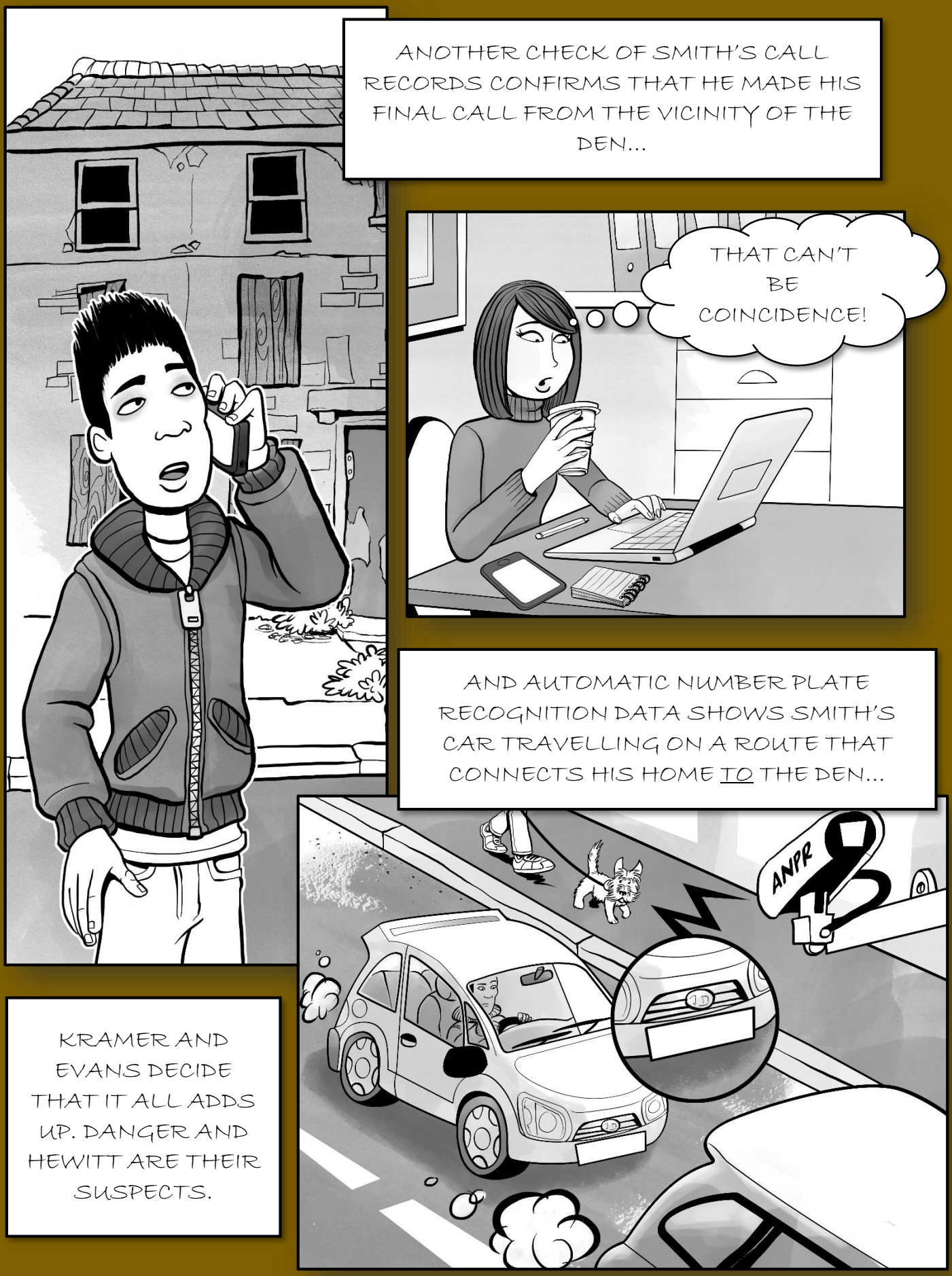
IF THE DEVICE BELONGED TO EITHER THE VICTIM OR HIS KILLER, IT COULD HOLD CRUCIAL DATA.

IT TURNS OUT THAT THE VICTIM, PAUL SMITH, MADE SEVERAL CALLS ON THE DAY HE DIED; ALL TO A KNOWN DRUG DEALER NAMED TERRY DANGER...

MR. DANGER HAS A VIOLENT RECORD...

THE POLICE CAN'T SEE WHAT WAS SAID ON THE CALLS, BUT JUST FINDING THE CONNECTION BETWEEN THE TWO MEN IS A VERY IMPORTANT LEAD.

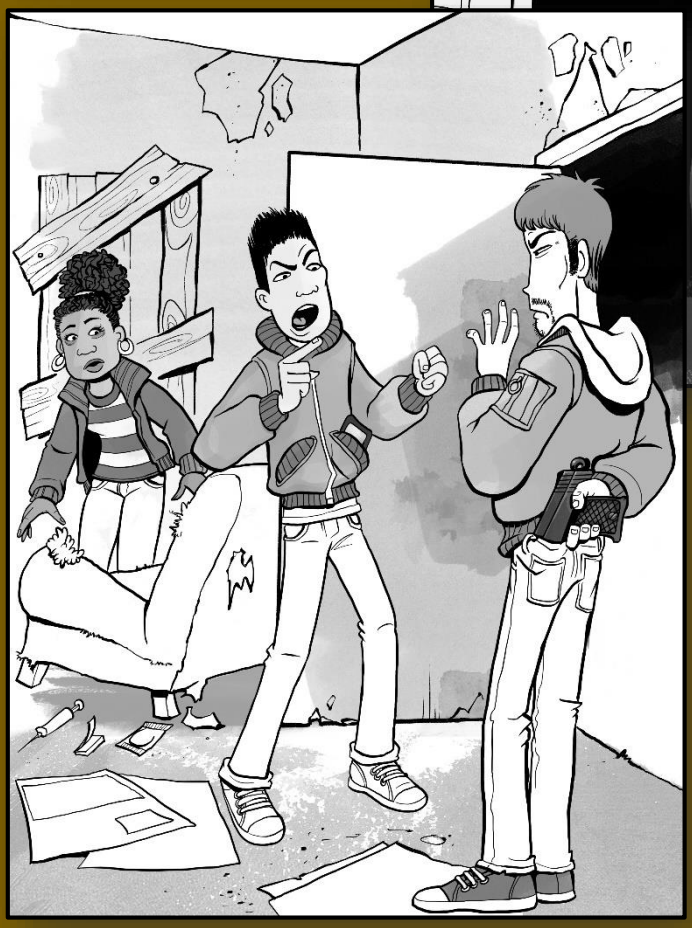
DANGER AND SMITH ALSO HAVE ANOTHER FACEBOOK FRIEND IN COMMON; ONE AMELIA HEWITT.
DID SMITH VISIT HER?
WE KNOW HEWITT RUNS TERRY DANGER'S DRUGS DEN...
A WITNESS REPORTED A DISTURBANCE AT THE ADDRESS ON THE NIGHT OF THE MURDER.


ANOTHER CHECK OF SMITH'S CALL RECORDS CONFIRMS THAT HE MADE HIS FINAL CALL FROM THE VICINITY OF THE DEN...
THAT CAN'T BE COINCIDENCE!
AND AUTOMATIC NUMBER PLATE RECOGNITION DATA SHOWS SMITH'S CAR TRAVELLING ON A ROUTE THAT CONNECTS HIS HOME TO THE DEN...
ANPR
KRAMER AND EVANS DECIDE THAT IT ALL ADDS UP. DANGER AND HEWITT ARE THEIR SUSPECTS.

ARMED POLICE SWOOP ON THE DEN.

DANGER AND HEWITT ARE BOTH PRESENT AND ARE TAKEN IN.

DANGER IS SILENT, BUT HEWITT HAS A LOT TO SAY!



HEWITT DESCRIBES HOW SMITH CAME TO THE DEN. HE THREATENED TO REPORT DANGER TO THE COPS IF THE DEALER DIDN'T HAND OVER DRUGS SMITH HAD PAID FOR.

SMITH WAS FORCED INTO THE BOOT OF DANGER'S CAR...

MEANWHILE, HEWITT DROVE SMITH'S CAR AWAY AND SET FIRE TO IT.

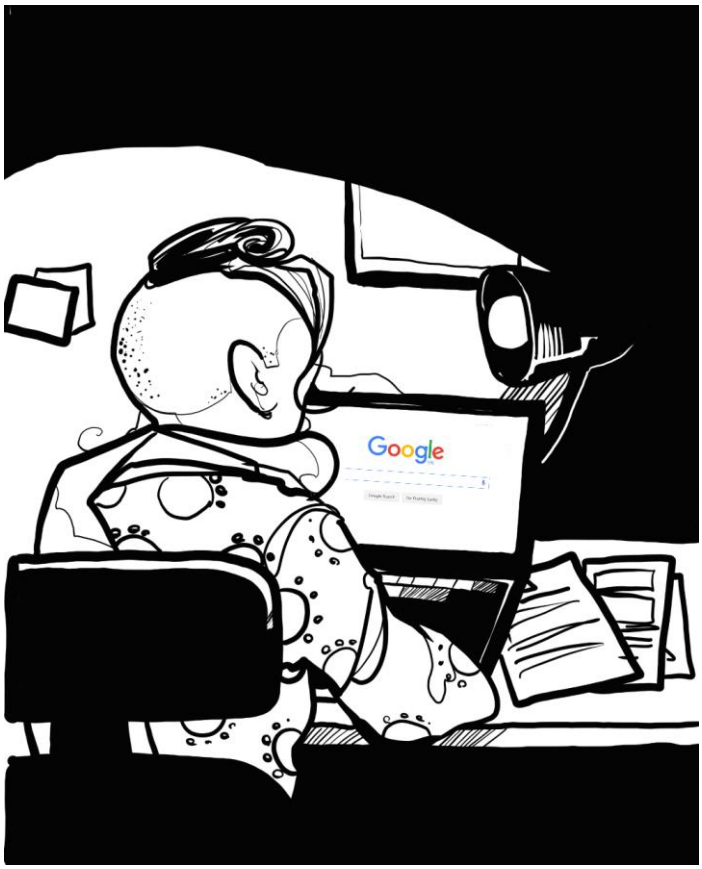
WHEN DANGER RANG HEWITT TO CHECK UP ON HER, HE TOLD HER THAT HE HAD 'SORTED BOYO PERMANENTLY'.

THE EVIDENCE IS BULLET PROOF. DANGER IS CONVICTED AND SENTENCED TO LIFE.

COMMUNICATIONS DATA ANALYSIS, OPEN SOURCE (ONLINE) INTELLIGENCE, AND DEVICE FORENSICS ARE ALL KEY ELEMENTS OF EFFECTIVE MODERN POLICING.

Secure Browsers

HACKER GIRL IS ALWAYS WORRIED THAT SOMEONE COULD ACCESS HER LAPTOP OR MONITOR HER ONLINE AND SEE WHAT SHE'S BEEN UP TO. SHE PROTECTS HERSELF, IN PART, BY USING PRIVATE BROWSING FEATURES AND TRYING TO LIMIT WHAT SITES RECORD ABOUT HER ACTIVITIES AND LOCATION.

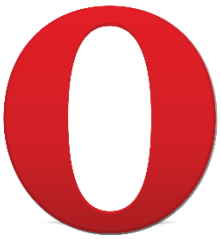


If you use the default browser settings on most browsers, all of your browsing activities may be logged on your device.

This means that anyone who gains access to your device, including a hacker operating remotely, can see what you've been looking at. If this is case data, it might be very sensitive, but personal data is also of great value to criminals.

Adjusting your browser settings is not a catch-all solution; internet service providers and visited sites will also capture and store the details of your activities, but at least you will have reduced your risks and ensured that a simple error, such as failing to log-off, or leaving your laptop on the train, is less likely to cause major grief. Other controls, including encryption of data and secure login procedures, are equally important and effective; it's all about using a combination of techniques.

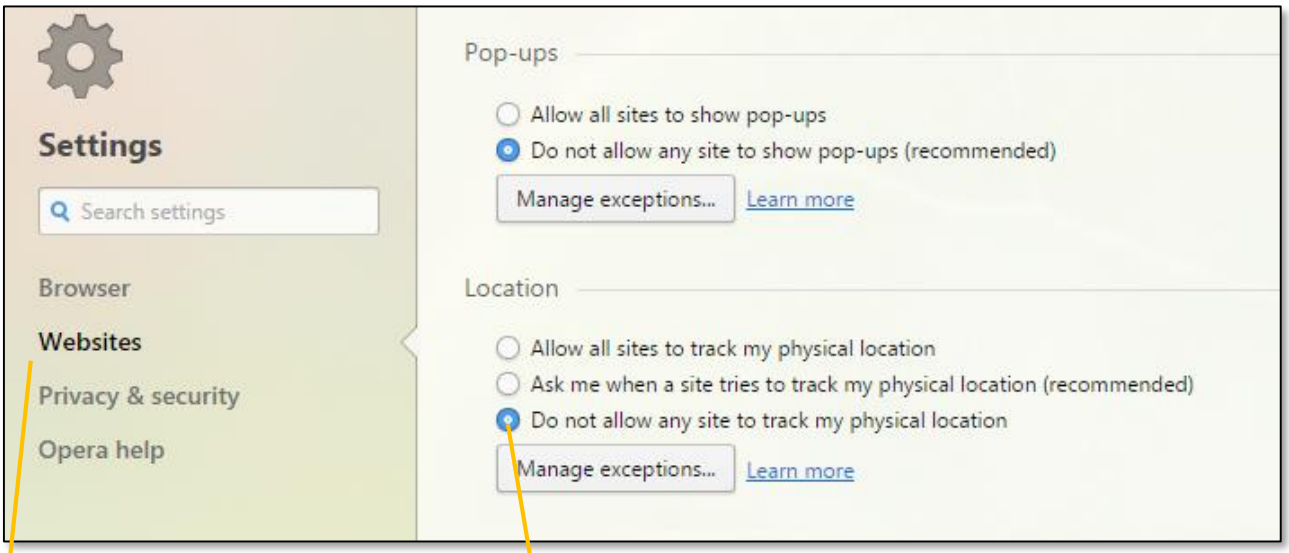
Secure Opera



Note: all screenshots taken from the .com site. Mobile versions may have differing features.

Accessing Settings

Location tracking



Select 'Websites'… 1

Set to 'Do not allow' location tracking 2

Privacy & security

Select 'Privacy & security'... 1

Click Clear browsing data... 2

Settings

Search settings

Browser

Websites

Privacy & security

Opera help

Privacy

Clear browsing data... Learn more

Opera may use web services to improve your browsing experience. You may optionally disable these services.

- [ ] Use a prediction service to help complete searches and URLs typed in the address bar
- [ ] Predict network actions to improve page load performance
- [ ] Help improve Opera by sending feature usage information
- [ ] Automatically send crash reports to Opera
- [x] Send a 'Do Not Track' request with your browsing traffic

Want even more privacy?
Enhance your online experience and enjoy superior privacy, security, and freedom, even on public Wi-Fi. Learn more about SurfEasy VPN.
SurfEasy is an Opera Software company.

Autofill

- [ ] Enable auto-filling of forms on webpages

Manage Autofill settings

Passwords

Clear browsing data

Obliterate the following items from: the beginning of time

- [x] Browsing history
- [x] Download history
- [x] Delete cookies and other site data
- [x] Empty the cache
- [x] Saved passwords
- [x] Clear saved Autofill form data

Saved content settings and search engines will not be cleared and may reflect your browsing habits.

Learn more Clear browsing data Cancel

Decide what you want to clear and then click Clear browsing data 3

Privacy & security

Settings

Search settings

Browser

Websites

Privacy & security

Opera help

Privacy

Clear browsing data... Learn more

Opera may use web services to improve your browsing experience. You may optionally disable these services.

- [ ] Use a prediction service to help complete searches and URLs typed in the address bar
- [ ] Predict network actions to improve page load performance
- [ ] Help improve Opera by sending feature usage information
- [ ] Automatically send crash reports to Opera
- [x] Send a 'Do Not Track' request with your browsing traffic

Want even more privacy?

Enhance your online experience and enjoy superior privacy, security, and freedom, even on public Wi-Fi. Learn more about SurfEasy VPN.

SurfEasy is an Opera Software company.

1

Autofill

- [ ] Enable auto-filling of forms on webpages

Manage Autofill settings

Passwords

- [ ] Offer to save passwords I enter on the web

Manage saved passwords

Deselect these options.

2

HTTPS/SSL

Manage certificates... Learn more

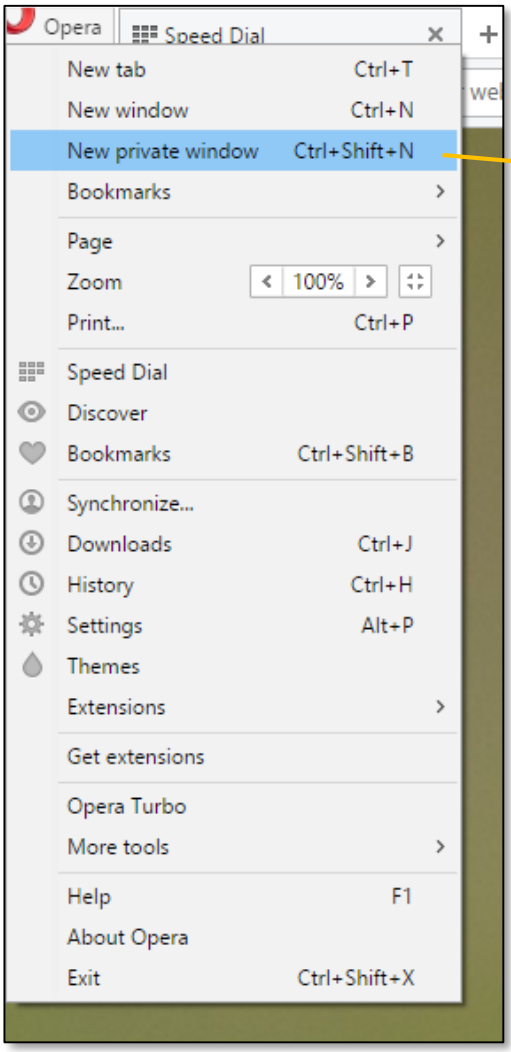
Cookies

- ( ) Allow local data to be set (recommended)
- (•) Keep local data only until I quit my browser
- ( ) Block sites from setting any data
- [ ] Block third-party cookies and site data

Manage exceptions... All cookies and site data... Learn more

Select this option.

Private browsing



Click here.

1

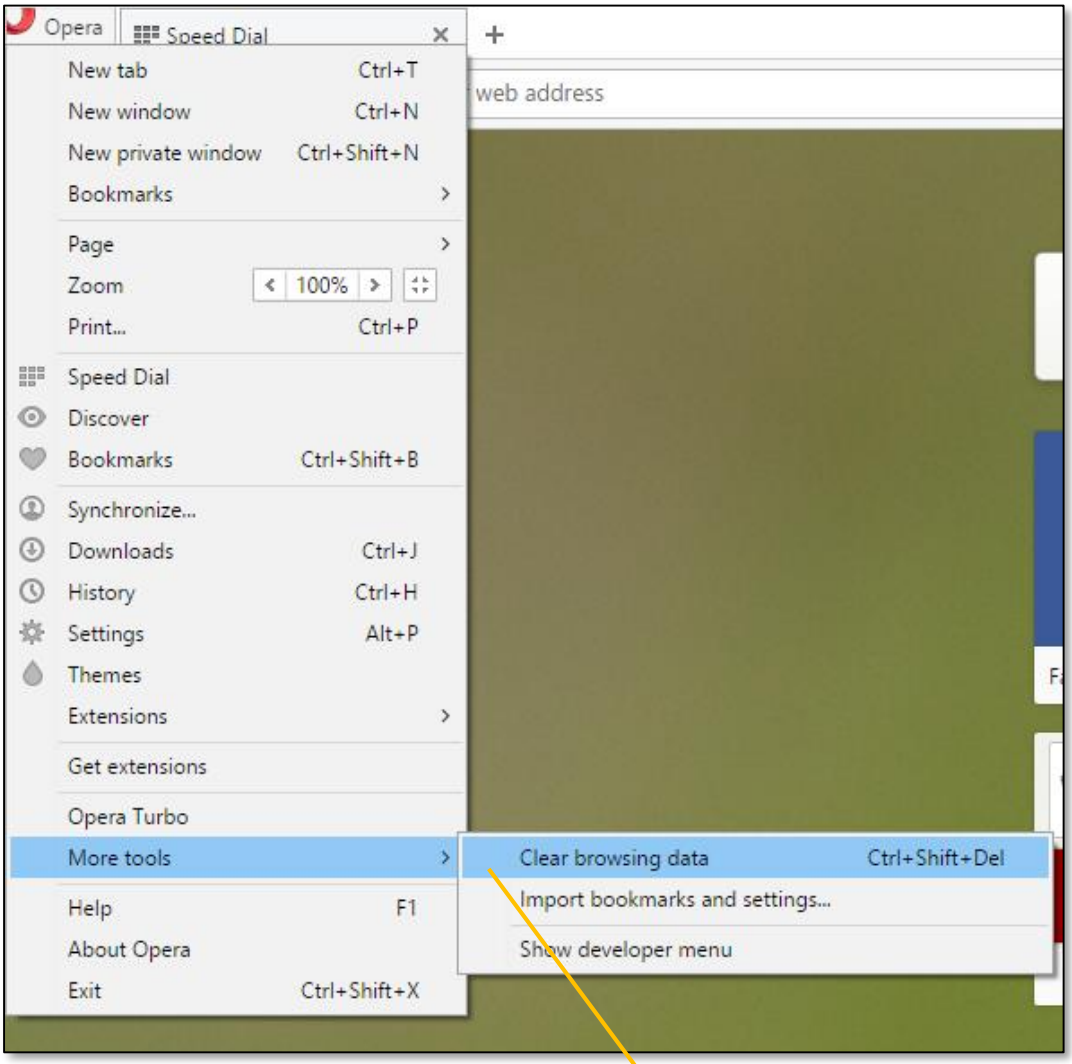
By using a private window, or tab, you can browse without leaving any trace of the websites you visit.

When you close an Opera private tab, the following data is deleted:

- browsing history
- items in cache
- cookies
- logins

A closed private tab or window cannot be recovered.

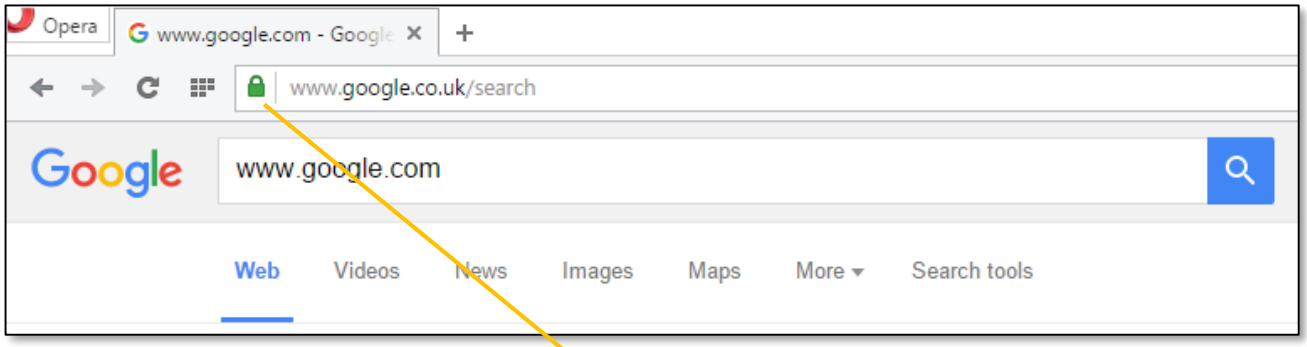
Clear browsing data shortcut



1

Access the menu as shown or press the Ctrl+Shift+Del keys to quickly clear your browsing history.

