



# Contents

<b>Foreword</b>	<b>03</b>
<i>The Case of the Naïve Banker</i>	<b>04</b>
<b>Social Media</b>	<b>08</b>
10 Do's and Don'ts	<b>09</b>
Facebook	<b>13</b>
LinkedIn	<b>20</b>
Twitter	<b>27</b>
Google+	<b>36</b>
<i>The Case of the Facebook Friends</i>	<b>42</b>
<b>Browsers</b>	<b>52</b>
Opera	<b>53</b>
Chrome	<b>59</b>
Firefox	<b>67</b>
Internet Explorer	<b>70</b>
<b>Smartphones</b>	<b>77</b>
Android	<b>78</b>
Blackberry	<b>86</b>
iOS	<b>90</b>
Windows	<b>99</b>
<b>Credits</b>	<b>107</b>

# 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.



**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 1

# The Case of the Naïve Banker



Created by Mark Johnson  
Illustrated by Nic Brennan

Copyright: The Risk Management Group  
January 2016

**Criminals regularly use social media as a reconnaissance tool.**

**H**ACKER 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...



**S**HE 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.



**A**FTER SEVERAL TRIES, SHE FINALLY SPOTS HER MAN.

THERE HE IS!

I'LL TRY THIS NEW WIFI HIJACKING TOOL...

**H**ACKER GIRL USES A SPECIAL TOOL\* TO HIJACK THE BANKER'S WIFI CONNECTION.

**T**HE BANKER'S IS USING A PUBLIC WIFI HOTSPOT DURING HIS BREAK TO SEND UNENCRYPTED EMAILS TO CLIENTS.

*\*Modelled on a popular toolset...*

**Zap!**

BINGO!!!



**B**ACK AT HOME, HACKER GIRL UPLOADS THE STOLEN EMAILS AND ATTACHMENTS TO THE CRIME GANG...



**T**HE GANG WANTS MORE FROM HER...

**M**EANWHILE, EOB CLIENTS HAVE BEEN DEFRAUDED AND BANK STAFF ARE BEING FIRED.



**H**ACKER GIRL HAS A CHANCE ENCOUNTER WITH HER EOB TARGET IN THE PARK. HE LOOKS VERY DEJECTED...



**W**HAT WILL HACKER GIRL DO NEXT? CAN SHE MAKE AMENDS, OR WILL SHE CONTINUE TO WORK FOR THE CRIME GANG? STAY TUNED FOR MORE IN OUR FEBRUARY ISSUE...

# 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.

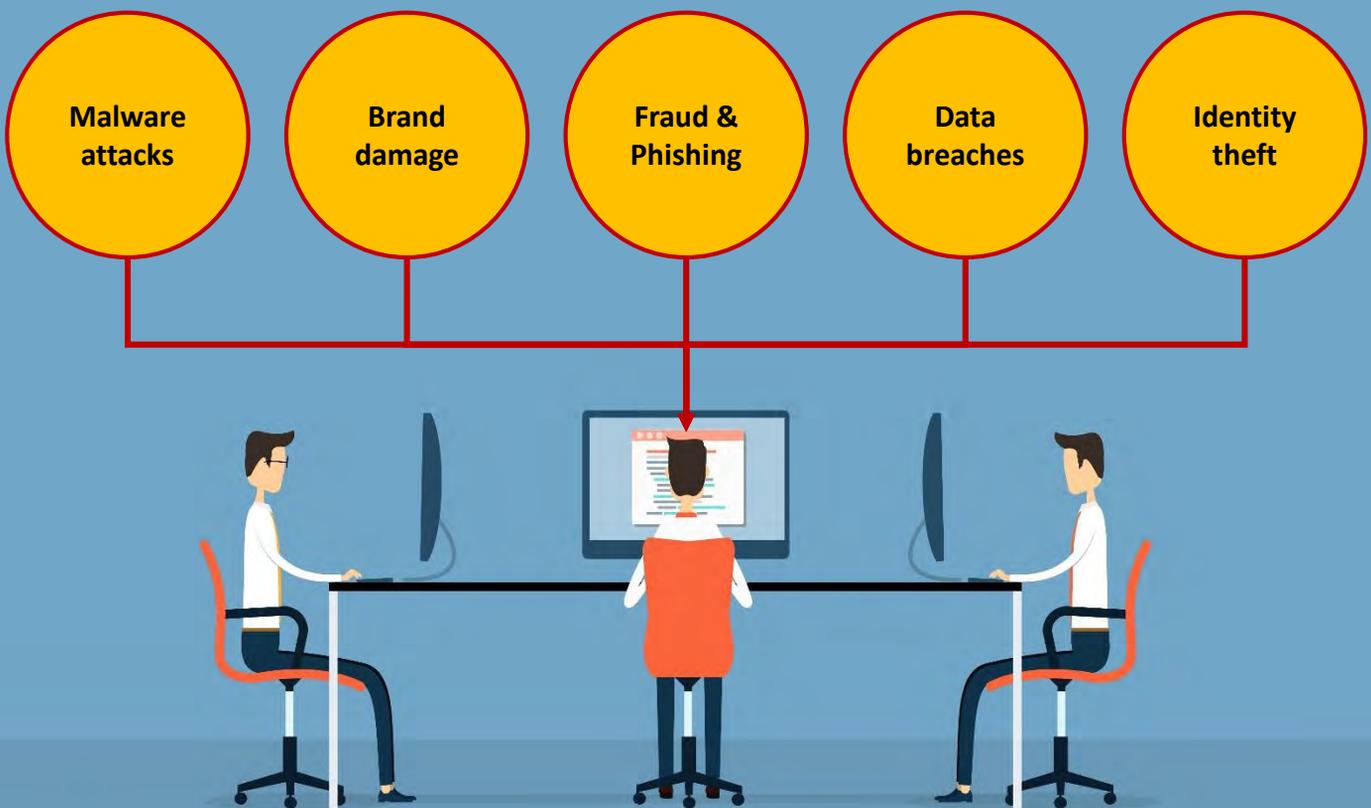
This section of the guide provides some high level advice about secure social media practices, as well as details on how you can adjust your security settings to better protect yourself and your colleagues online.