Site security badges



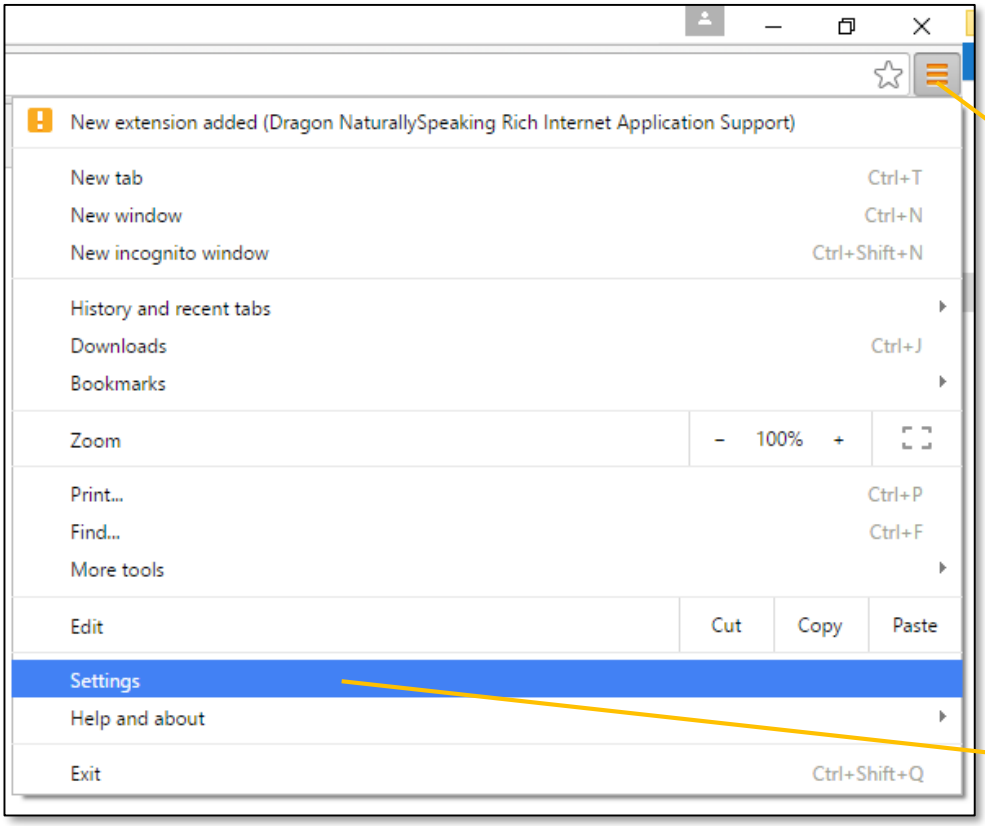
Site security badge. 1

Icon	Indicates...
	Accelerated connection
	Camera access
	Fraud or malware warning
	Local file
	Location access
	Opera page
	Secure connection
	Unprotected connection

Take careful note of the site security badges displayed for each website you visit.

Secure Chrome

Accessing the Menu



Click here to access the menu…

1

Then select 'Settings'

2

Accessing Advanced Settings

Settings

chrome://settings

Chrome

History

Extensions

Settings

About

Settings

Search settings

Sign in

Sign in to get your bookmarks, history, passwords and other settings on all your devices. You'll also automatically be signed in to your Google services. Learn more

Sign in to Chrome

On startup

Open the New Tab page

Continue where you left off

Open a specific page or set of pages. Set pages

Appearance

Get themes | Reset to default theme

Show Home button

Always show the bookmarks bar

Search

Set which search engine is used when searching from the omnibox.

Google | Manage search engines...

People

Person 1 (current)

Enable Guest browsing

Let anyone add a person to Chrome

Add person... | Edit... | Remove... | Import bookmarks and settings...

Default browser

Make Google Chrome the default browser

Google Chrome is not currently your default browser.

Show advanced settings...

1

Scroll down to the end of the page and then click 'Show advanced settings'

Privacy and saved passwords

Privacy

Content settings... | Clear browsing data...

Google Chrome may use web services to improve your browsing experience. You may optionally disable these services. Learn more

- [ ] Use a web service to help resolve navigation errors
- [ ] Use a prediction service to help complete searches and URLs typed in the address bar or the app launcher search box
- [x] Prefetch resources to load pages more quickly
- [ ] Automatically report details of possible security incidents to Google
- [x] Protect you and your device from dangerous sites
- [ ] Use a web service to help resolve spelling errors
- [ ] Automatically send usage statistics and crash reports to Google
- [x] Send a "Do Not Track" request with your browsing traffic

Passwords and forms

- [ ] Enable Autofill to fill out web forms in a single click. Manage Autofill settings
- [ ] Offer to save your web passwords. Manage passwords

Using the settings shown above does not guarantee security, but will help to reduce exposure. Note that websites can ignore 'Do Not Track' preferences.

1

Accessing Content Settings

Privacy

Content settings... | Clear browsing data...

Click to access Content settings

1

Google Chrome may use web services to improve your browsing experience. You may optionally disable these services. Learn more

- [ ] Use a web service to help resolve navigation errors
- [ ] Use a prediction service to help complete searches and URLs typed in the address bar or the app launcher search box
- [x] Prefetch resources to load pages more quickly
- [ ] Automatically report details of possible security incidents to Google
- [x] Protect you and your device from dangerous sites
- [ ] Use a web service to help resolve spelling errors
- [ ] Automatically send usage statistics and crash reports to Google
- [x] Send a "Do Not Track" request with your browsing traffic

Passwords and forms

- [ ] Enable Autofill to fill out web forms in a single click. Manage Autofill settings
- [ ] Offer to save your web passwords. Manage passwords

Content settings - Cookies

Content settings

Cookies

- Allow local data to be set (recommended)
- Keep local data only until you quit your browser
- Block sites from setting any data
- Block third-party cookies and site data

Manage exceptions... | All cookies and site data...

Images

- Show all images (recommended)
- Do not show any images

Manage exceptions...

JavaScript

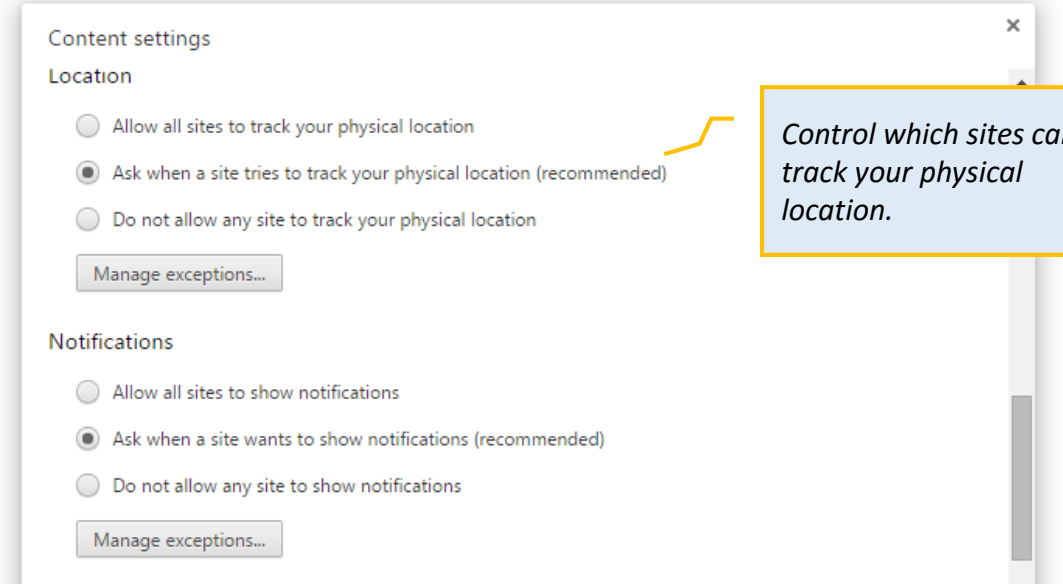
- Allow all sites to run JavaScript (recommended)
- Do not allow any site to run JavaScript

Set as shown to limit the data saved by cookies.

1

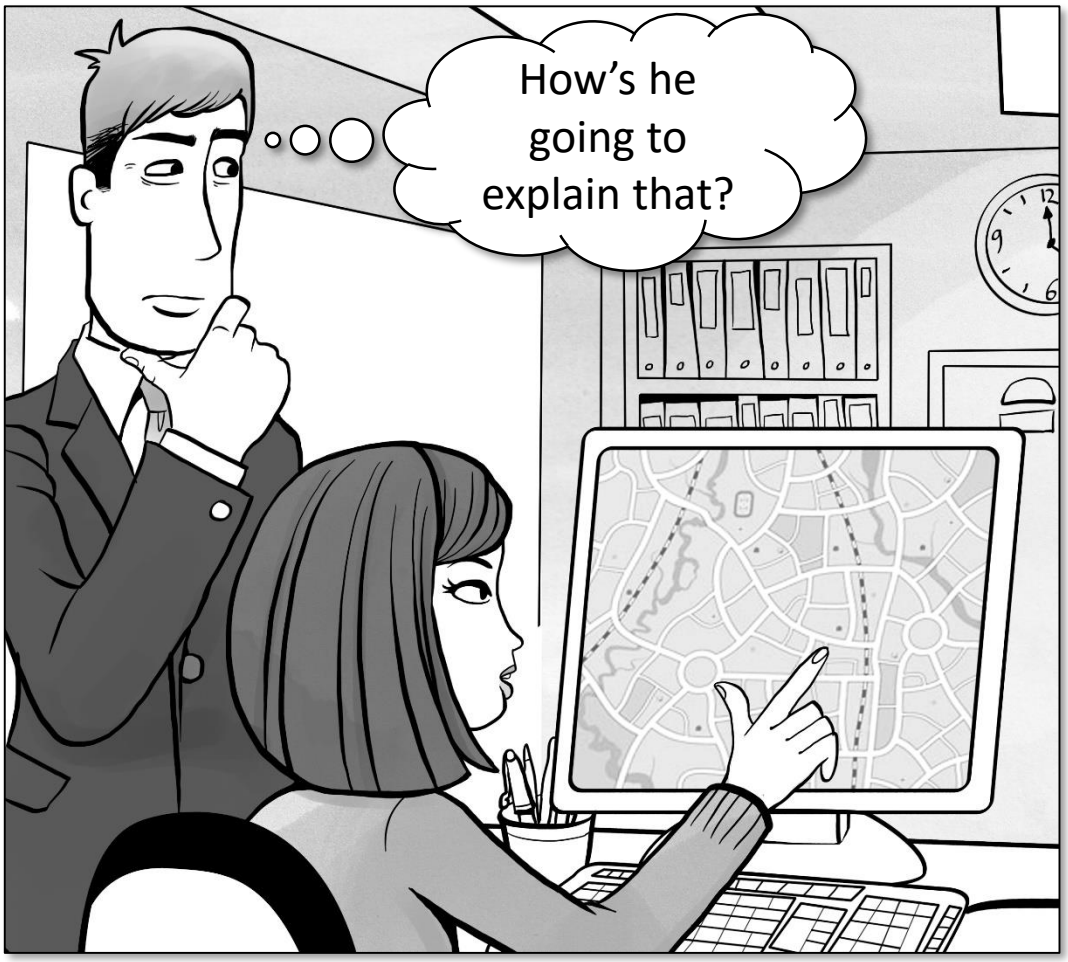
Cookies can be used to track and record your preferences and browsing habits.

Control location tracking



Control which sites can track your physical location.

1



Content settings – Microphone & Camera

Content settings

Manage exceptions...

Protected content

Some content services use machine identifiers to uniquely identify you for the purposes of authorizing access to protected content.

☑ Allow identifiers for protected content (computer restart may be required)

Microphone

Default

○ Ask when a site requires access to your microphone (recommended)

◉ Do not allow sites to access your microphone

Manage exceptions...

Adobe Flash Player microphone settings are different. Change

Camera

Logitech QuickCam I

○ Ask when a site requires access to your camera (recommended)

◉ Do not allow sites to access your camera

Manage exceptions...

Done

Unless required, do not allow sites to access your microphone or camera.

1

Plugin access

Content settings

Unsandboxed plugin access

1

○ Allow all sites to use a plugin to access your computer

◉ Ask when a site wants to use a plugin to access your computer (recommended)

○ Do not allow any sites to use a plugin to access your computer

Manage exceptions...

Done

Limit the ability of websites to freely use browser plugins to access your device.

Only expert users and administrators should adjust the other settings on this page.

Access 'Clear browsing data'

Privacy

Content settings... | Clear browsing data...

Click 'Clear browsing data'

1

Google Chrome may use web services to improve your browsing experience. You may optionally disable these services. Learn more

- [ ] Use a web service to help resolve navigation errors
- [ ] Use a prediction service to help complete searches and URLs typed in the address bar or the app launcher search box
- [x] Prefetch resources to load pages more quickly
- [ ] Automatically report details of possible security incidents to Google
- [x] Protect you and your device from dangerous sites
- [ ] Use a web service to help resolve spelling errors
- [ ] Automatically send usage statistics and crash reports to Google
- [x] Send a "Do Not Track" request with your browsing traffic

Passwords and forms

- [ ] Enable Autofill to fill out web forms in a single click. Manage Autofill settings
- [ ] Offer to save your web passwords. Manage passwords

2

Set as shown to clear most of your browsing history.

Using the settings shown does not guarantee security, but will help to reduce exposure. Note that parts of your browsing history may still be saved elsewhere.

3

Clear browsing data

Obliterate the following items from: the beginning of time

- [x] Browsing history
- [x] Download history
- [x] Cookies and other site and plugin data
- [x] Cached images and files
- [x] Passwords
- [x] Autofill form data
- [ ] Hosted app data
- [ ] Content licenses

Learn more | Clear browsing data | Cancel

Saved content settings and search engines will not be cleared and may reflect your browsing habits.

Secure Firefox

Note: all screenshots taken from the .com site. Mobile versions may have differing features.

Accessing Settings

1 *Click here…*

2 *Then click here to use private browsing (more secure)*

3 *Or here to review (and optionally clear) browsing history.*

4 *Finally, access Options here*

Options - Search

General
Search
Content
Applications
Privacy
Security
Sync
Advanced

Search

Select 'Search'... 1

Default Search Engine

Choose your default search engine. Firefox uses it in the location bar, search bar, and start page. 2

Google

Provide search suggestions

Set this to 'On' for optimum search performance

One-click search engines

The search bar lets you search alternate engines directly. Choose which ones to display.

Search Engine	Keyword
Google	
Yahoo	
Bing	

Restore Default Search Engines | Remove

Add more search engines...

Options - Privacy

General
Search
Content
Applications
Privacy
Security
Sync
Advanced

Privacy

Select 'Privacy'... 1

Tracking

Tell sites that I do not want to be tracked

Learn More

Select to turn off tracking 2

History

Firefox will: Never remember history

Firefox will use the same settings as private browsing, and will not remember any history as you browse the Web.

You may also want to clear all current history.

Set to 'Never remember history' 3

Location Bar

When using the location bar, suggest:

History

Bookmarks

Open tabs

?

You can clear your current history (recommended). 4

Options - Advanced - General

General
Search
Content
Applications
Privacy
Security
Sync
Advanced

Advanced

General | Data Choices | Network | Update | Certificates

Accessibility

- [ ] Always use the cursor keys to navigate within pages
- [ ] Search for text when I start typing
- [x] Warn me when websites try to redirect or reload the page

Browsing

- [x] Use autoscrolling

Set this to 'on'

1

Options - Advanced - Update

General
Search
Content
Applications
Privacy
Security
Sync
Advanced

Advanced

General | Data Choices | Network | Update | Certificates

Firefox updates:

- (•) Automatically install updates (recommended: improved security)
  - [x] Warn me if this will disable any of my add-ons
- ( ) Check for updates, but let me choose whether to install them
- ( ) Never check for updates (not recommended: security risk)

Show Update History

- [x] Use a background service to install updates

Automatically update:

- [x] Search Engines

!

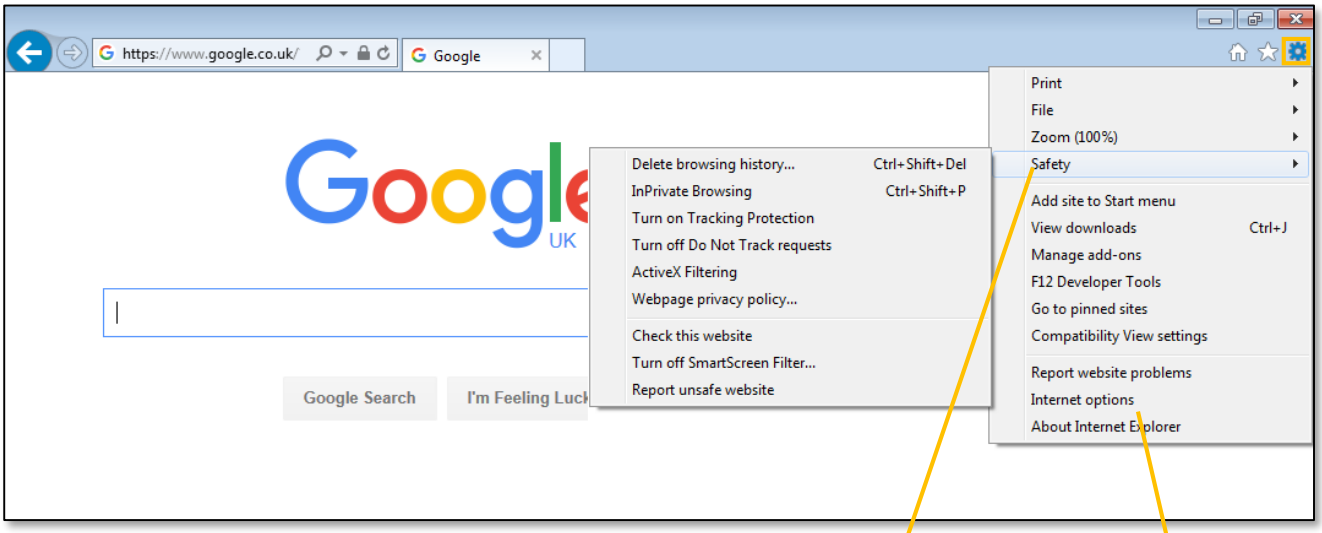
Failure to update browsers & add-ons can be exploited by hackers & malware.

Secure IE

Note: all screenshots taken from the .com site. Mobile versions may have differing features.

Accessing Safety Options & Settings

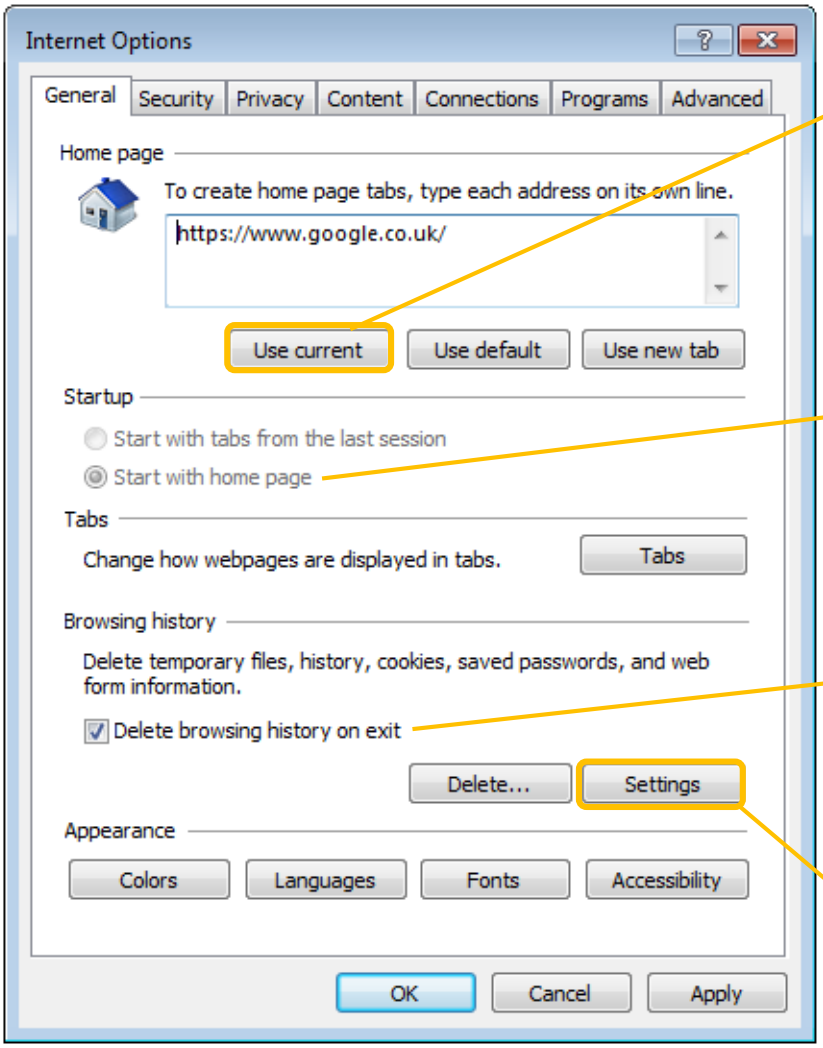
1 *Click to access the menu*



2 *Then select 'Safety' for a quick list of popular options*

3 *Or click 'Internet options' to access the main security settings area.*

Internet Options - General



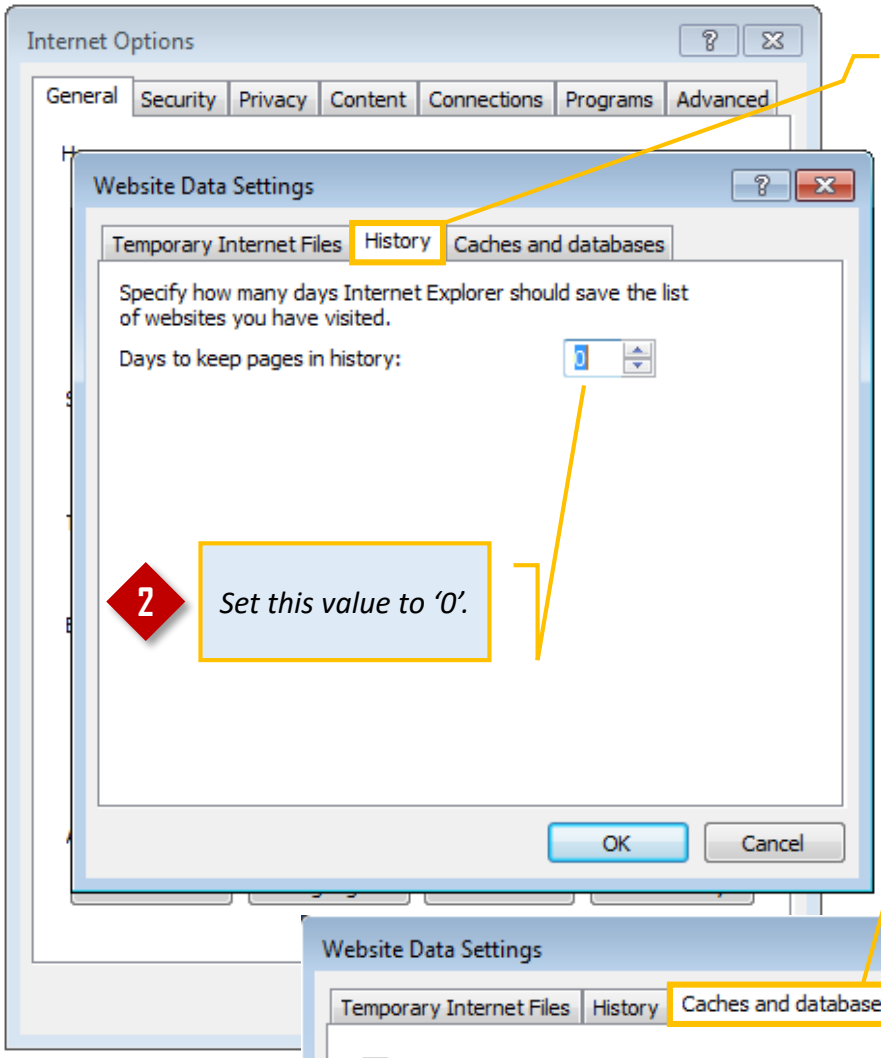
Select a 'safe' home page that does not imply any specific browsing habits. **1**

Set IE to start with the home page. **2**

Set to delete browsing history on exit. **3**

Now click 'Settings'. **4**

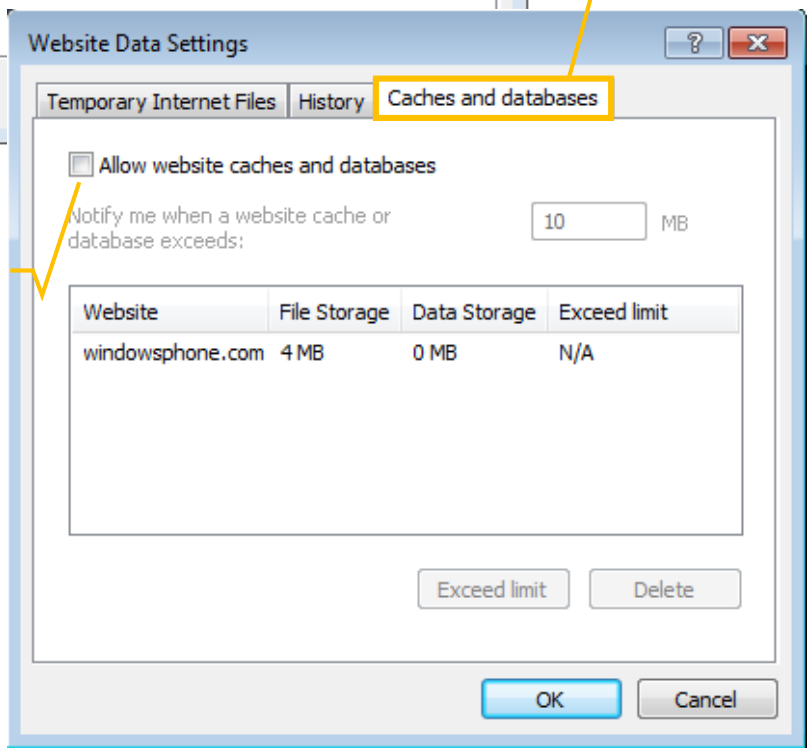
Internet Options – General - Settings



1 *Select the 'History' tab…*

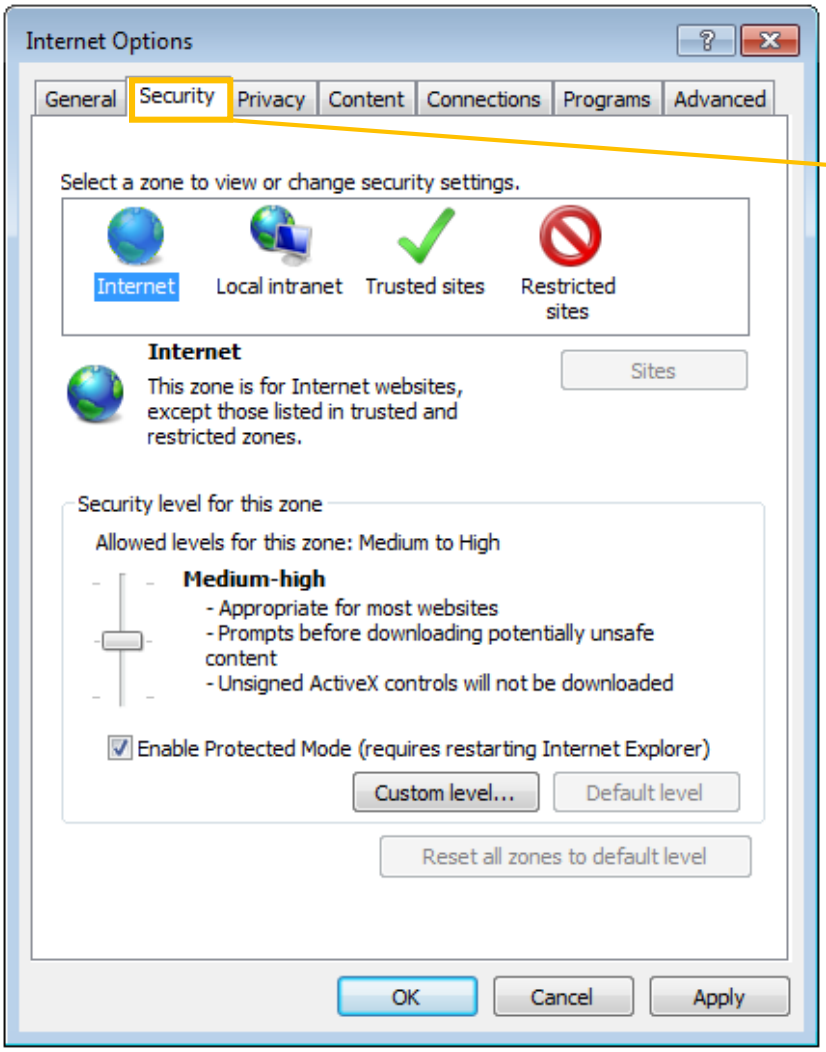
2 *Set this value to '0'.*

3 *Select the 'Caches and databases' tab…*



4 *Deselect this option.*

Internet Options – Security



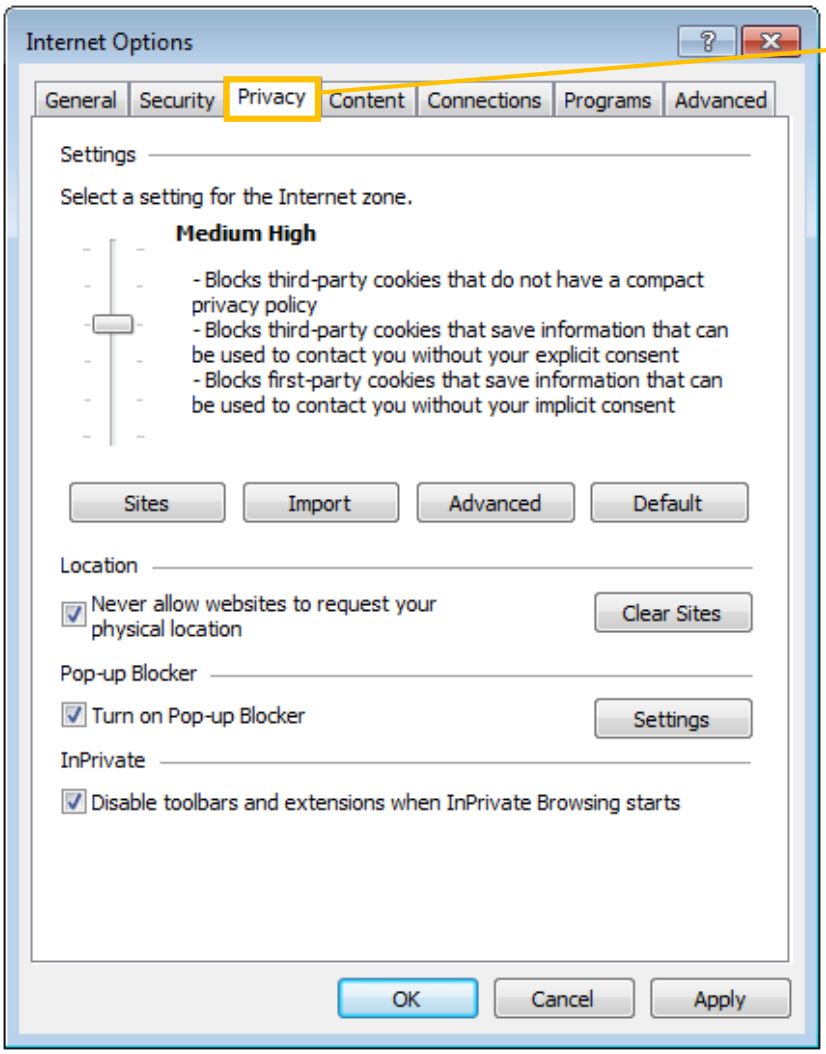
Select the 'Security' tab…

1

2

Choose the security level that suits your role.

Internet Options – Privacy



Select the 'Privacy' tab…

1

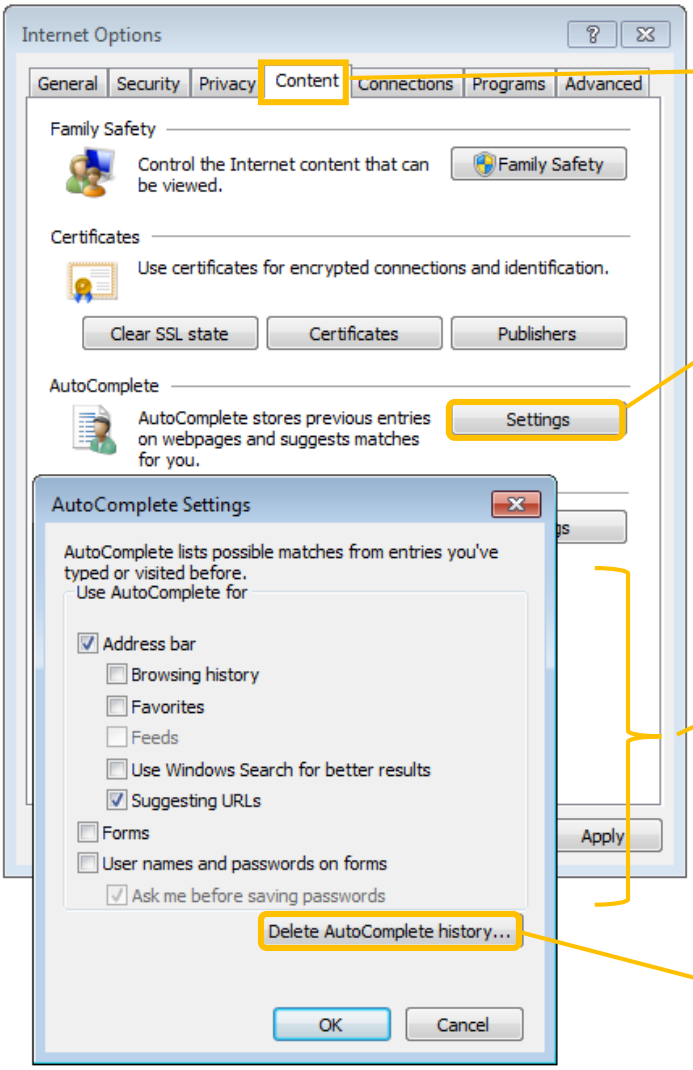
Choose the cookie setting that suits your role.

2

Select all three settings as shown (recommended).

3

Internet Options – Content



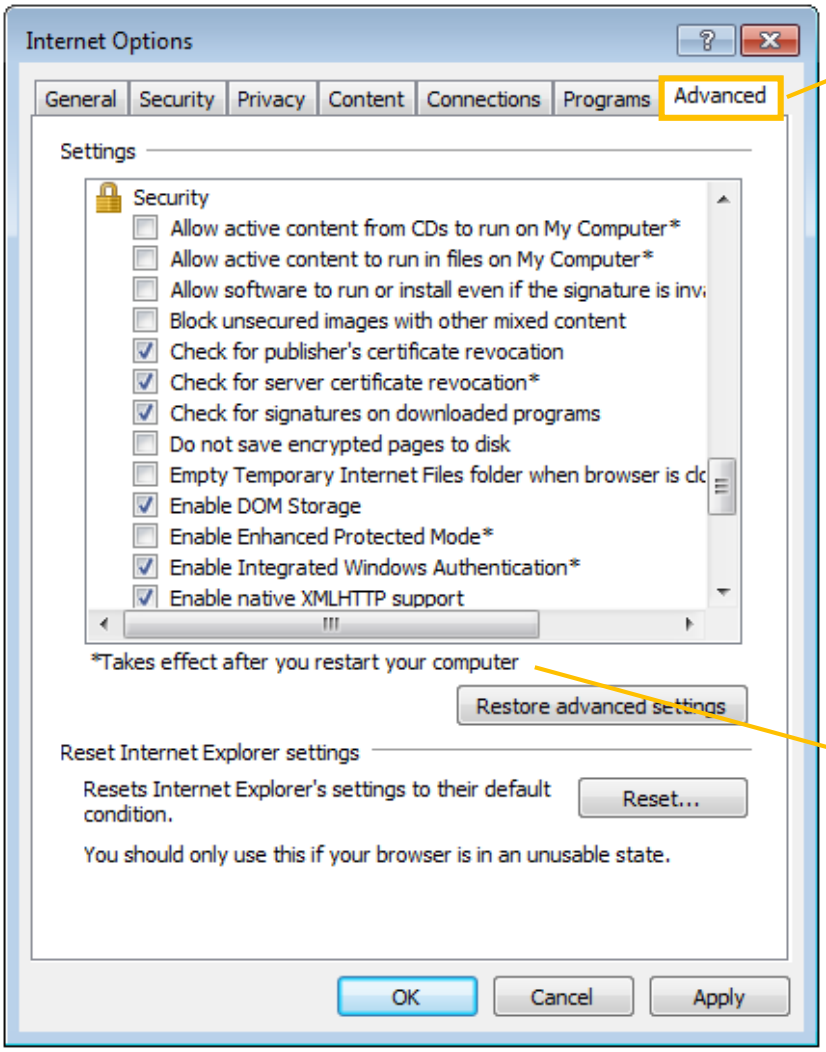
Select the 'Content' tab… **1**

Click 'Settings'… **2**

Choose the auto-complete settings that suit your role. **3**

Click 'Delete AutoComplete history'. **4**

Internet Options – Advanced



Select the 'Advanced' tab…

1

2

Scroll down to 'Security'. Consult your administrator for the settings required in your organisation.

Restart your computer to make sure that all new settings take effect.

3

Secure Smart Phone

SMART PHONES ARE INCREASINGLY USED BY ALMOST EVERYONE, FROM TOP EXECUTIVES TO FRONTLINE STAFF. BOTH VICTIMS AND PERPETRATORS OF CRIME USE THESE DEVICES, WHICH REPRESENT A REAL TARGET FOR CRIMINALS AND INVESTIGATORS

If a criminal gets hold of your smart device, and you have not made sure that it is secure, the stolen smart phone could put you at risk.

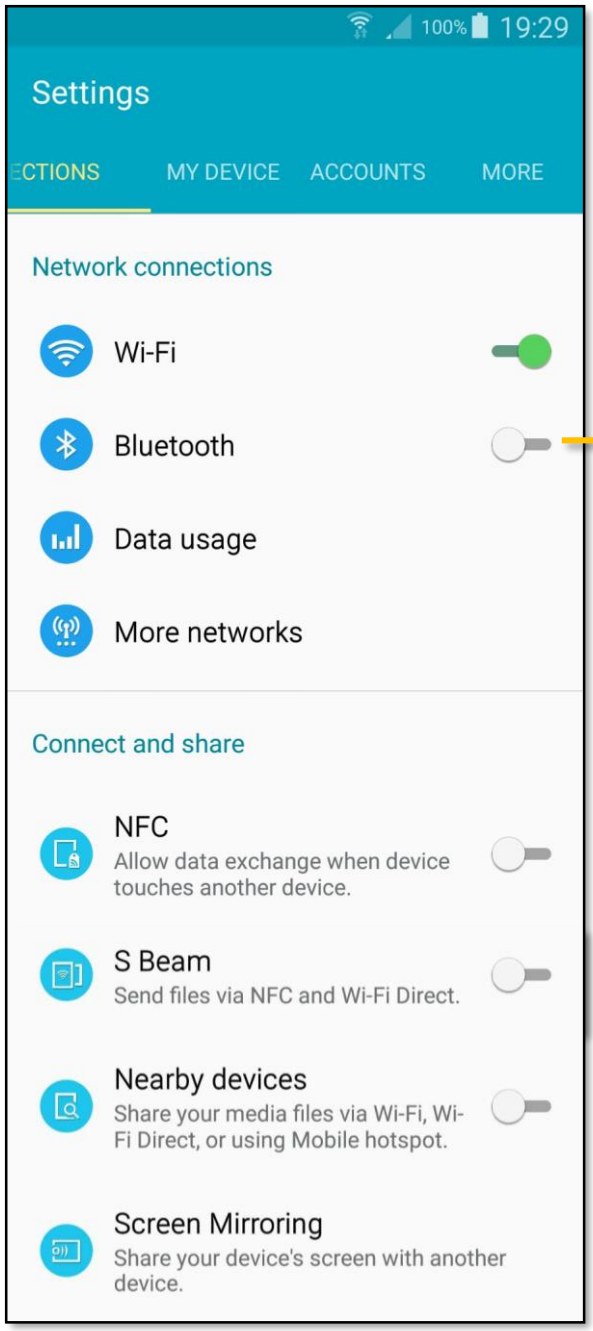
Contact information, messages, photos, social media feeds, location data and more can all be derived from a mobile device.

While deeper device forensics requires a great deal of skill and the right equipment, even a layman might be able to learn a lot about you from a quick look through an insecure handset or tablet.

Secure Smart Phone

Android devices

Connections



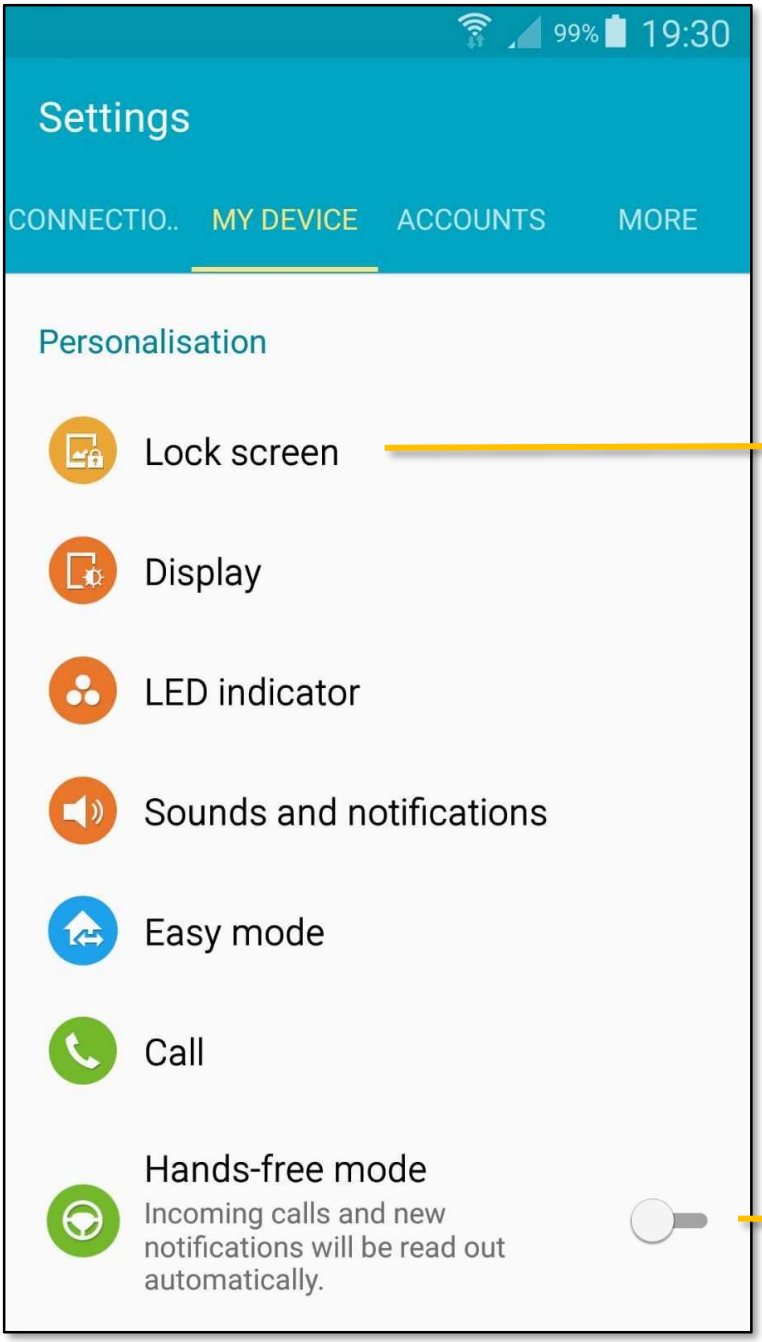
1

Turn off Bluetooth unless required. ***Always keep it off when not in use.***

2

Turn off Connect and Share options unless essential

My Device



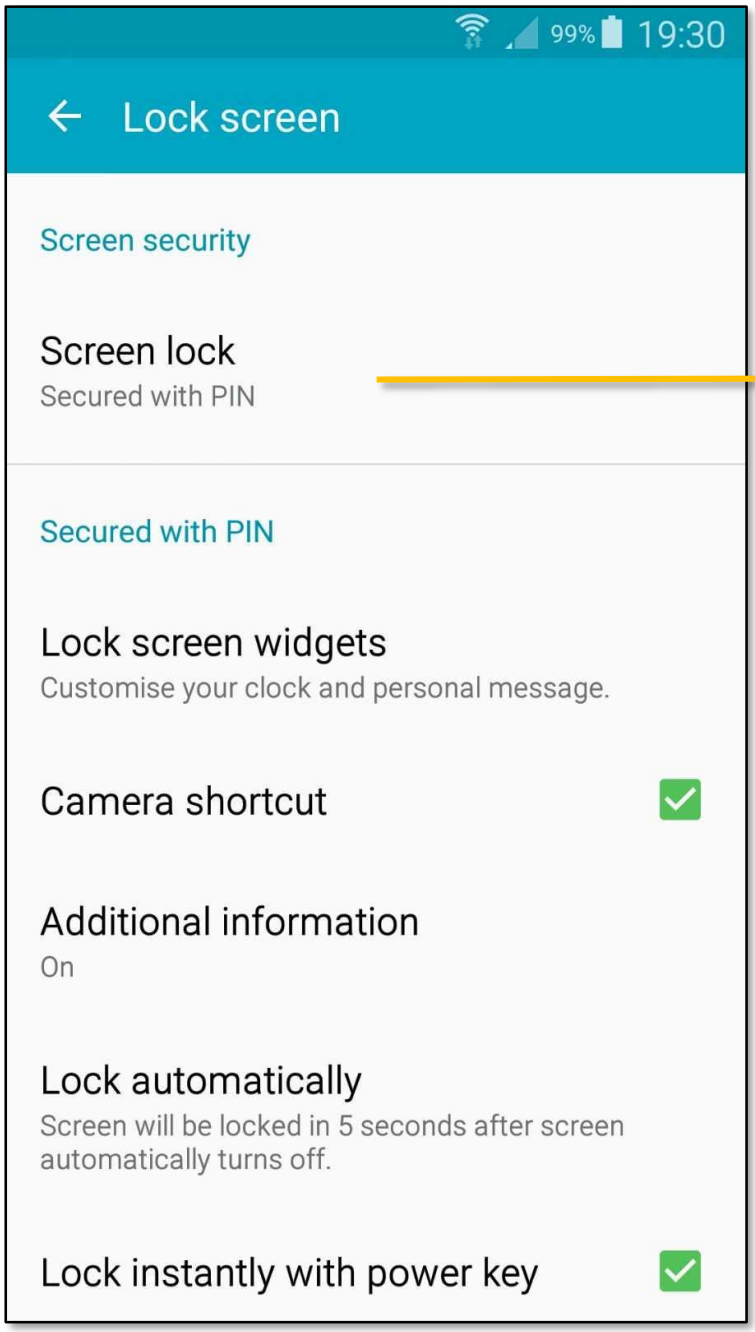
1

Set a reasonable lock screen period. (See next page)