# 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

Online activity is recorded by visited sites, or by spyware on infected devices.

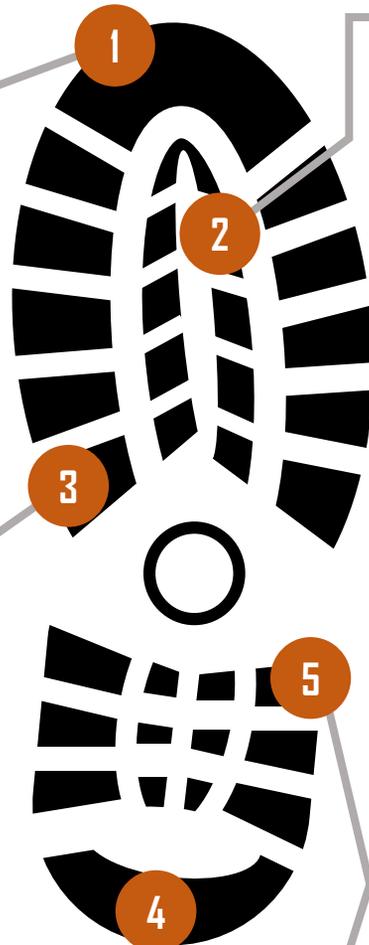
Geo-location data, check in and travel updates on social media and other sites may be published online.

Examination of email headers & other records can reveal IP your address.