2

Turn off hands-free mode unless required

Lock Screen



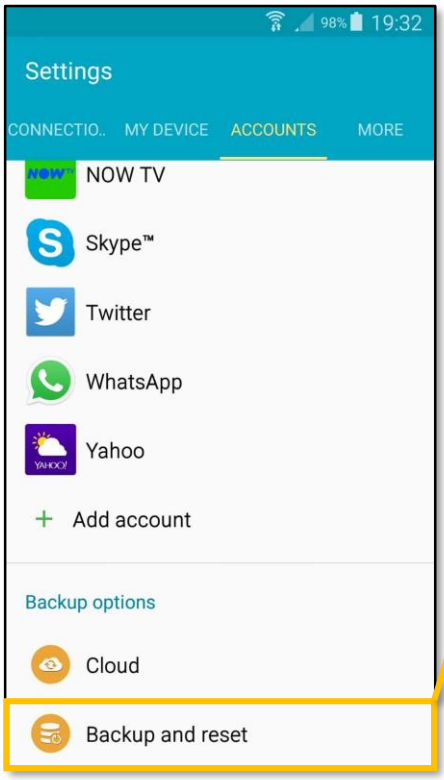
1

Set a lock screen PIN

2

Set automatic locking and power key locking to ON

Backup options

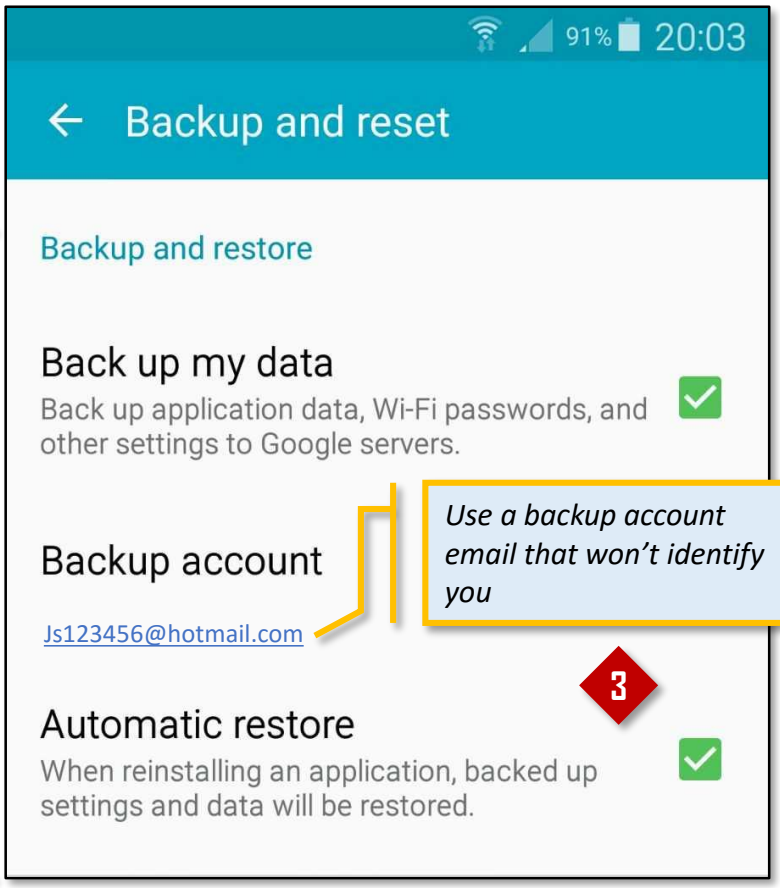


1

Press to access Backup options

2

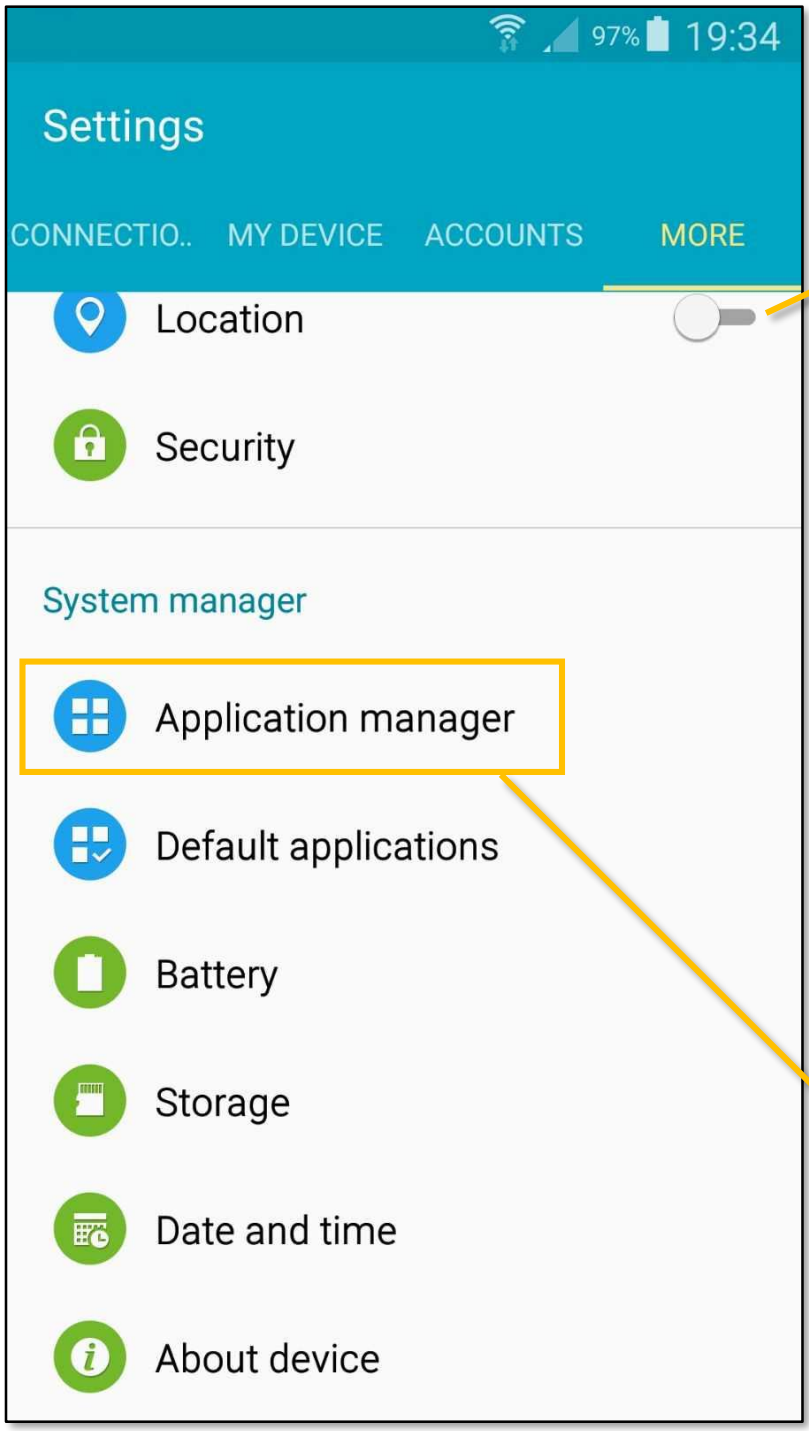
Set appropriate backup and restore settings, based on your role



Use a backup account email that won't identify you

3

Location and Application management



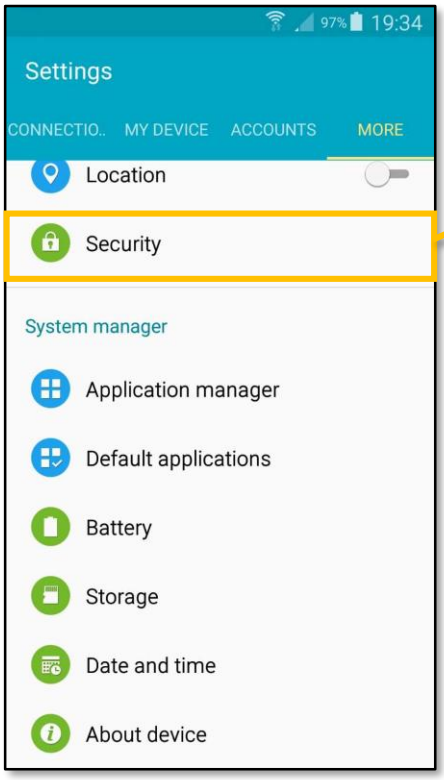
1

Turn off location services, unless required

2

Review your installed Apps and remove any unwanted ones.

Security

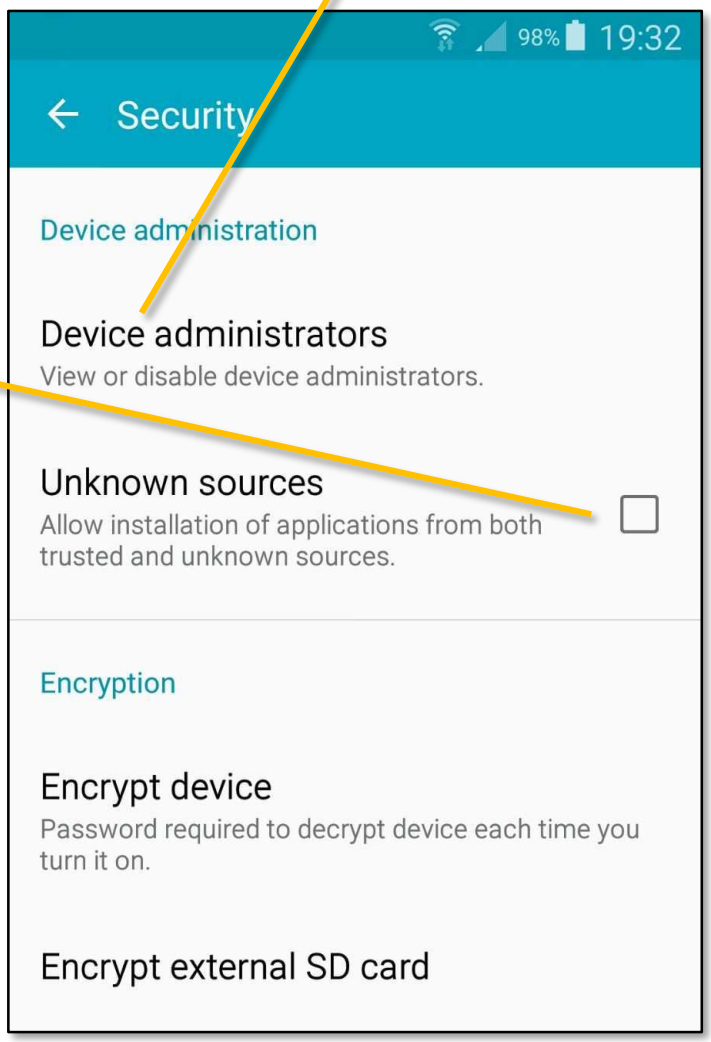


Press to access Security management

1

2

Review your device administrators



3

Disable unknown sources

Consider encrypting your device & any SD cards, if permitted

4

Security

*Though useful, the **Find My Mobile** feature could be exploited by a hacker to track your location*

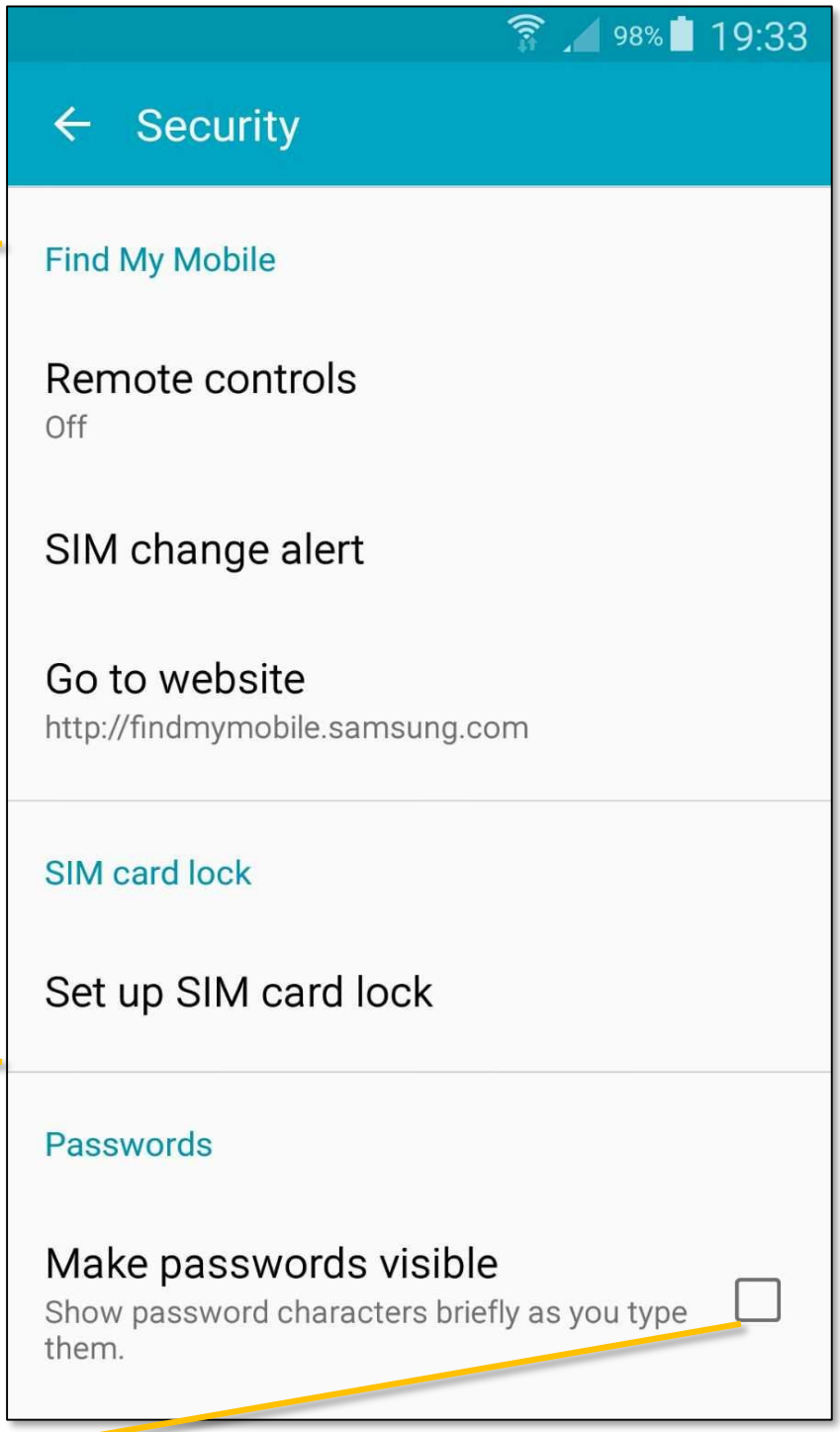
1

Request local policy guidance for each of these settings

SIM card lock will prevent the switching of SIM cards

2

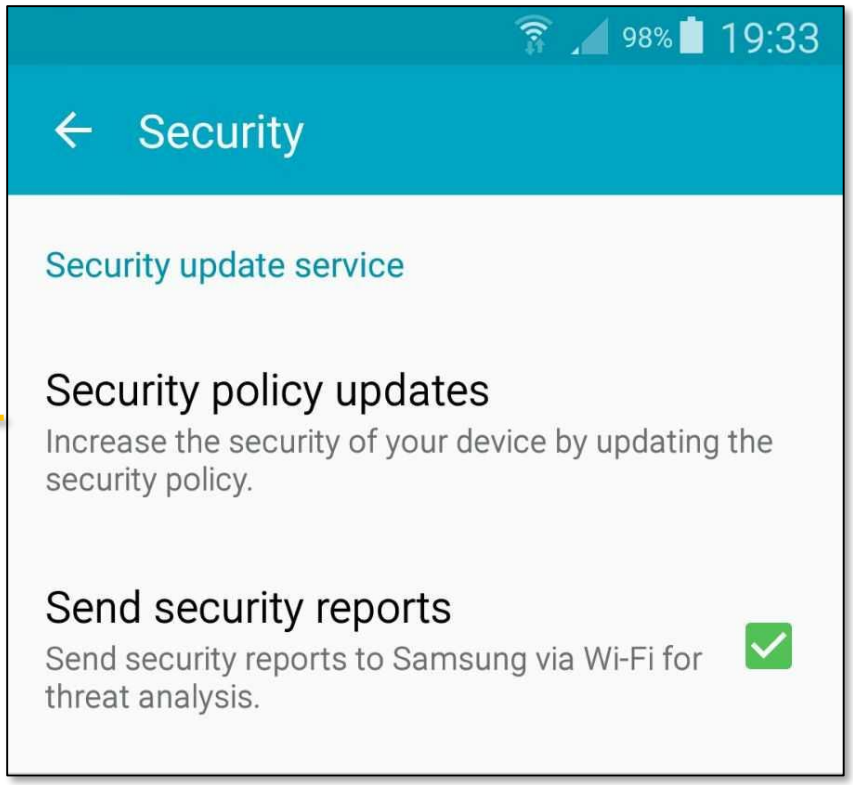
Do not make passwords visible



Security updates

1

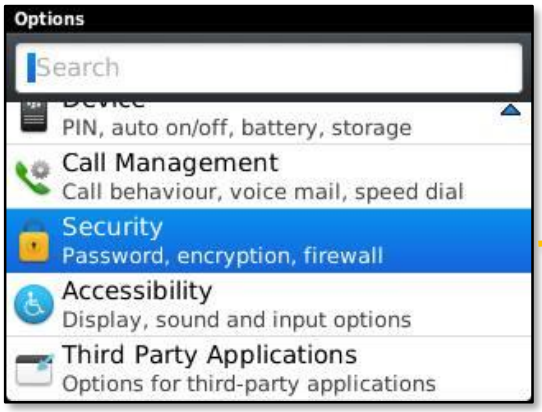
Ensure that your security policies are up-to-date



Secure Smart Phone

Blackberry

To access Security settings



Enter the Options menu and then select Security

1

Password

Select Password from the Security menu

1

- *Enable password control*
- *Select a strong password*
- *Limit the number of attempts*
- *Set a lock screen period*
- *Set to prompt on App install*

2

Holstering lock

1

Set the device to auto-lock when holstered.

Encryption

Now select Encryption from the Security menu

1

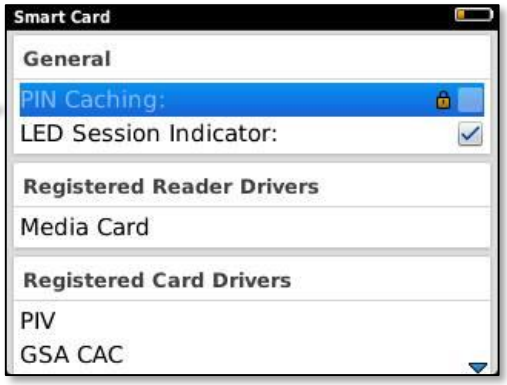
- *Select strong encryption*
- *Consider using two-factor*
- *Encrypt Contacts*
- *Encrypt Media Files*
- *Encrypt the Media Card*

2

PIN Caching

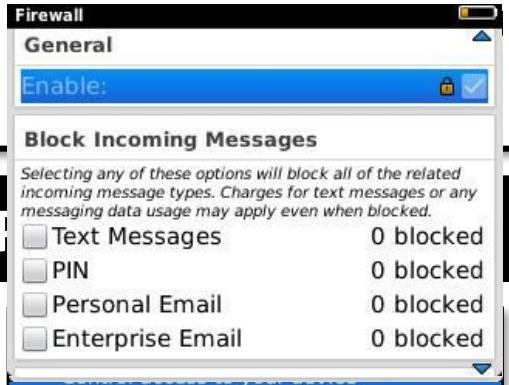
Next, select Smart Card from the Security menu

1



2

Deactivate PIN Caching



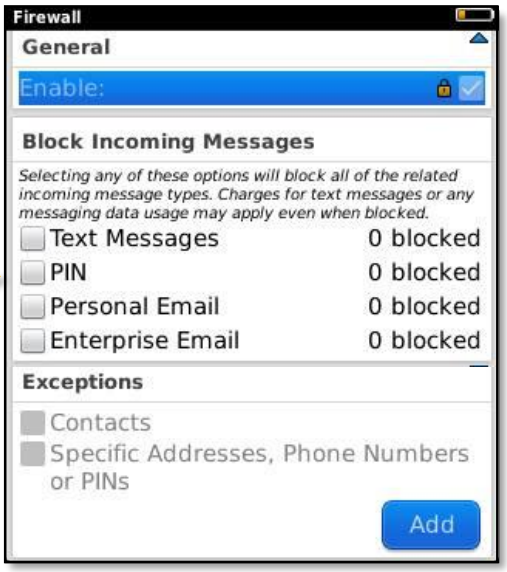
Select Parental Controls and consider whether to activate

1

Firewall

Select Firewall

1



2

Decide whether to block any message types

Firewall

2

Wipe all data and/or Apps from your device when appropriate

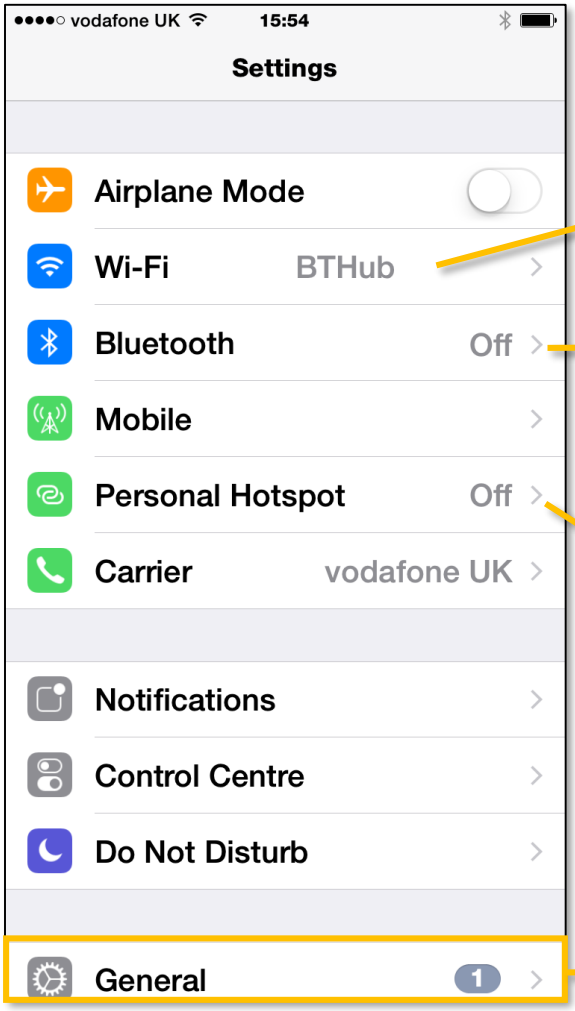
Secure Smart Phone

iOS (iPhone/iPad) devices

To access Settings

Locate the Settings icon on your device and press it

1



Only use trusted, secure WiFi networks

2

Turn Bluetooth off unless needed

3

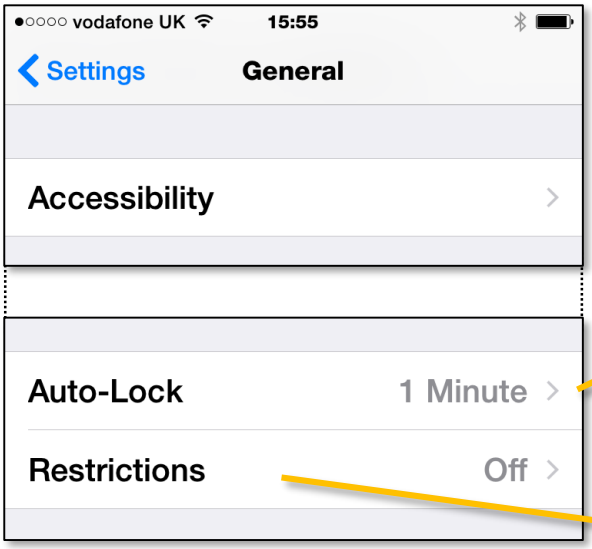
Turn Hotspot off unless needed

4

Now press the 'General' menu option

5

Auto-Lock



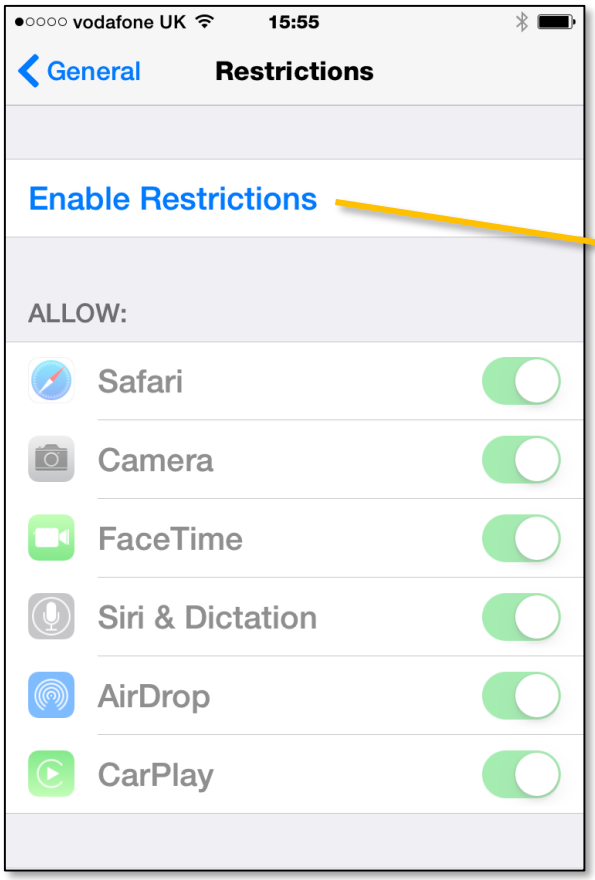
1

Set the period after which your device will automatically lock and require a password or Touch ID (fingerprint) to access.

2

Now press 'Restrictions' if you ever share your device with a child or other vulnerable person.

Restrictions



1

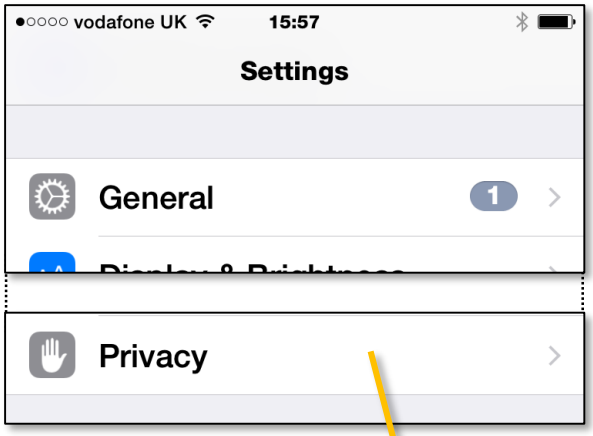
Press 'Enable Restrictions' if you want to restrict access to specific applications.

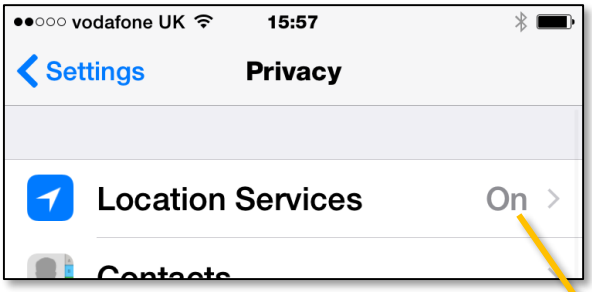
You will be asked to select a Restrictions Password.

2

Disallow access to those applications you do not want other users of your device to use. You can also do this on any iOS device you have given to a child or other vulnerable person.

Privacy - Location Services



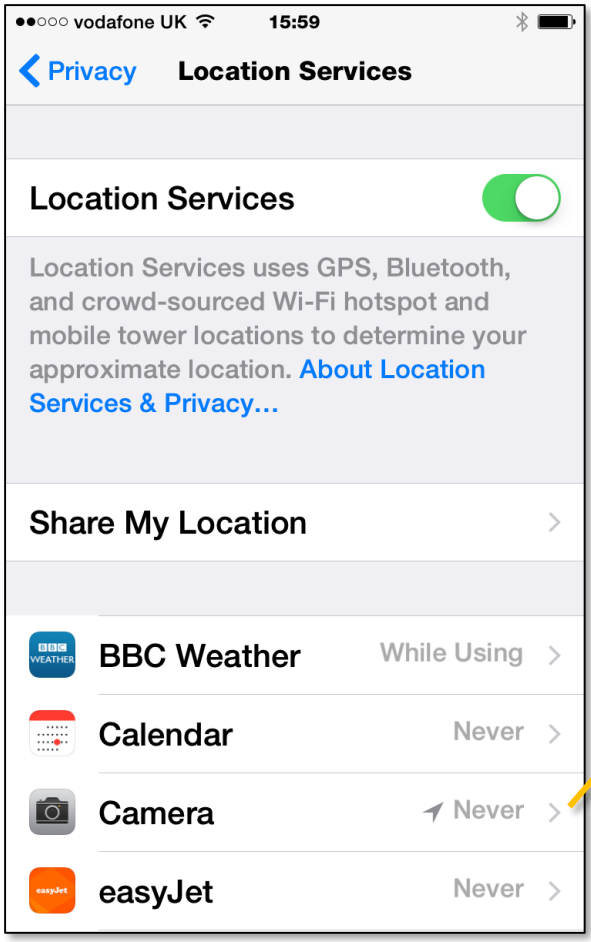


1

Return to 'Settings' and select 'Privacy'

2

Then select 'Location Services'

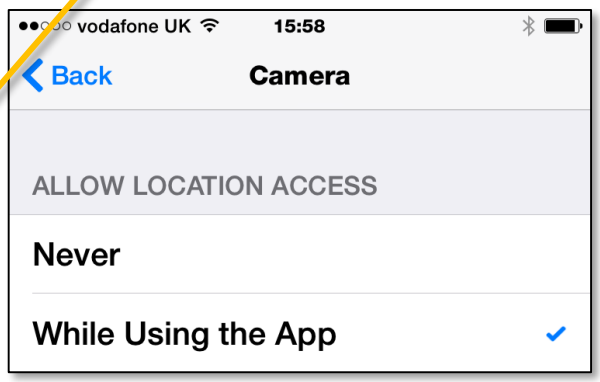


3

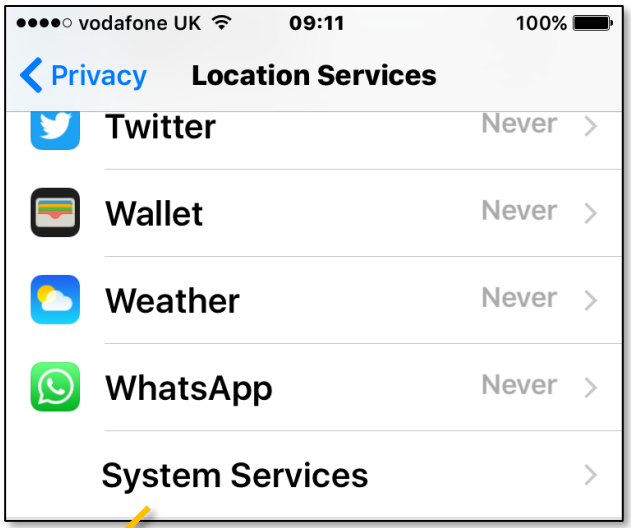
*Turn Location Services **OFF** for maximum security (recommended)*

4

Alternatively, you can leave Location Services ON and edit which Apps are allowed to use your location and when.



Privacy – Frequent Locations

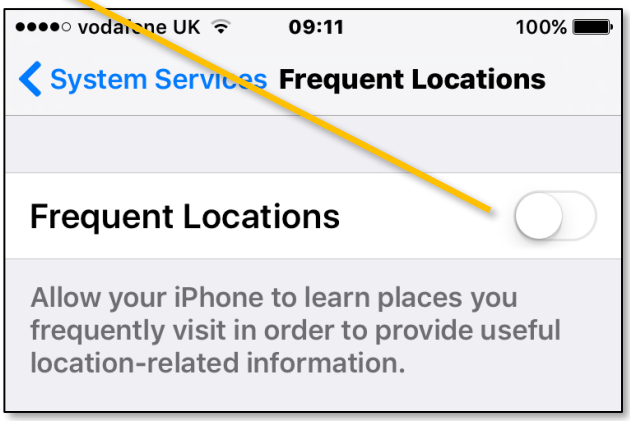


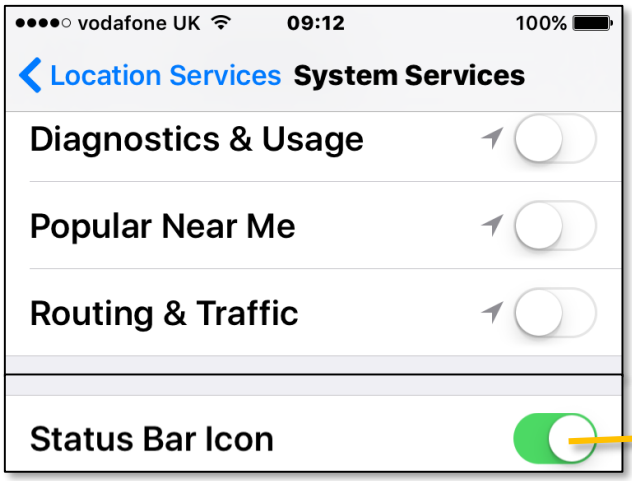
1

Stay in the 'Location Services' screen and scroll down to 'System Services'...

2

*To prevent Apple from collecting data on your frequent locations, turn this option **OFF**.*

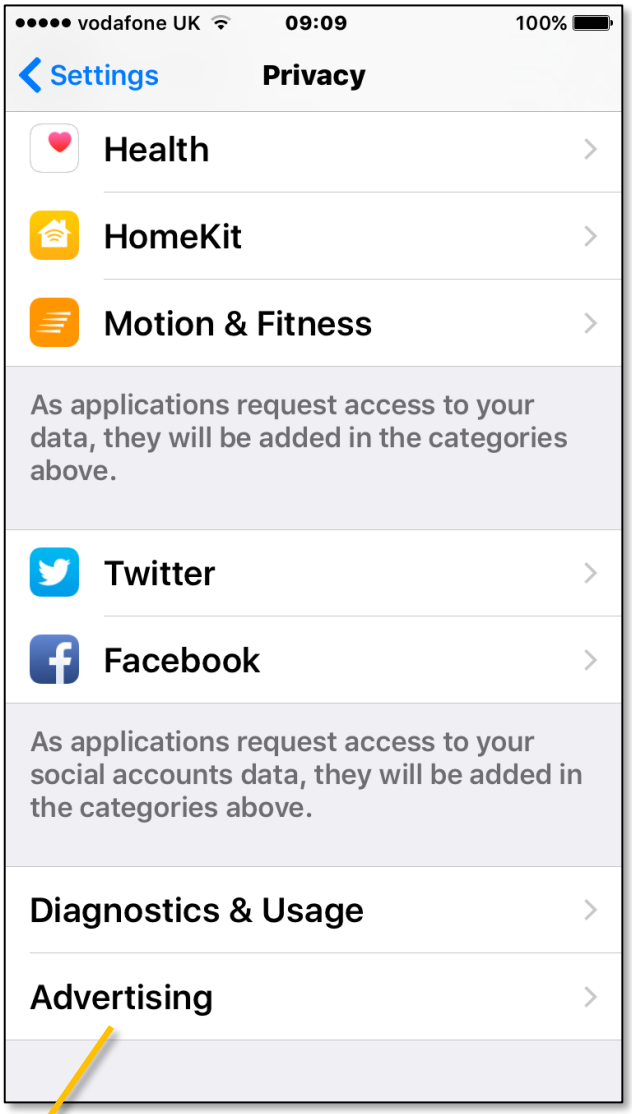




3

*Scroll down to the bottom of the System Services screen and turn 'Status Bar Icon' **ON** to receive alerts in your status bar when a service requests your location.*

Privacy – Ad Tracking

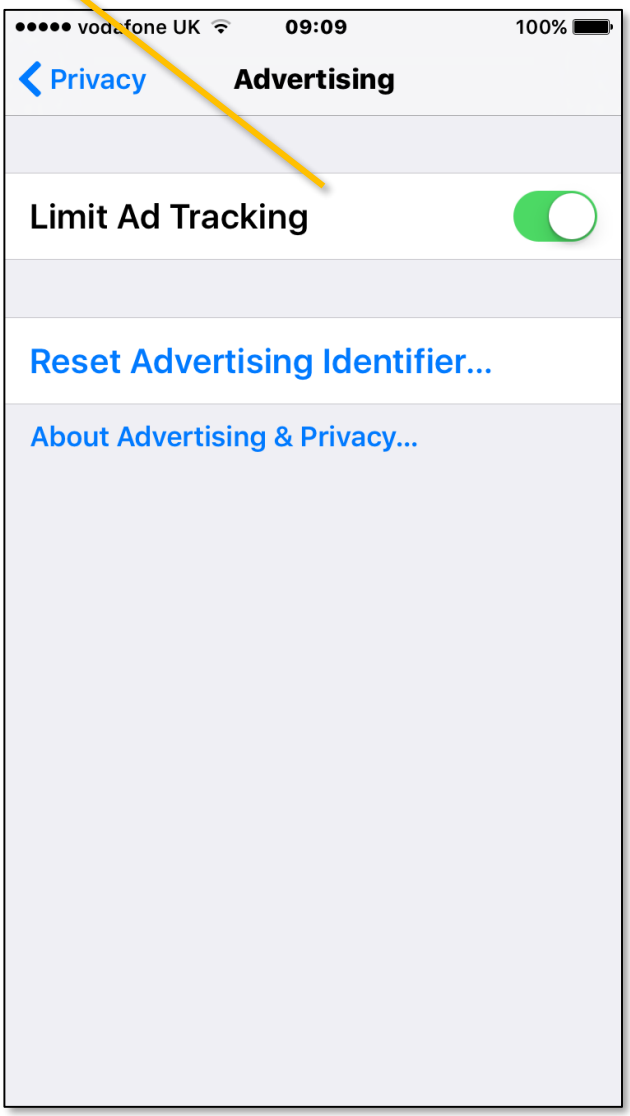


Return to 'Privacy' and scroll down to 'Advertising'…

1

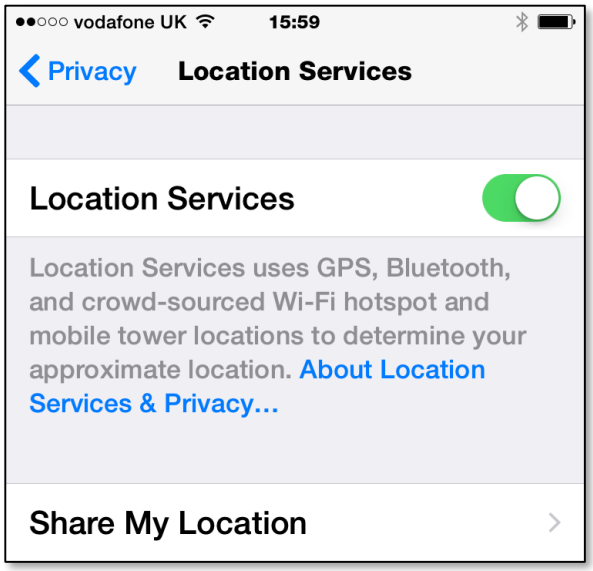
2

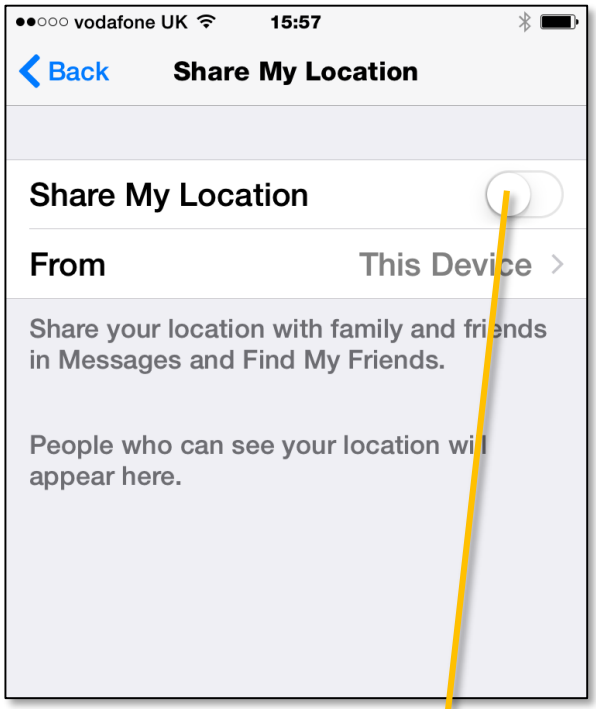
*To limit the amount of data collected by Apple, turn 'Limit Ad Tracking' **ON**.*



Share My Location

Share My Location





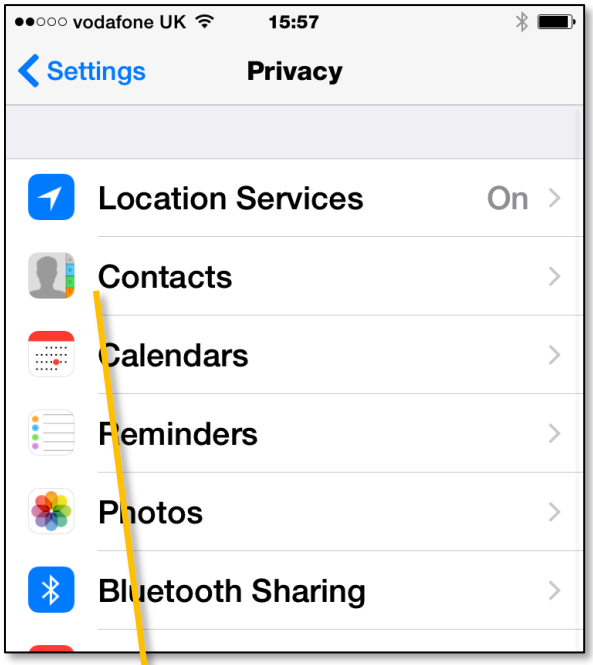
*Set Share My Location to **OFF**.*

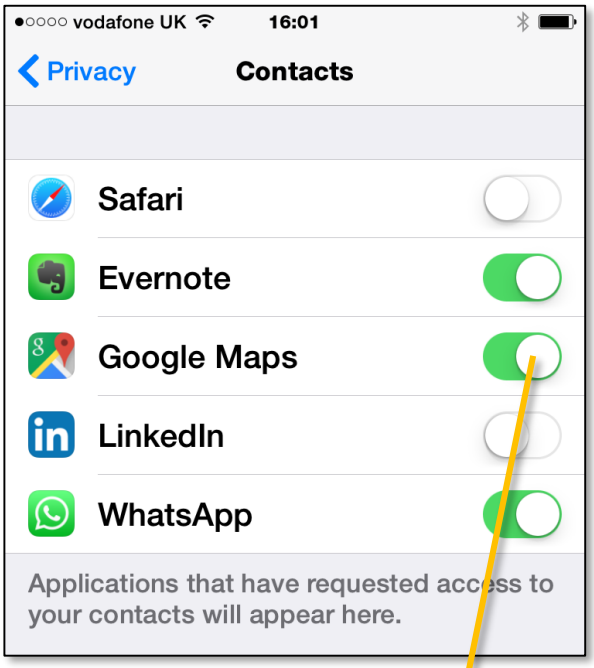
1

I was able to track the banker's location because he:

1. Left location services and location sharing on.
2. Was running a social App that automatically signed him in <u>and</u> showed his location in his public profile.

Contacts



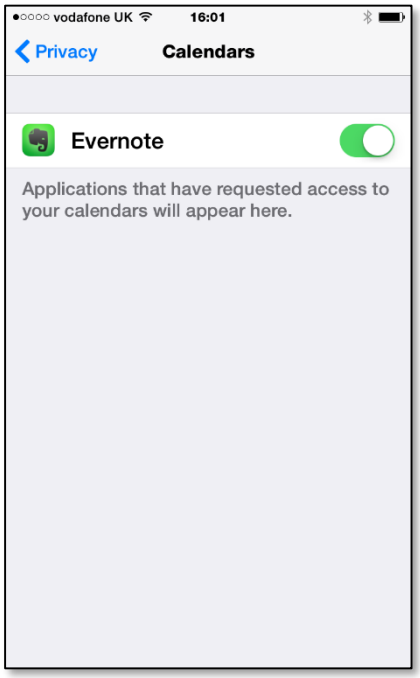


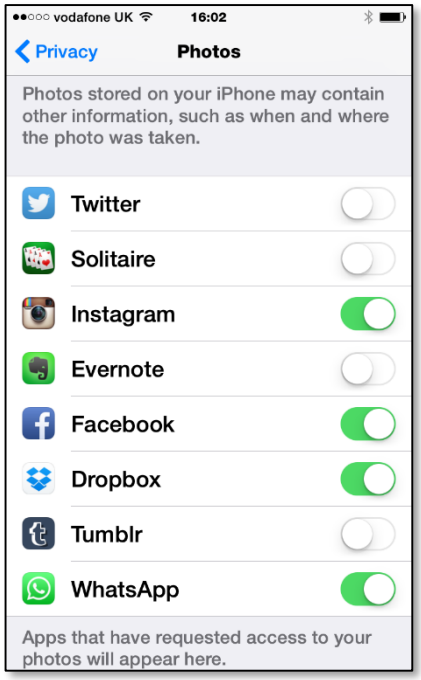
1

Return to Settings/Privacy and select 'Contacts'.

Decide which Apps genuinely need to access your contacts list. Turn the others OFF.

2

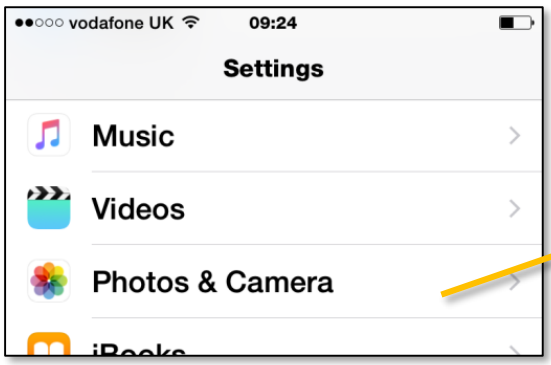




3

Repeat the process for Calendars, Photos and Microphone, etc.

Photos and Camera



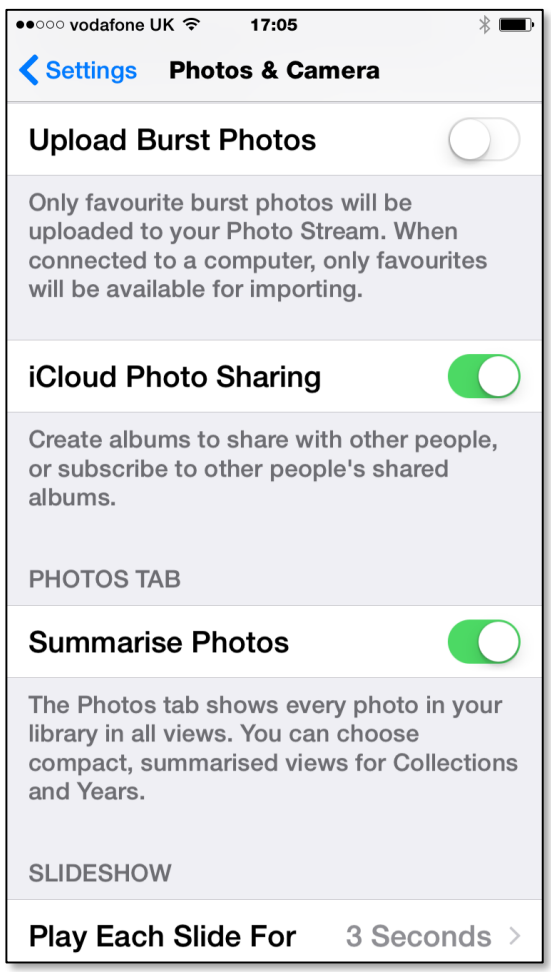
1

Return to Settings and click on 'Photos & Camera'.

2

Decide whether or not you want to automatically share and upload your photos.

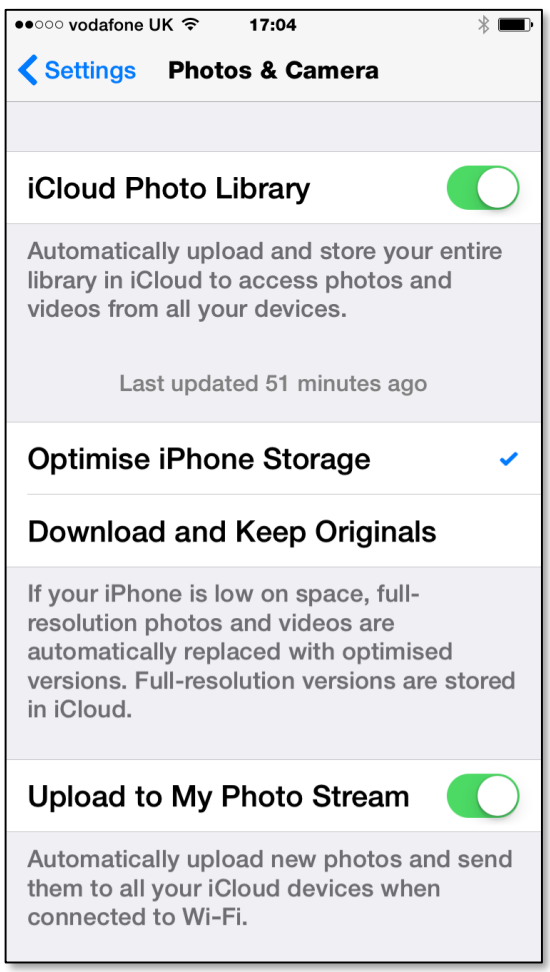
Note that Cloud Photo Library will copy your photos onto ALL of your iCloud connected devices.