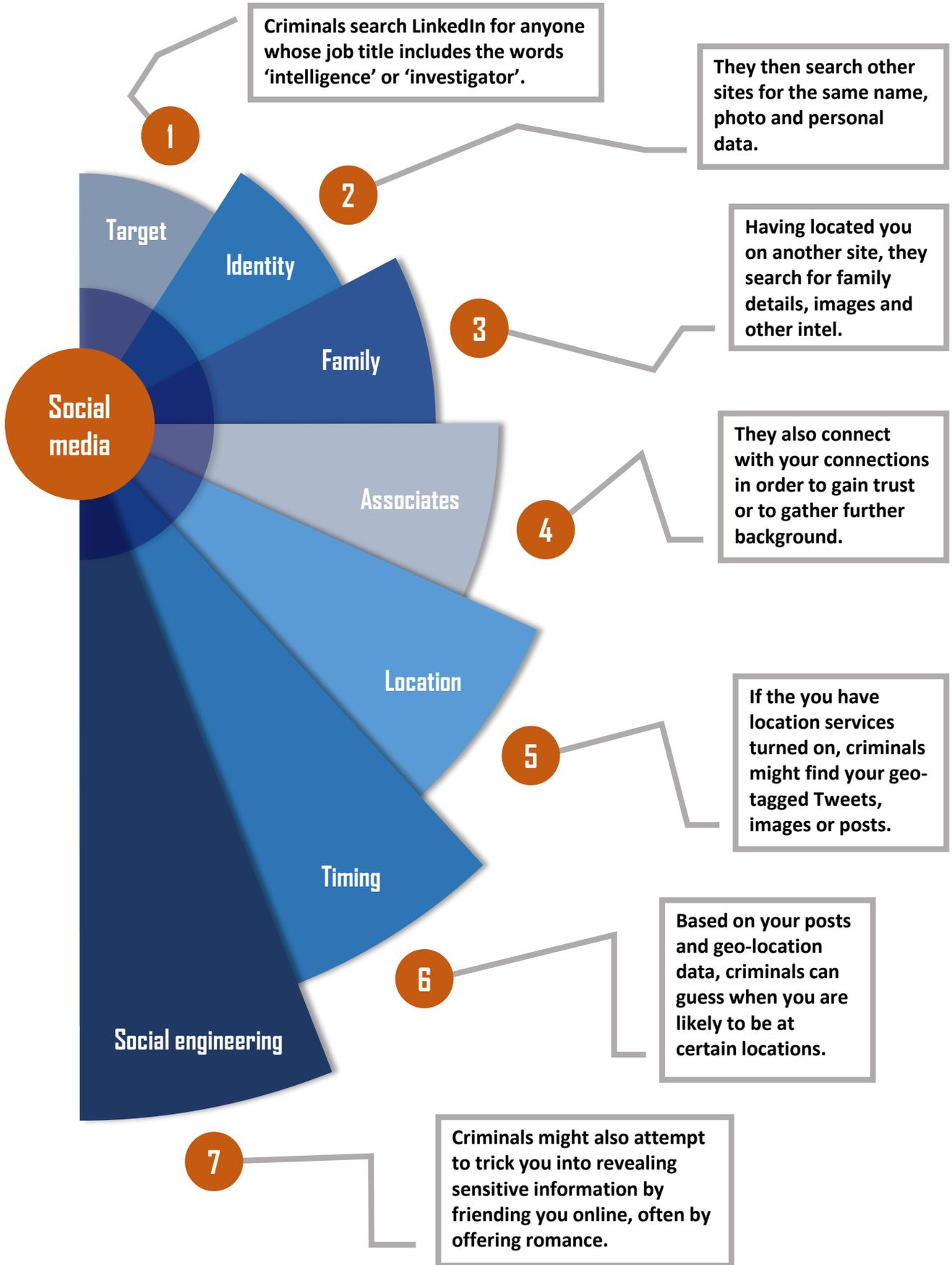
Insecure network connections, such as some public WiFi services, can expose you to interception.

'Whois' information on registered domains listed in social media profiles can be freely obtained and often includes home addresses for small business or personal websites.

...and this is only the tip of the iceberg!



# How a criminal might investigate you...



# 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

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	<a href="#">End Activity</a>
Location	Amsterdam, Netherlands (Approximate)	
Device Type	Firefox on Windows 8	

**Facebook for iPhone (1) ▲**

**Messenger (2) ▲**

**Facebook for iPad (1) ▲**

**1**

Review all sessions that Facebook regards as active.

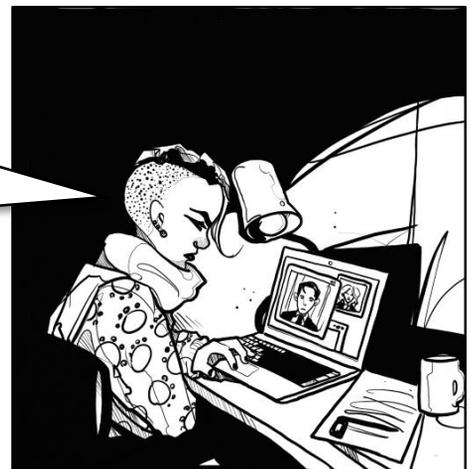
**3**

Check your active mobile device and Messenger sessions as well.

**2**

Click to end any active sessions

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

*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.

*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](https://www.facebook.com/help/delete_account)*

# Privacy

1

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

**Privacy Settings and Tools**

<b>Who can see my stuff?</b>	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
<b>Who can contact me?</b>	Who can send you friend requests?	Friends of Friends	Edit
<b>Who can look me up?</b>	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 ▼



Sites may revert your settings to the defaults (which are often less than secure) when they perform updates. Check your settings regularly!

# 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](mailto:DCGFutures@met.police.uk)) for the latest version of this guide.