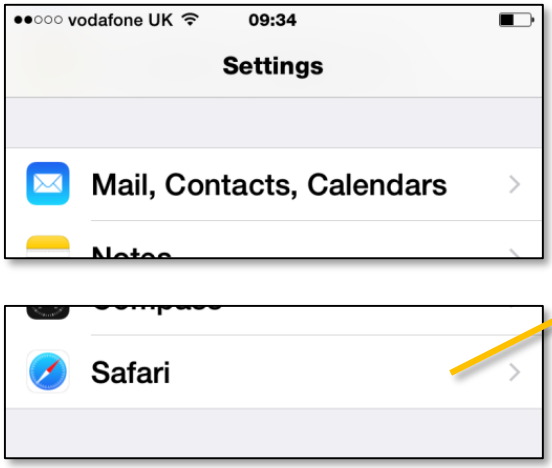
Off = safer

Off = safer

Off = safer



Safari Browser

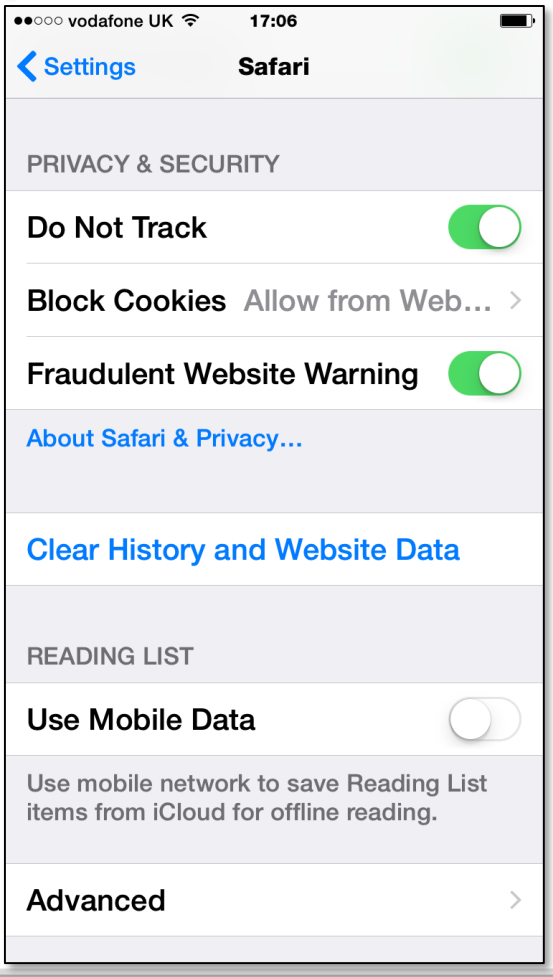


1

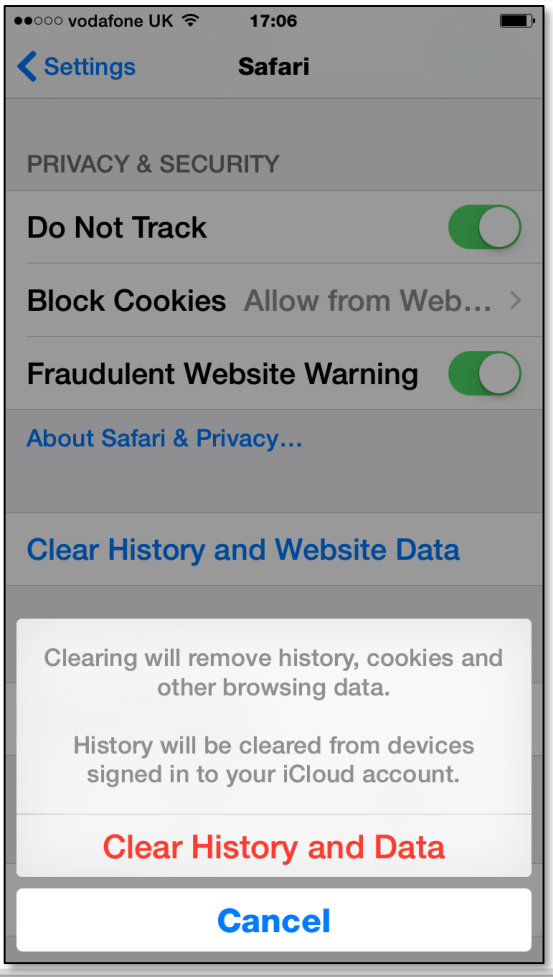
Return to Settings and scroll down until you locate the settings access for your Safari Web Browser. Press this.

2

Tell websites not to track you, then clear your history and website data regularly to remove browsing history and cookies.



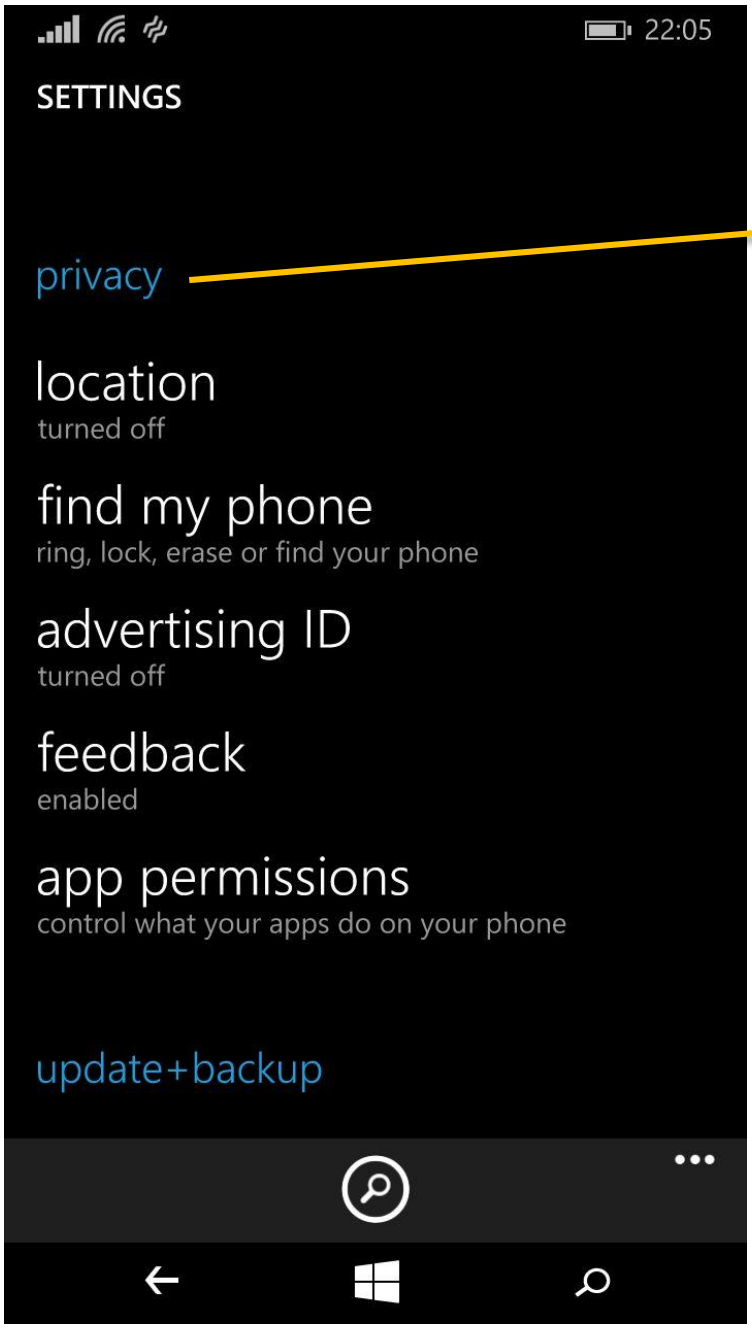
Regularly



Secure Smart Phone

Windows devices

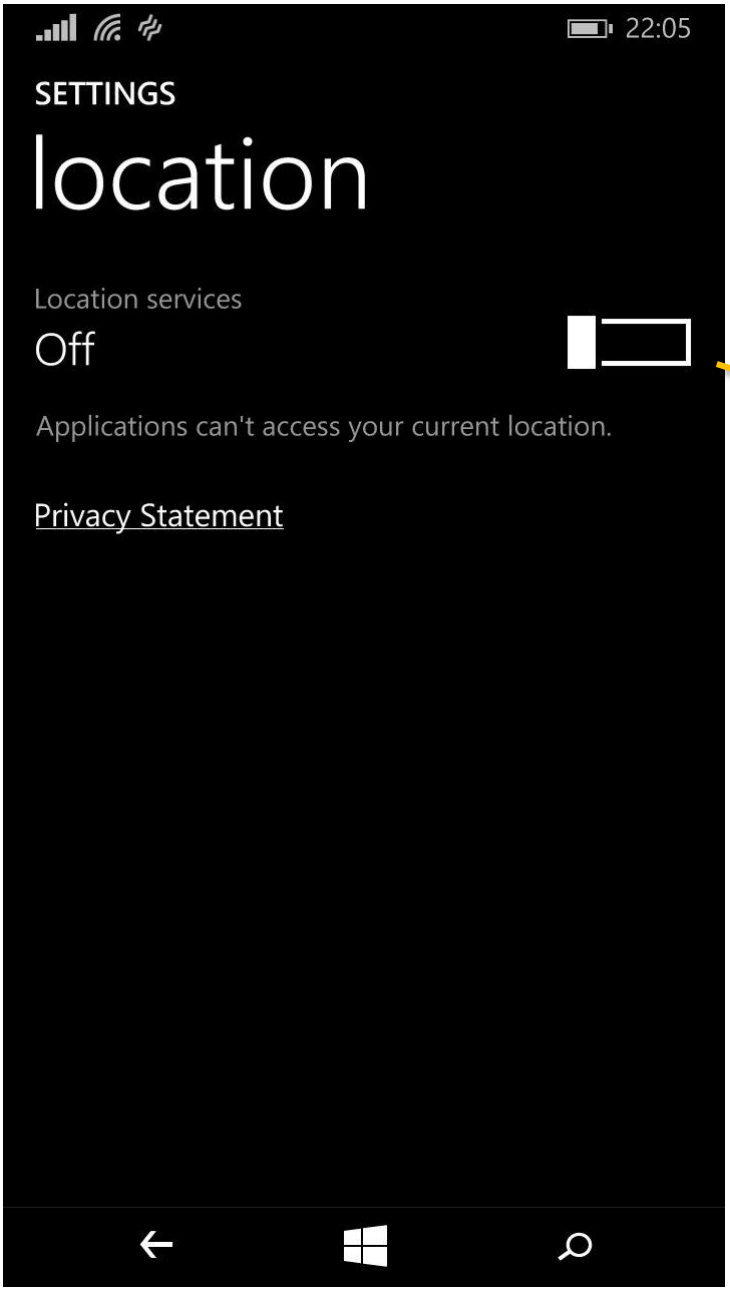
Settings - Privacy



Access and set each option as shown in the following pages

1

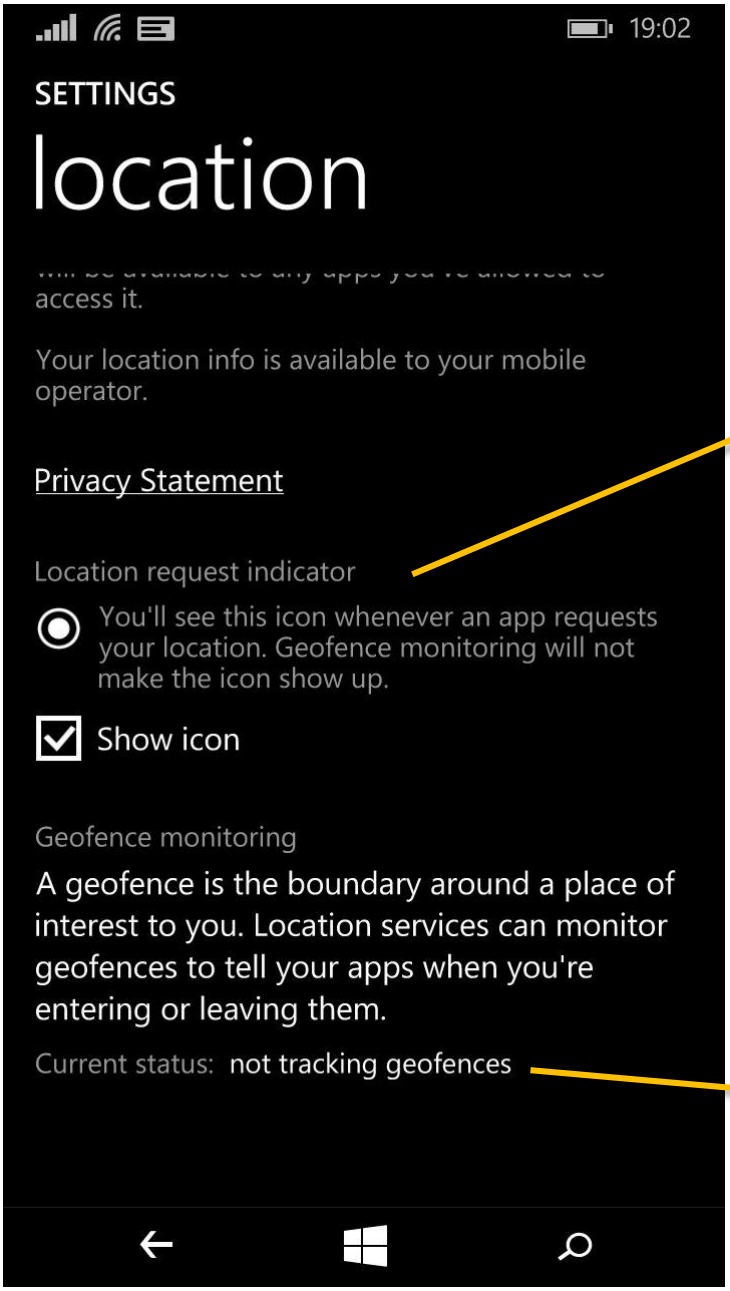
Location services



Turn Location Services OFF unless required

1

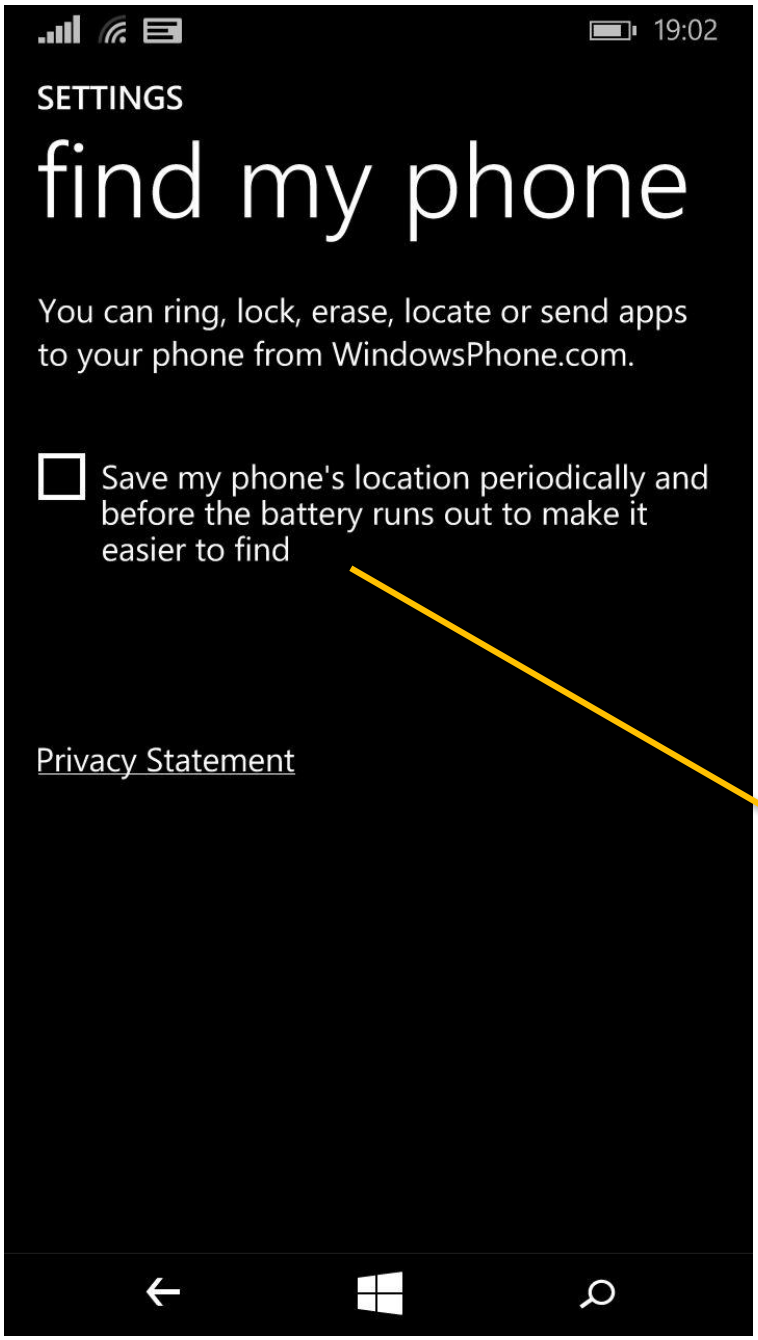
Location settings



Turn request indicator ON 1

Turn Geofence monitoring OFF 1

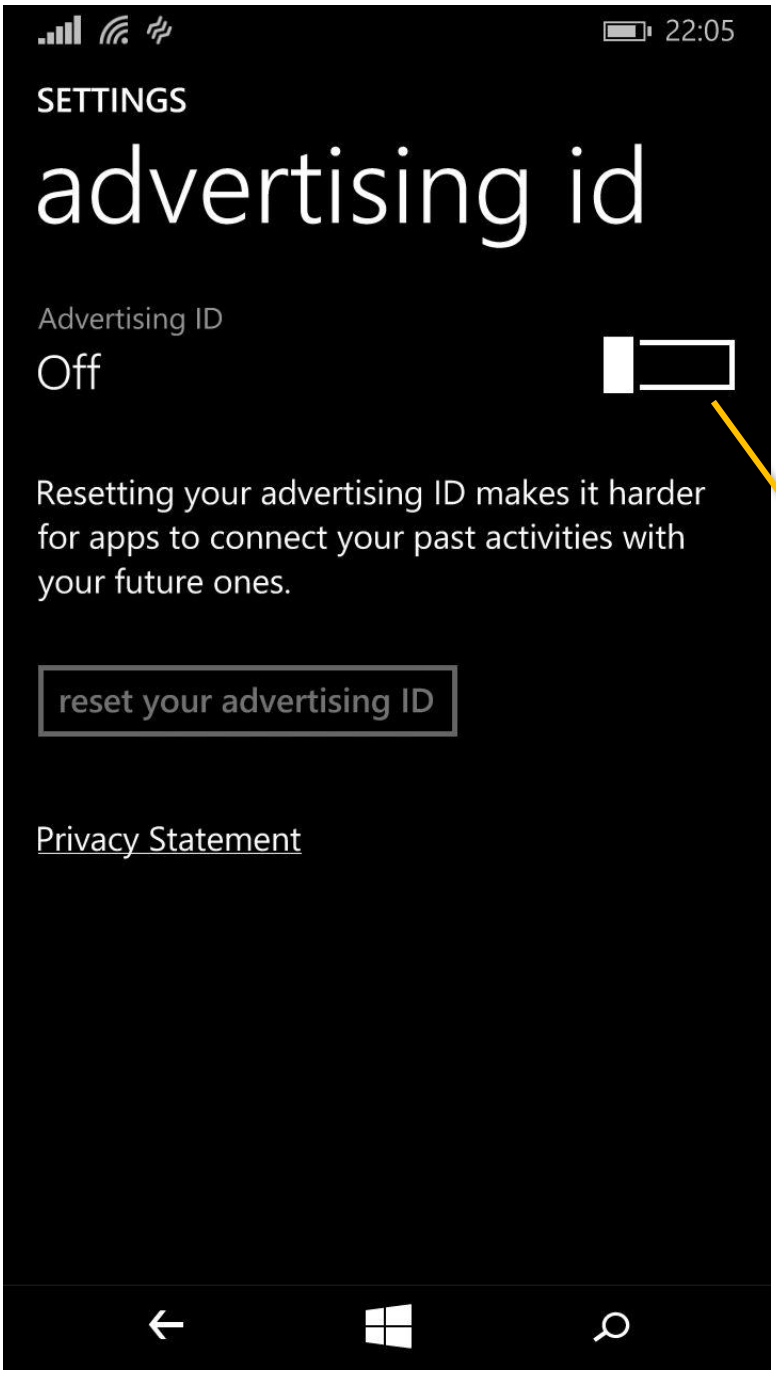
Find my phone



Set the saving of phone location OFF

1

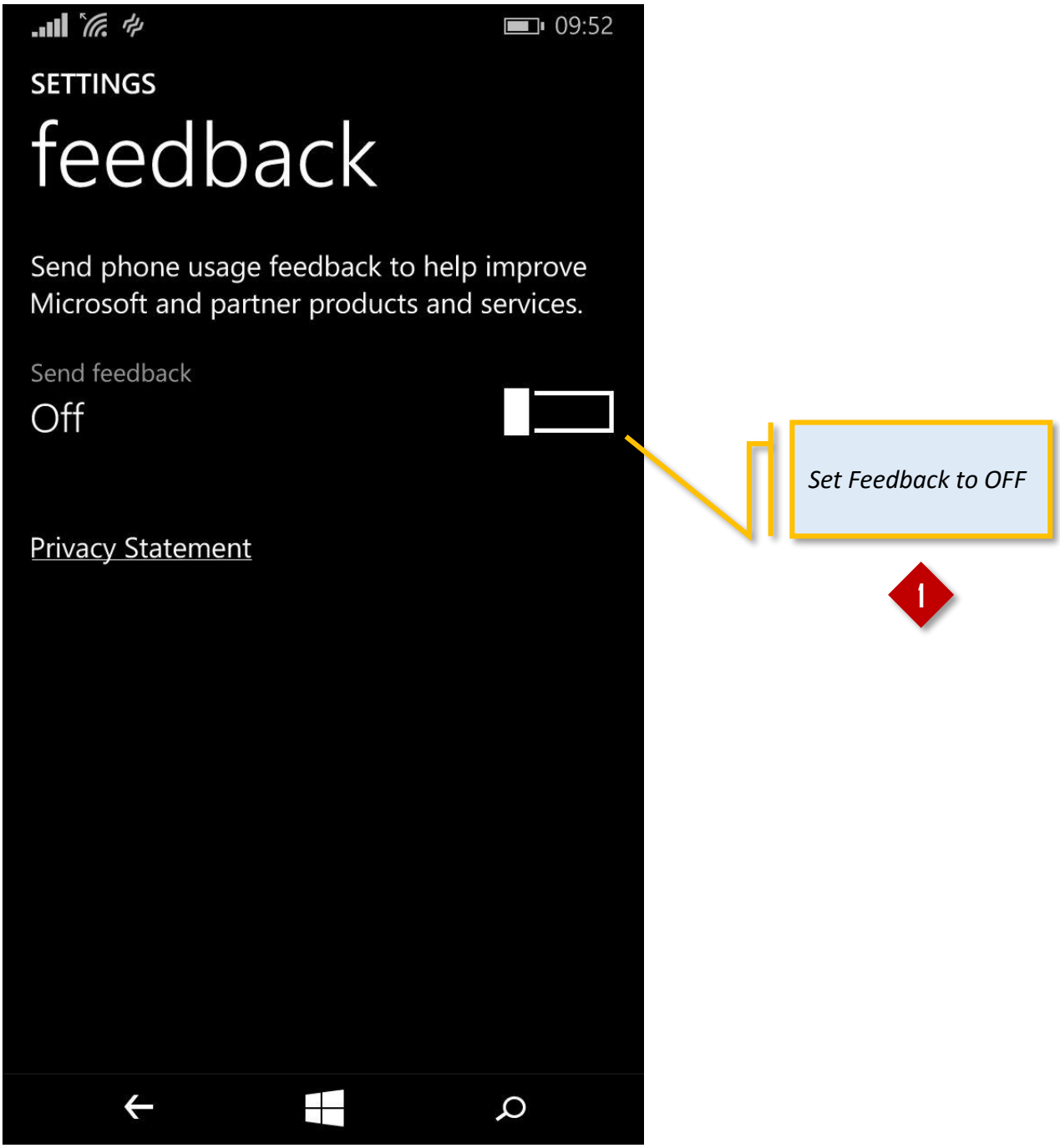
Advertising ID



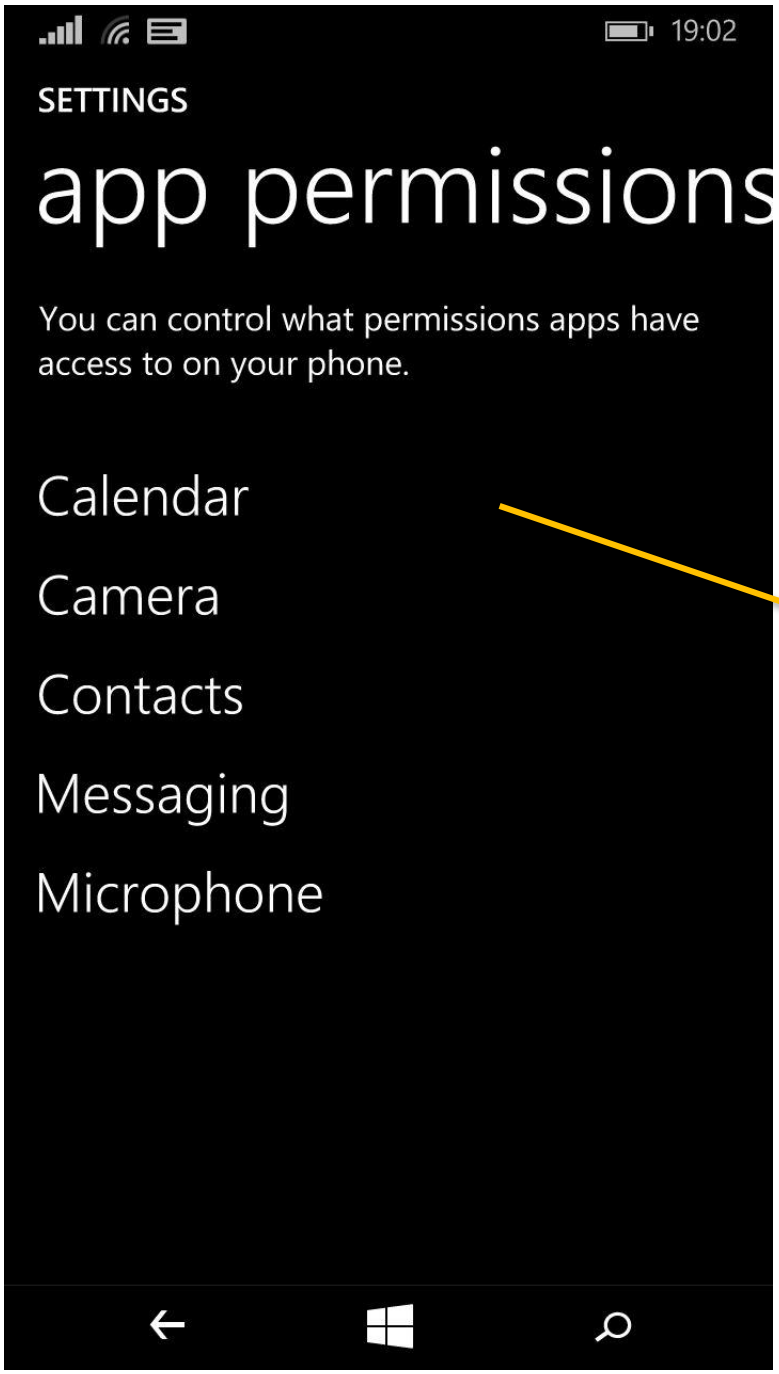
Set Advertising ID to OFF

1

Feedback


09:52
SETTINGS
feedback
Send phone usage feedback to help improve Microsoft and partner products and services.
Send feedback
Off
Privacy Statement
Set Feedback to OFF
1

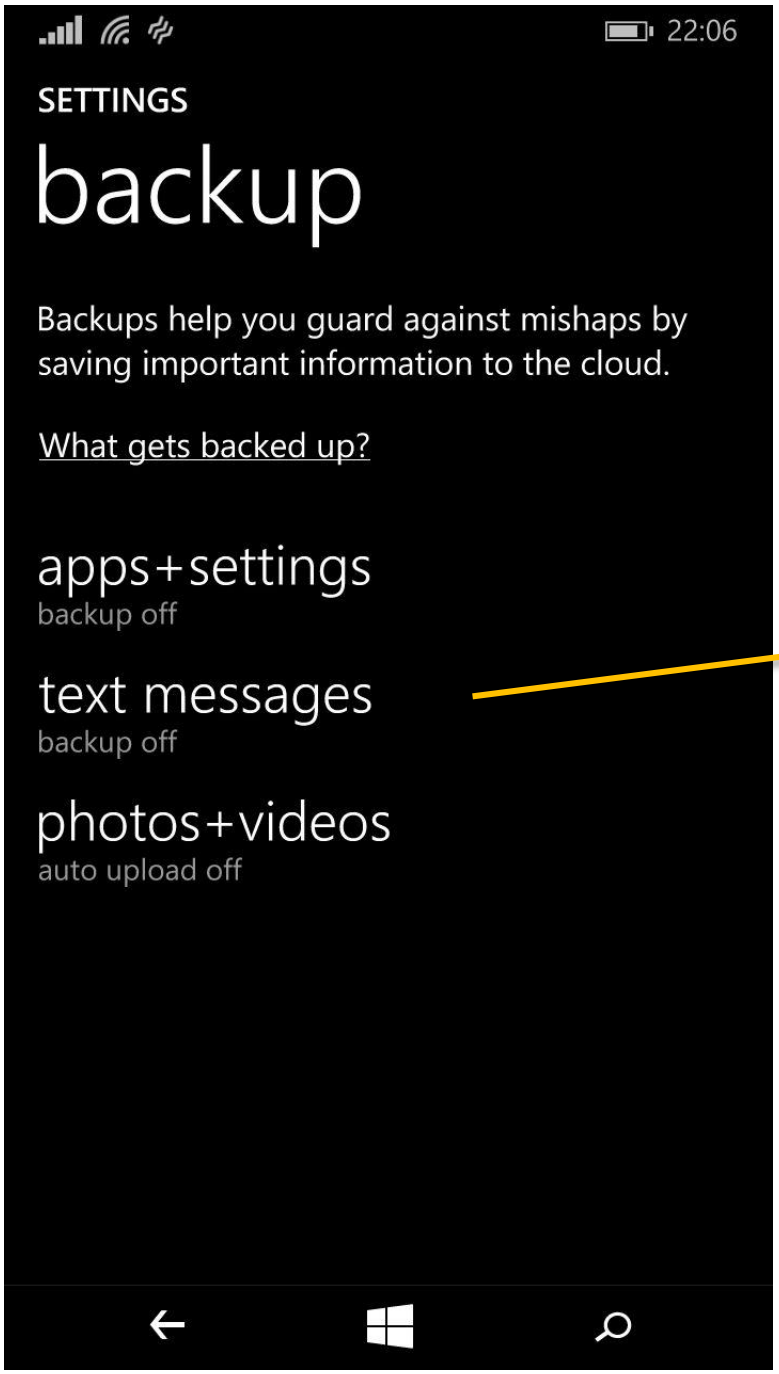
App permissions



Manage App permissions as shown in the following pages

1

Backup

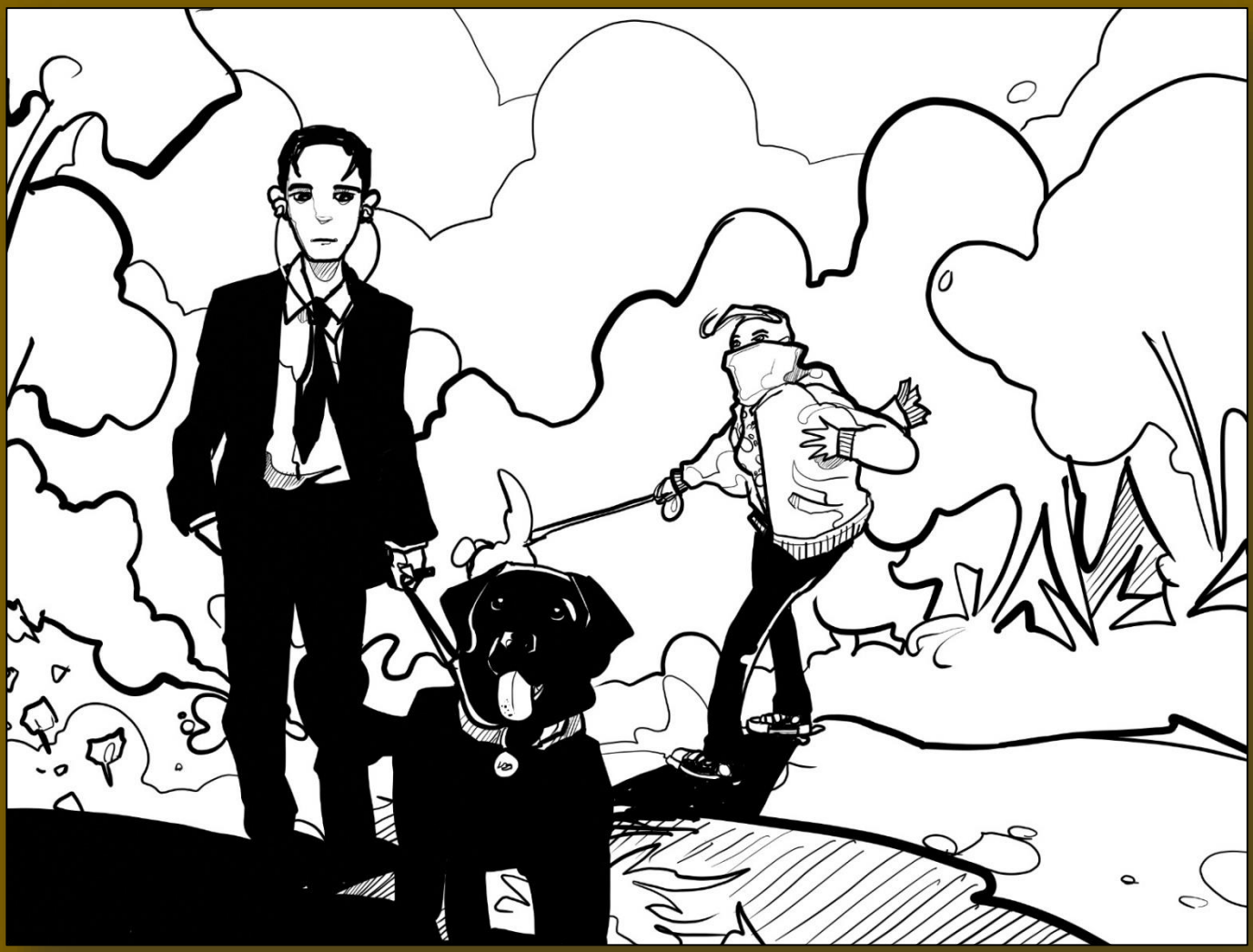


Carefully consider what, if anything, you want to backup to the Cloud

1

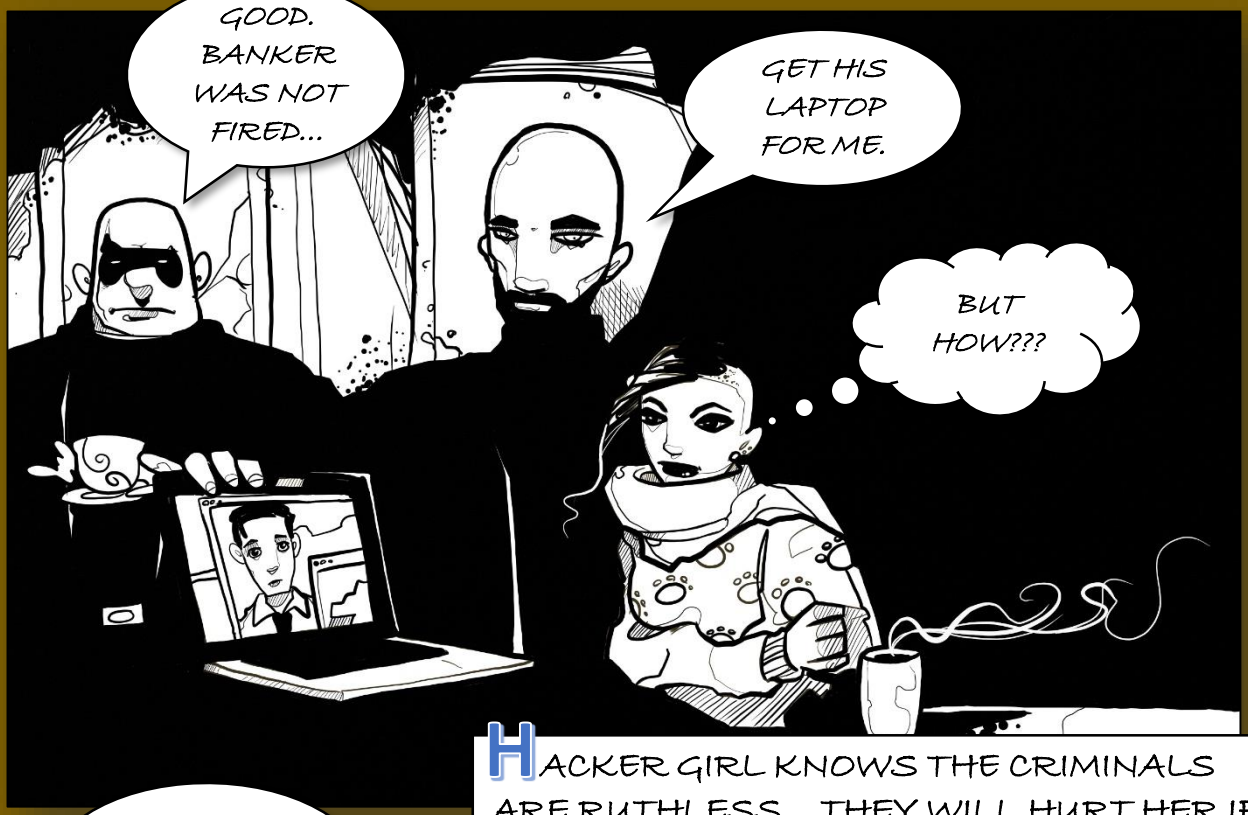
Hacker Girl Episode Two

Will you be my friend?



Copyright: The Risk Management Group
January 2016

HACKER GIRL MANAGEED TO STEAL THE BANKER'S EMAILS FOR A CRIME GANG, BUT THEY WERE NOT SATISFIED. NOW THEY WANT HER TO STEAL HIS LAPTOP FOR THEM!



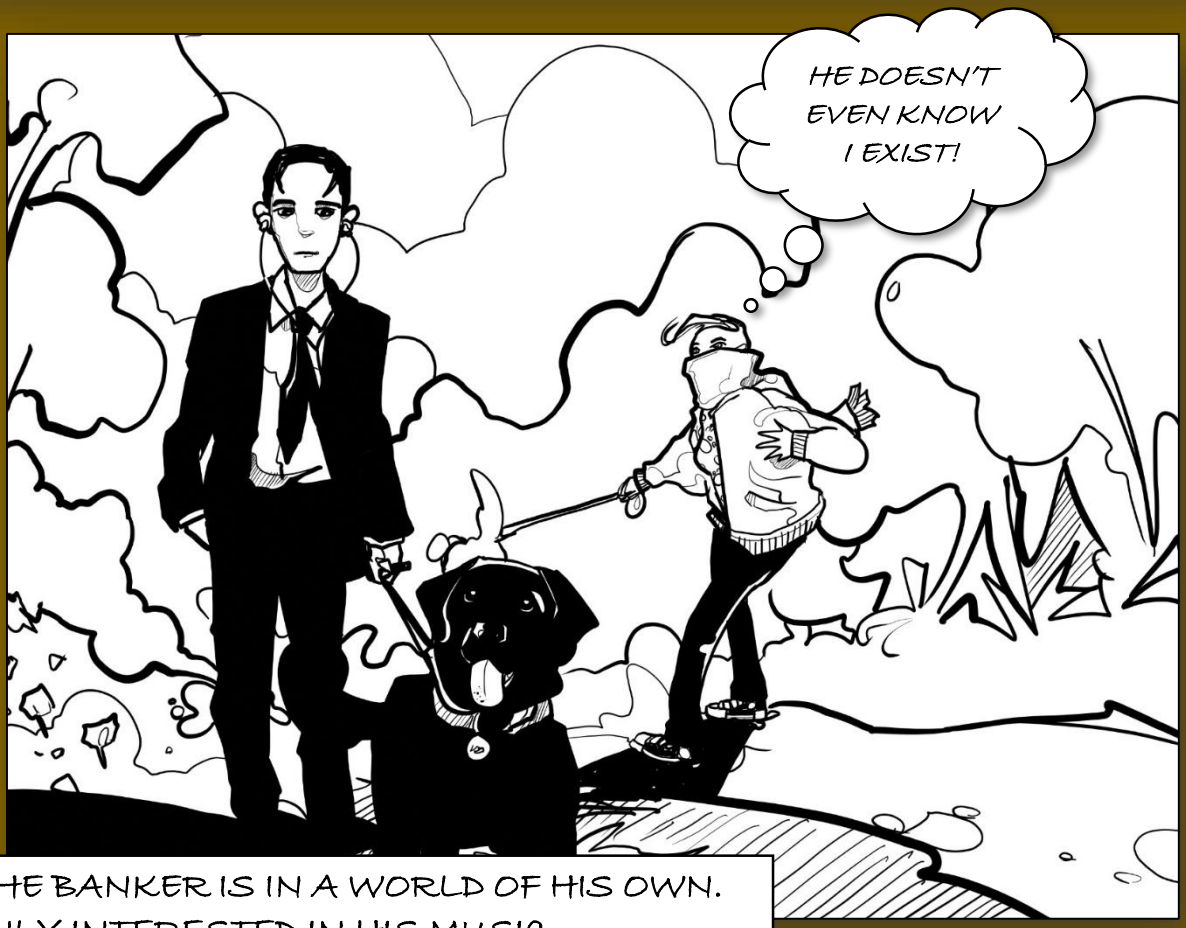
HACKER GIRL KNOWS THE CRIMINALS ARE RUTHLESS... THEY WILL HURT HER IF SHE DOESN'T DO WHAT THEY SAY.

HACKER GIRL IS ALREADY COMING UP WITH A PLAN. SHE'S RELUCTANT, BUT ACCESSING SYSTEMS AND ENGINEERING PEOPLE ARE HER KEY TALENTS; SHE CAN'T HELP BUT FEEL STIMULATED BY THE CHALLENGE...

HACKER GIRL RECALLS HER ENCOUNTER WITH THE BANKER IN THE PARK. SO, SHE KNOWS HE'S A DOG LOVER...

MEANWHILE, THE GANG MAKES AN OVERSEAS CALL.

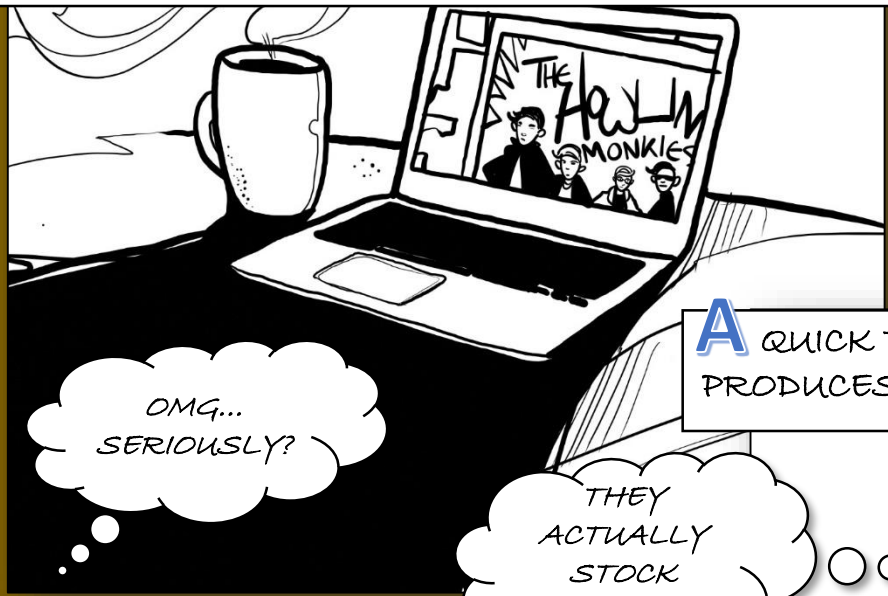
HACKER GIRL SPENDS A LOT OF TIME WALKING HER DOG, KEYSTROKE, IN THE PARK NEAR HER HOME. OVER THE NEXT FEW DAYS, SHE SPOTS THE BANKER SEVERAL TIMES AND SMILES AT HIM AS THEY PASS...



BUT THE BANKER IS IN A WORLD OF HIS OWN. HE'S ONLY INTERESTED IN HIS MUSIC.

HACKER GIRL ALSO FREQUENTS THE BANKER'S FAVOURITE CAFÉ, CLOSE TO HIS OFFICE...
NOPE – NADA. MR MUSIC IS ON ANOTHER PLANET!
THE CRIMINALS ARE STARTING TO GROW IMPATIENT...
OH BOY... HMMM... MUSIC. I WONDER...
TRY HARDER OR... YOU KNOW WHAT!
HACKER GIRL DECIDES TO TRY A DIFFERENT APPROACH.

A SEARCH ON FACEBOOK REVEALS THAT THE BANKER LIKES AN INDIE MUSIC BAND CALLED THE HOWLING MONKIES...



A QUICK TRIP TO THE SHOPS PRODUCES RESULTS...

THAT LUNCHTIME HACKER GIRL ACCIDENTALLY DROPS THE CD...

AS THE BANKER SQUATS TO PICK UP THE CD, HE READS THE LABEL. HE FREEZES IN SURPRISE...

REALLY?

THE HOWLING MONKIES?!?

FINALLY, A BREAKTHROUGH!

GOTCHA!

YOU LIKE THE MONKIES?

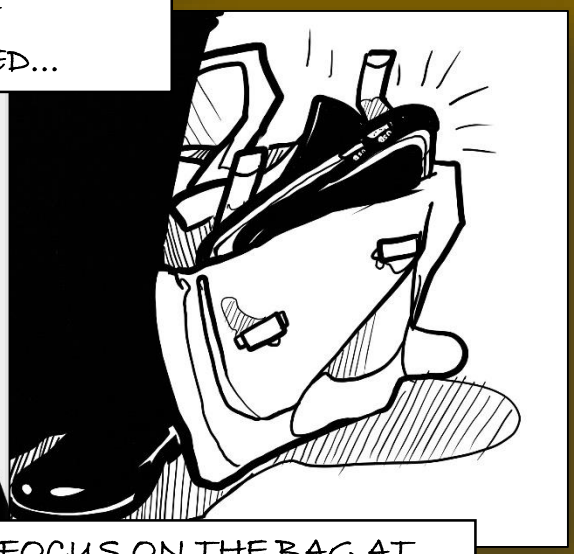
TOO GOOD TO BE TRUE!

I LOVE THEM!

BUT IF IT'S TOO GOOD TO BE TRUE, IT PROBABLY ISN'T...

A FRIENDLY COFFEE FOLLOWS...

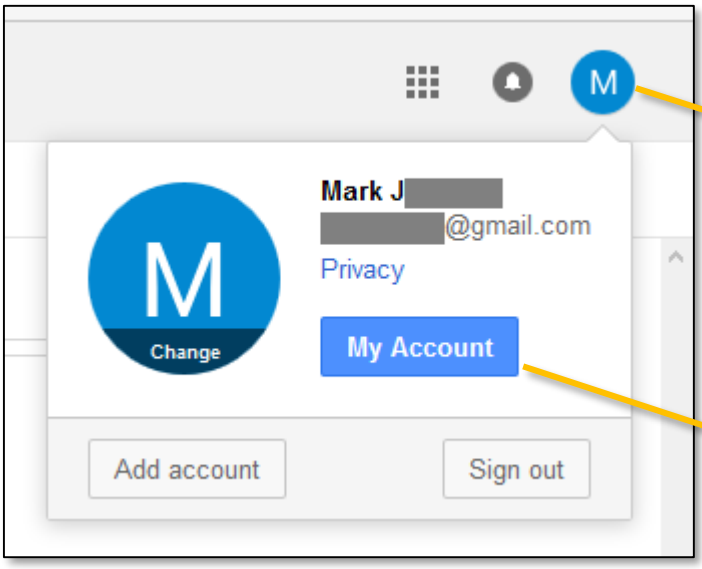
SHE IS ACTUALLY ENJOYING HERSELF, BUT HACKER GIRL KNOWS SHE'S BEING WATCHED...



SHE NEEDS TO FOCUS ON THE BAG AT THE BANKER'S FEET, BUT HOW WILL HACKER GIRL GET IT? STAY TUNED FOR MORE...