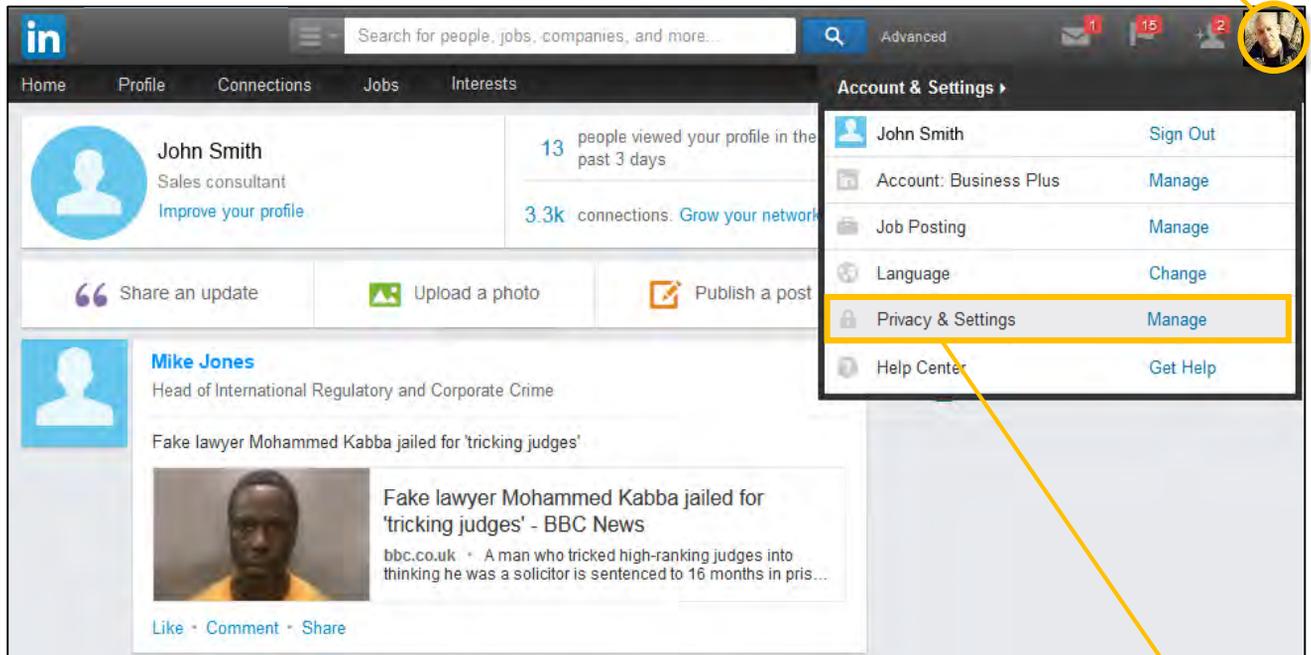
# Secure LinkedIn



*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

**4** Now click here

John Smith  
Member since: January 12, 2006

Primary Email [Change/Add](#)  
js12345@hotmail.com

Phone numbers [Add/remove](#)

Your active sessions  
• [See where you're signed in](#)

# Security: Active sessions

*Review all sessions that LinkedIn regards as current.*

**1**

*Click to end any active sessions*

**2**

**You're currently signed into 5 sessions**

Here's a list of all the places you're signed in to LinkedIn right now. You can see details about each session, sign out of individual sessions, or sign out of everywhere at once.

Current session

Details	
Now	London, United Kingdom (Approximate location) Firefox on Windows IP Address: <a href="#">?</a> 81.156.56.108 IP Address Owner: <a href="#">?</a> BT

Other active sessions (4) [Sign out of all these sessions](#)

Last accessed	Details	
1 day ago	Cambridgeshire, United Kingdom (Approximate location) LinkedIn on iOS	<a href="#">Sign out</a> ▾
6 days ago	Netherlands (Approximate location) Firefox on Windows	<a href="#">Sign out</a> ▾

# Security: Profile photo & visibility

1 *Return to Privacy & Settings*

Profile  
Communications  
Groups, Companies & Applications  
Account

Privacy Controls

- Turn on/off your news mention broa
- Turn on/off your activity broadcasts
- Select who can see your activity fee
- Select what others see when you've
- Turn on/off How You Rank
- Select who can see your connections
- Choose who can follow your updates
- Change your profile photo & visibility »**
- Show/hide "Viewers of this profile also viewed" box
- Manage who you're blocking »
- Manage who can discover you

Account & Settings ▾

- John Smith Sign Out
- Account: Business Plus Manage
- Job Posting Manage
- Language Change
- Privacy & Settings Manage**
- Help Center Get Help

Edit your public profile »  
Manage your recommendations »

2 *Select 'Change your profile photo & visibility'*

# Security: Edit your photo & visibility

1 *Click to change your photo*

Adjust Photo  
Drag the yellow square to change position and size. [Change photo.](#)

Preview  
How you appear across LinkedIn.

2 *Restrict who can see your photo*

3 *Click to delete your photo **if desired.***

Photo visible to...

- My Connections
- My Network
- Everyone

Save Cancel Delete Photo

# Security: What others see when you view them

1

Return to Security & Settings, then click here...

Select what others see when you've viewed their profile

Edit your name, loc

Turn on/off How You Rank

What others see when you've viewed their profile

Select who can see your connections

Edit your public pro

What others see when you've viewed their profile

Your name and headline (Recommended)

 **John Smith**  
Sales Consultant

London, United Kingdom | Sales

Anonymous profile characteristics such as industry and title

 **Someone on LinkedIn**

You will be totally anonymous.

**2**

Select the 3<sup>rd</sup> 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...

Save changes or Cancel

# Security: Who can see your activity feed

Return to Security & Settings and click 'Select who can see your activity feed'.

1

Privacy Controls

Turn on/off your news mention broadcasts

Turn on/off your activity broadcasts

Select who can see your activity feed

Who can see your activity feed

Your activity feed displays actions you've performed on LinkedIn. Please note that any Updates you "Share with Public" and all Posts that you publish will be visible to everyone on your activity feed regardless of this setting.

Your connections

Everyone

Your network

Your connections

Only you

**2**

Based on your role, choose either 'Your connections' or 'Only you', then click 'Save changes'.

Cancel

# Security: who can see your connections

Now go back and click 'Select who can see your connections'.

[Select who can see your connections](#)

[Choose who can follow your updates](#)

[Change your profile photo & visibility »](#)

Who can see your connections

1

## Who can see your connections

Select who can see your list of connections. Note: people will still be able to see connections who endorse you and connections they share with you. (Don't want your endorsements visible? Just choose to [opt out](#).)

Only you

Save changes or Cancel

To prevent your connections viewing your full list of contacts, select 'Only you', then click 'Save changes'.

2

# Security: View your applications (1)

Profile

Communications

**Groups, Companies & Applications**

Account

### Groups

[Select your group display order »](#)

[View your groups »](#)

[Set the frequency of group digest emails](#)

[Turn on/off group invitations](#)

[Turn on/off notifications when joining groups](#)

### Companies

[View companies you're following »](#)

### Applications

[View your applications »](#)

### Privacy Controls

[Turn on/off data sharing with 3rd party applications](#)

1

Return to Security & Settings and choose the **Groups, Companies & Applications** tab.

2

Now click 'View your applications'.

## Security: View your applications (2)

3

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.

### Authorized External Applications

Listed here are external partner applications to which you have granted access to your LinkedIn profile and network data. If you remove that access here, they will no longer be able to access your LinkedIn data. To re-enable them in the future, go to the application and grant access again.

	Partner Name
<input checked="" type="checkbox"/>	LinkedIn Help Center
<input checked="" type="checkbox"/>	LinkedIn for iPad
<input checked="" type="checkbox"/>	Cloze
<input type="checkbox"/>	Evernote
<input type="checkbox"/>	LinkedIn Outlook Connector
<input type="checkbox"/>	LinkedIn Mobile
<input checked="" type="checkbox"/>	LinkedIn Help Center - Customer Portal