Gmail 2-factor authentication

Accessing security

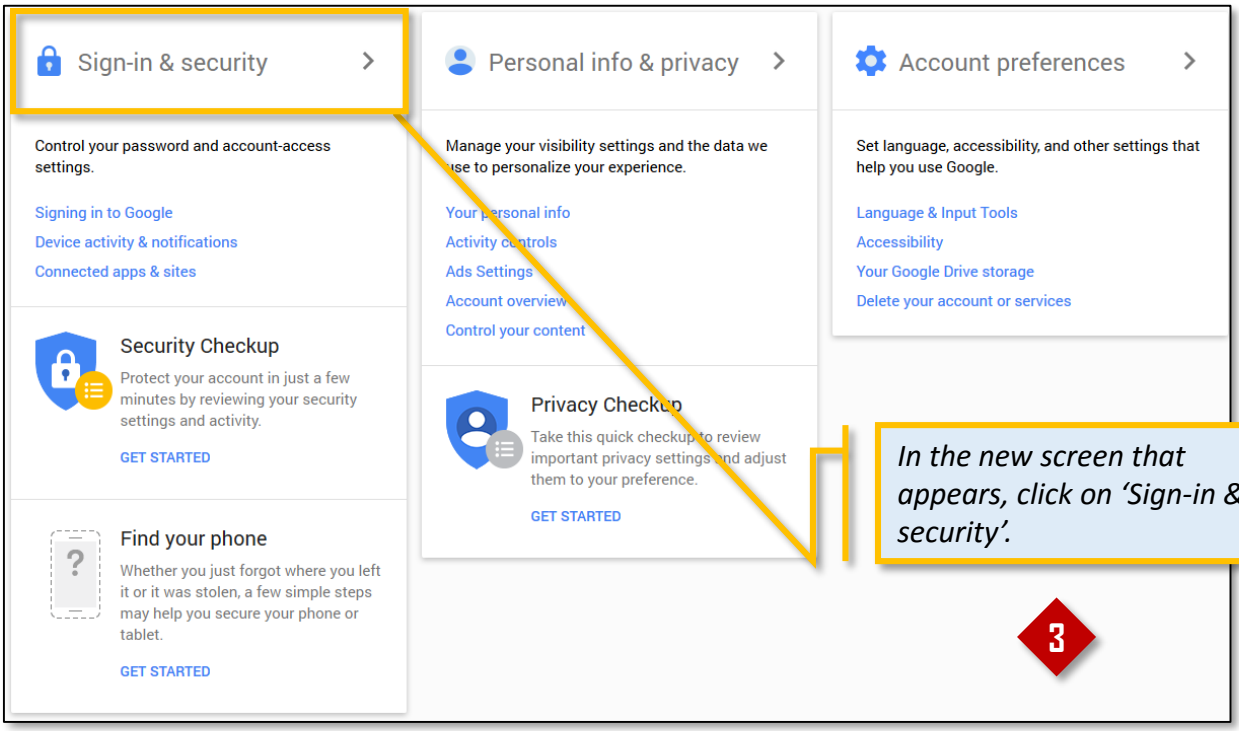


1

Click on your avatar icon in the top right corner of the screen.

2

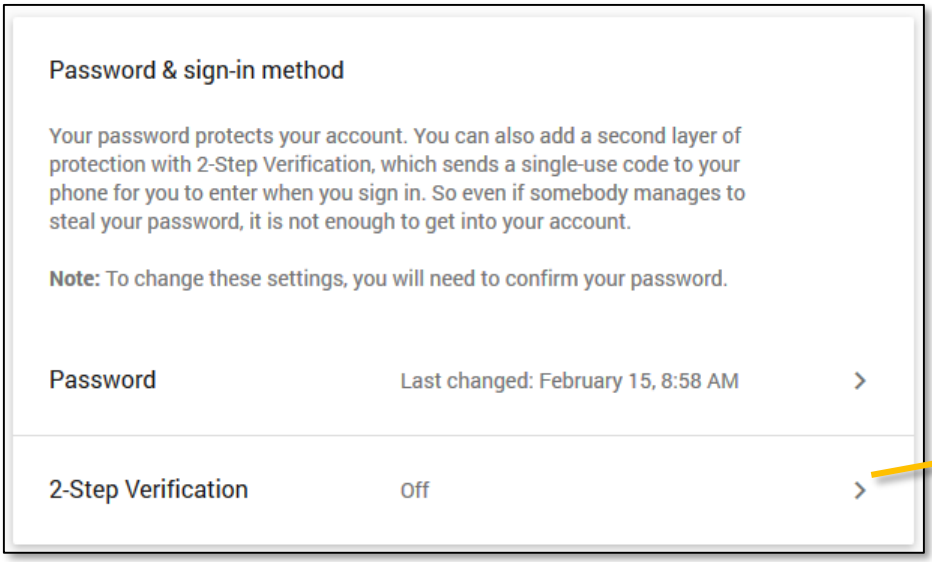
Now click the 'My Account' button.



In the new screen that appears, click on 'Sign-in & security'.

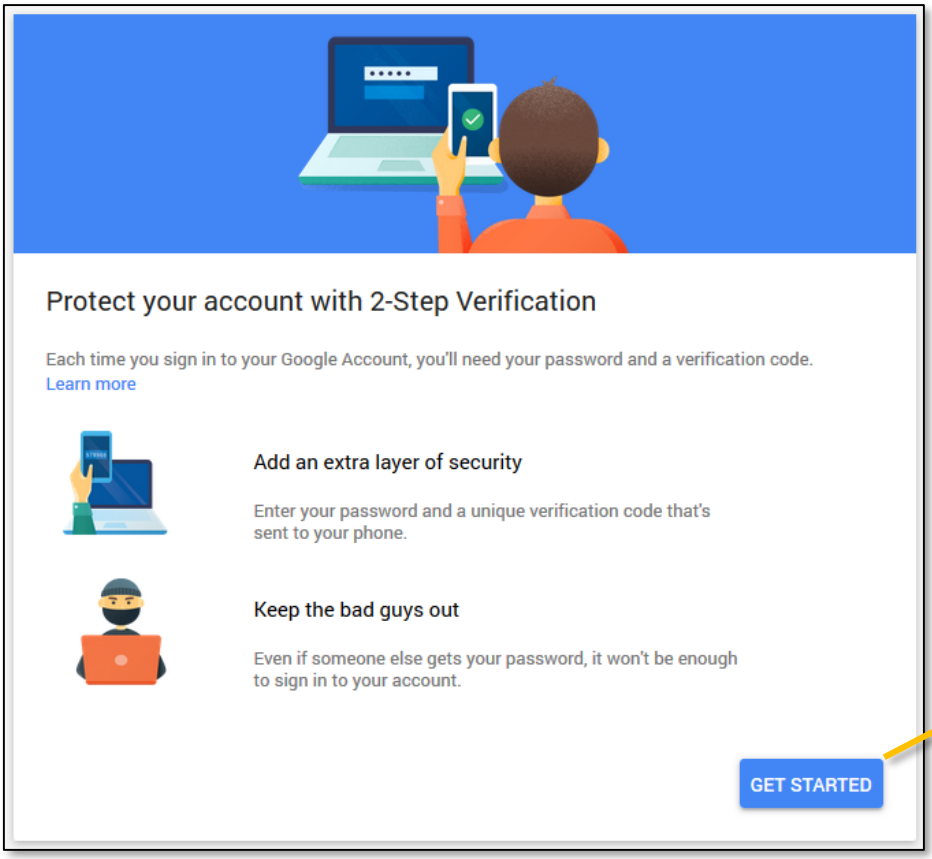
3

Choosing 2-step verification ('authentication')



1

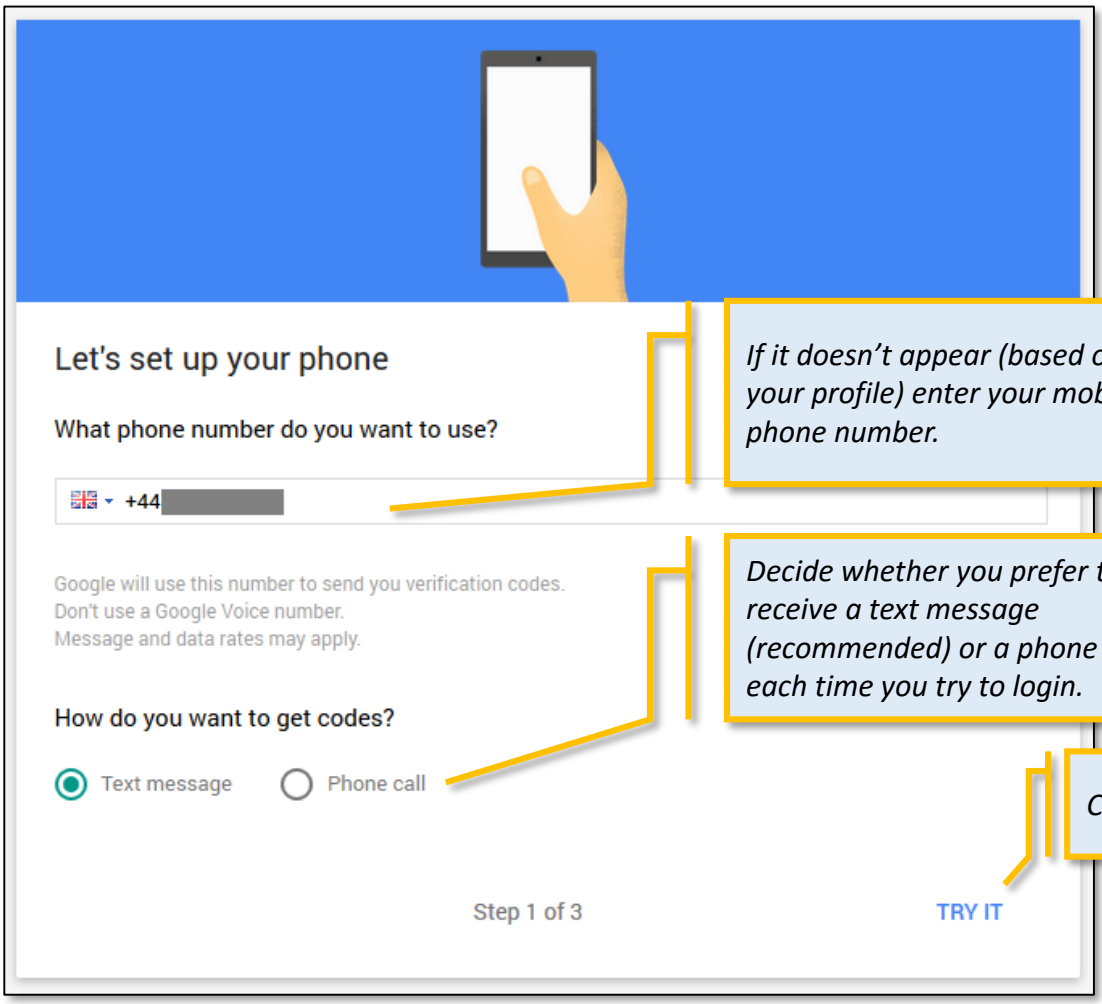
On the next screen that appears, click on '2-Step Verification'.



2

Now click the 'Get Started' button.

Configure 2-step verification



If it doesn't appear (based on your profile) enter your mobile phone number.

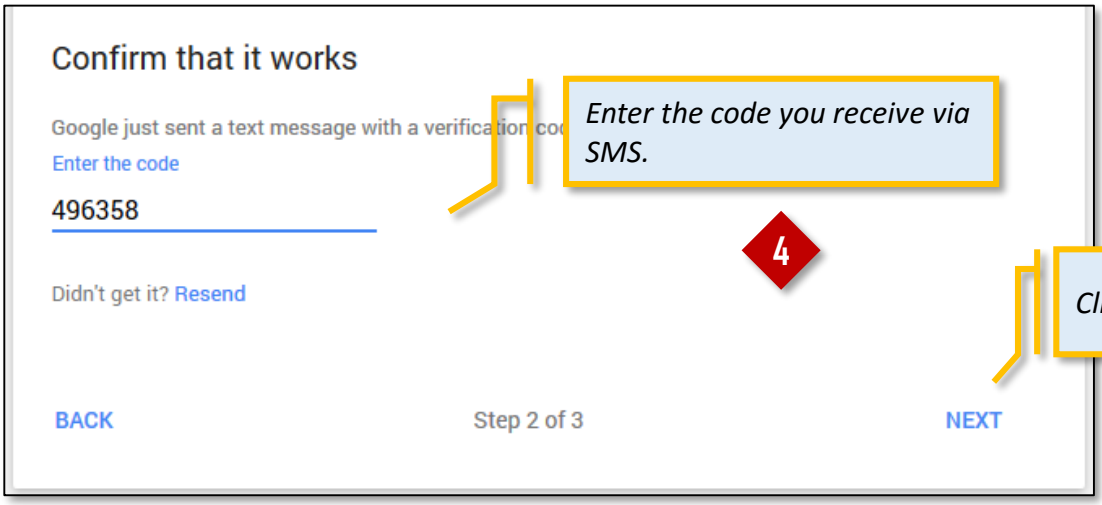
1

Decide whether you prefer to receive a text message (recommended) or a phone call each time you try to login.

2

Click 'Try It'.

3



Enter the code you receive via SMS.

4

Click 'Next'.

5

Configure 2-step verification

It worked! Turn on 2-Step Verification?

Now that you've seen how it works, do you want to turn on 2-Step Verification for your Google Account [redacted]@gmail.com?

BACK Step 3 of 3 TURN ON

If successful, you will see this acceptance dialogue. Click 'Turn On' to proceed.

1

2

Finally, you will see this confirmation dialogue.

If you change your mind about 2-step validation, click here to turn it off.

3

2-Step Verification is ON since Jun 24, 2016 TURN OFF

Your second step

After entering your password, you'll be asked for a second verification step.

Voice or text message (Default)

07[redacted]

Verification codes are sent by text message.

Set up alternative second step

Set up at least one backup option so that you can still sign in if you don't have your phone with you.

4

Backup verification options will be listed below the confirmation text.

Snapchat

Privacy & settings

Click here to enter Setting options

Add friends by using Snapcode

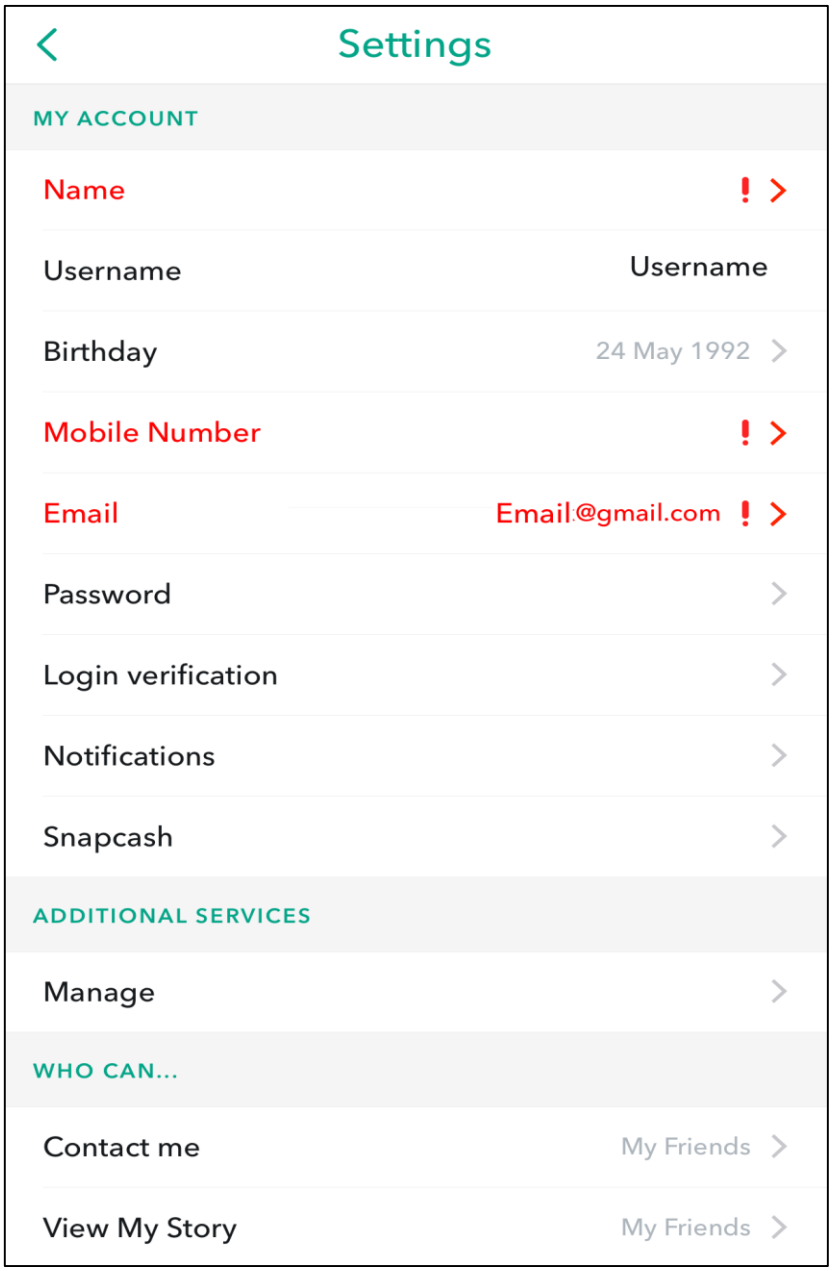
Check who has recently added you as a friend

Add friends by username, from your address book, by Snapcode or by 'nearby users'.

Click here to check your friend list

Security: Access & edit

1. *Don't give away your real name, mobile number, D.O.B or your official email address.*
2. *Avoid creating a Snapcash account*
3. *Hide the access to your profile by selecting 'My friends' in the **WHO CAN… Contact me** & **View My Story** sections.*

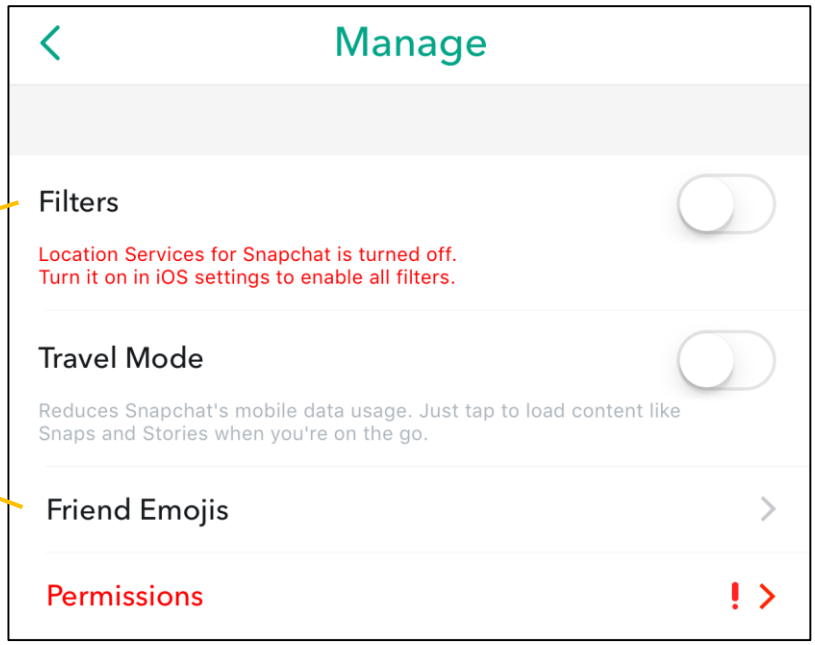


Security: Manage your privacy

1. *Click the **manage** option in the **Additional services** section.*

2. *Switch off your location services for Snapchat (**Filters** tab).*

3. *View the Snapchat Emojis used in the profile.*

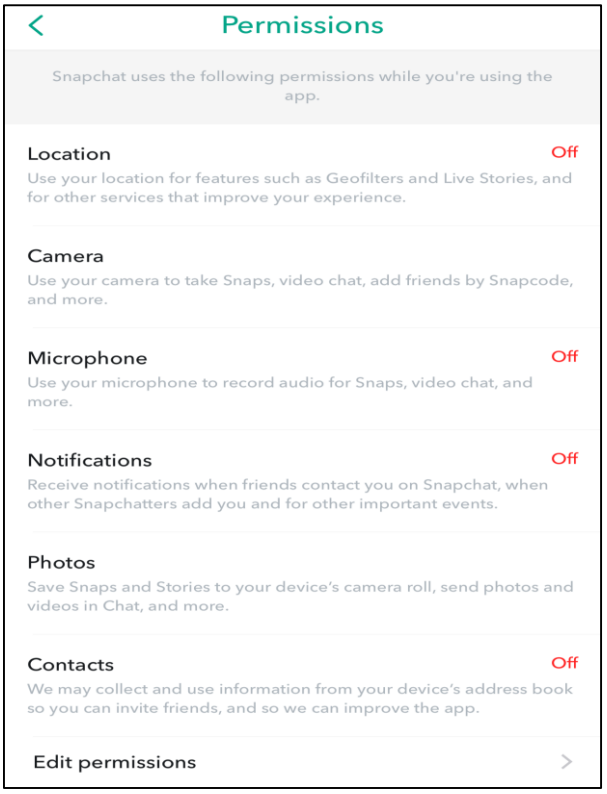


Security: Permissions

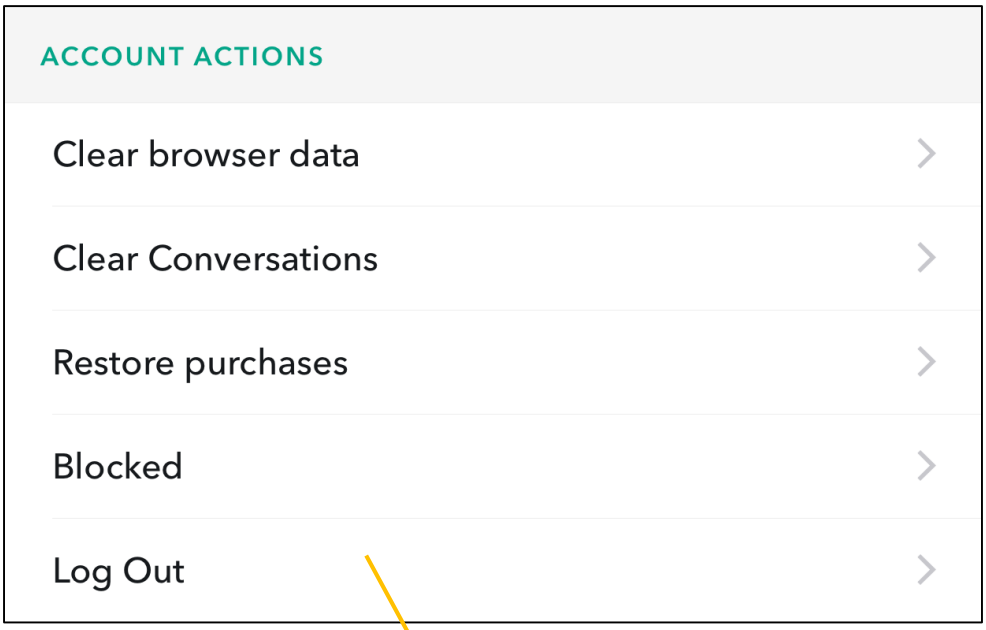
Apply your settings as shown in the image.

Switch off location, microphone and access to your contact list.

By clicking "Edit Permissions" you will go to your phone settings.



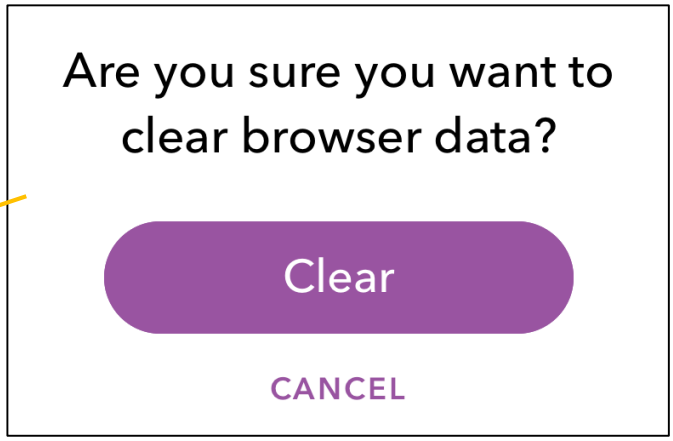
Security: Account actions



*Go back to your settings and choose the **Account Actions** tab.*

Here you can clear your browser data and conversations, block selected people, or log out from the account.

Security: Deleting data



1. *Click on clear your browser data tab and you will see this pop up window.*

2. *Choose the **Clear** option to delete your browser data from the app.*

Credits

Conceived and commissioned by Andrew Beet, National Policing DCG Futures Group
Written and produced by Mark Johnson, TRMG
OSINT Consultant, Esti Medynska, TRMG
Hacker Girl Artwork produced on commission by Nic Brennan

Disclaimer

Social Media, Browser, App and device security settings change constantly. Check your settings and options regularly to ensure that you are using the highest levels of security.

Neither the NPCC, nor TRMG, accept responsibility for any loss or breach arising from the use of this document. The document represents best efforts to encapsulate the common body of knowledge existing at the time of writing and is a guide to the security features available to users of online services and smartphones. This is not an operational guide and the reader is advised to consult his or her respective organisation for operational guidance on security and best practice.

Issued by the National Policing DCG Futures Group
DCGFutures@met.police.uk