4

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

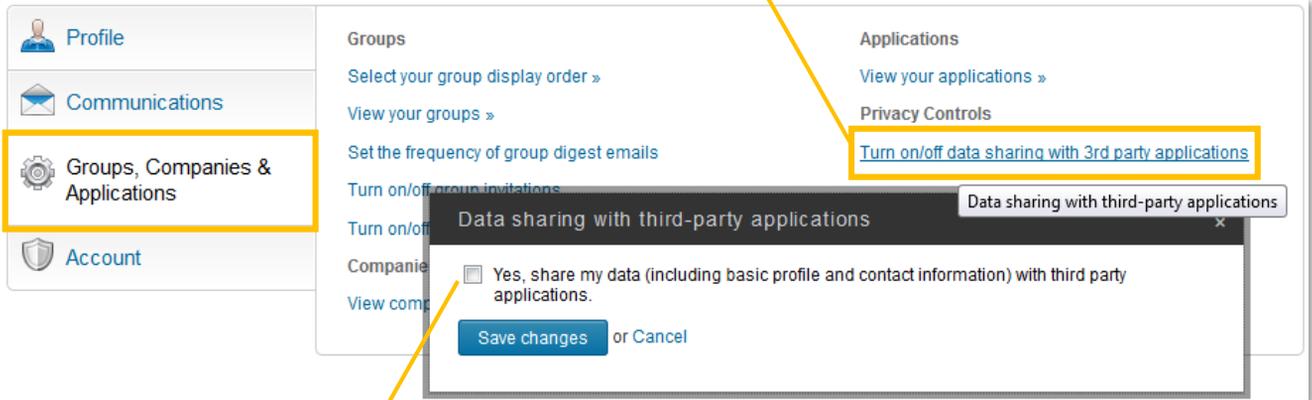
Remove or Cancel

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



# Security: Data sharing with 3<sup>rd</sup> party apps

1 Now click here...

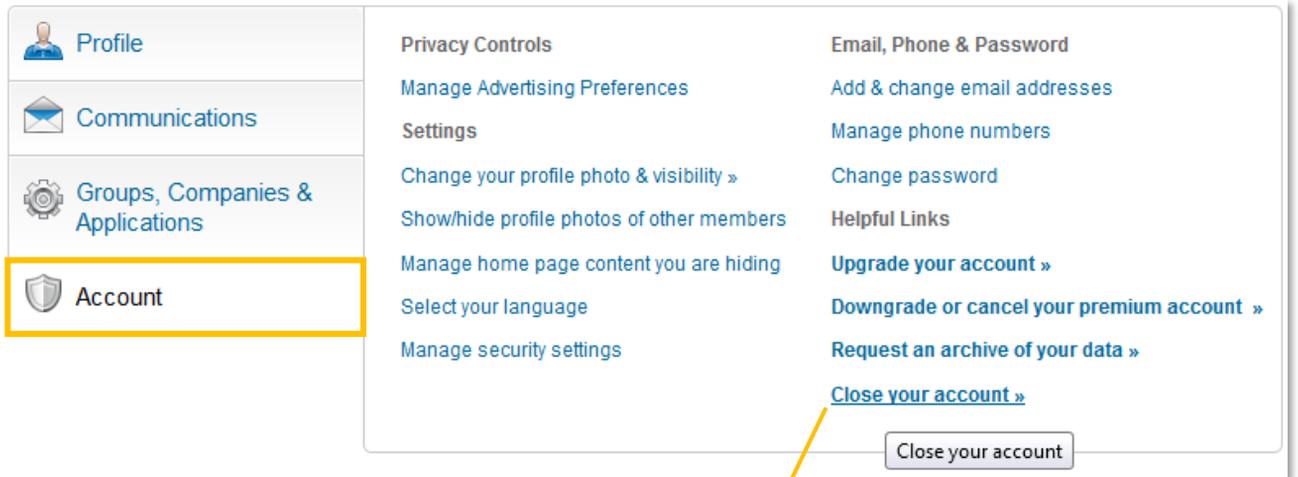


...and **deselect** data sharing.

2

**DO NOT DATA SHARE**

# Security: Closing your account



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

1

**ONLY WHEN NO LONGER NEEDED**

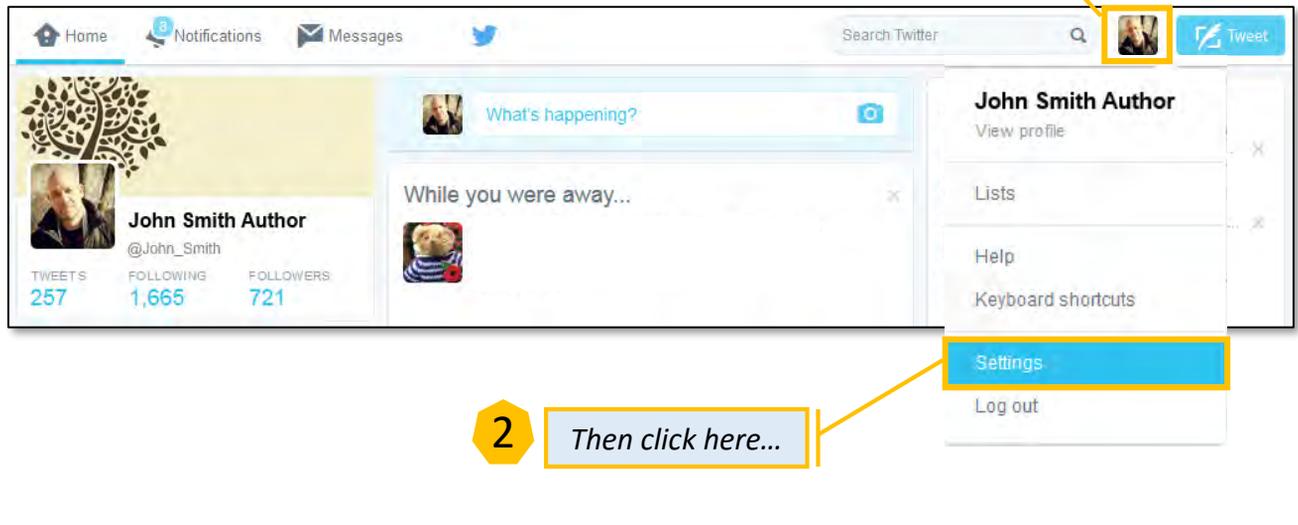
# Secure Twitter



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...



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

The screenshot shows the Twitter account settings page for a user named John Smith Author (@John\_Smith). The page is divided into two main sections: a left sidebar with navigation options and a main content area for account settings. The left sidebar includes 'Account', 'Security and privacy', 'Password', 'Cards and shipping', and 'Order history', each with a right-pointing arrow. The main content area is titled 'Account' and includes the subtitle 'Change your basic account and language settings.' Below this, there are four settings: 'Username' (js12345), 'Email' (js12345@hotmail.com), 'Language' (English), and 'Time zone' ((GMT+01:00) Casablanca). The 'Username' and 'Email' fields are highlighted with yellow boxes, and a yellow arrow points from the first callout box to the 'Username' field. Another yellow arrow points from the second callout box to the 'Email' field.

Setting	Value
Username	js12345
Email	js12345@hotmail.com
Language	English
Time zone	(GMT+01:00) Casablanca

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!**

**Security and privacy**  
Change your security and privacy settings

### Security

**Login verification**

- Don't verify login requests
- Send login verification requests to +1234567890  
After you log in, Twitter will send a SMS message with a code that you'll need to access your account.
- Send login verification requests to the Twitter app  
Approve requests with one tap when you enroll in login verification on Twitter for iPhone or Twitter for Android. [Learn more](#)

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

**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. \*

**Log in with code**

- Allow my account to log in with either a password or login code  
You are not eligible for this option because you have enabled login verification. [Learn more](#)
- Always require a password to log in to my account  
You will be asked for your password every time you log in. This means you will not be able to log in by simply receiving a login code (via SMS or email). [Learn more](#)

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

## 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

Optional

- Tweet privacy
- Protect my Tweets

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.

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

Off

- 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.

1

Apply the Privacy settings as shown...

# Password management

Now click here...

1

2

Choose a strong password\* & change it frequently.

The screenshot shows the Twitter account settings page. On the left, a navigation menu lists: Account, Security and privacy, Password (highlighted with a yellow box), Cards and shipping, Order history, Mobile, Email notifications, Web notifications, and Find friends. On the right, the 'Change password' form is visible. It includes fields for 'Current password', 'New password', and 'Verify password'. The 'New password' field contains the text 'sTr0ngP@s\$wor6'. A red warning message 'DO NOT USE THIS PASSWORD!' is displayed to the right of the 'New password' field. A 'Save changes' button is at the bottom. A yellow callout box with the number '2' points to the 'New password' field, containing the text 'Choose a strong password\* & change it frequently.' Another yellow callout box with the number '1' points to the 'Password' menu item, containing the text 'Now click here...'.

\* 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.

2

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

### 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

	<b>Silly Man 1</b> @sillyman1		Blocked
	<b>Silly Man 2</b> @sillyman2	<ul style="list-style-type: none"><li>Unblock</li><li>Report</li></ul>	Blocked
	<b>Silly Man 3</b> @sillyman3		Blocked

Advanced options ▾  
Export your list  
Import a list

# Manage your Apps

Apps >

- Design >
- Apps >**
- Widgets >
- Your Twitter data >

1

Revoke the access of any unwanted or unknown Apps.

2

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

### 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.](#)

	<b>Cloze</b> 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	<a href="#">Undo Revoke Access</a>	<a href="#">Report application</a>
--	---	------------------------------------	------------------------------------

# 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

[https://twitter.com/MarkJ\\_Books](https://twitter.com/MarkJ_Books)

Email

Email will not be publicly displayed. [Learn more.](#)

Language  ▼

Interested in helping translate Twitter? Check out the [Translation Center](#).

Time zone  ▼

## Content

Country  ▼

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

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.

**DO NOT CLICK  
UNLESS SURE!**

1

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

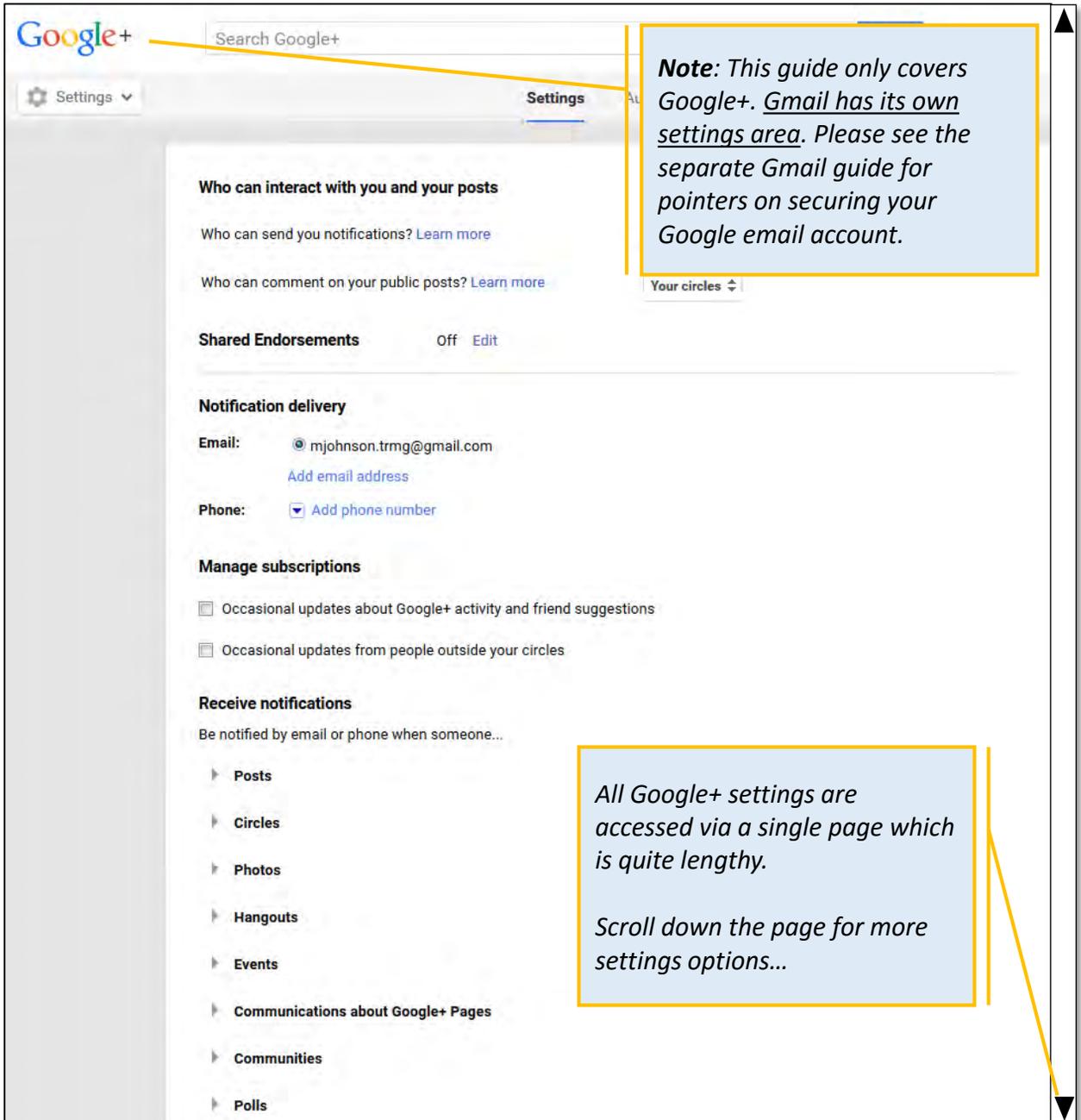
*At the time of writing, deactivated accounts remain in suspense for 30 days before Twitter permanently deletes them.*

# Secure Google+



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

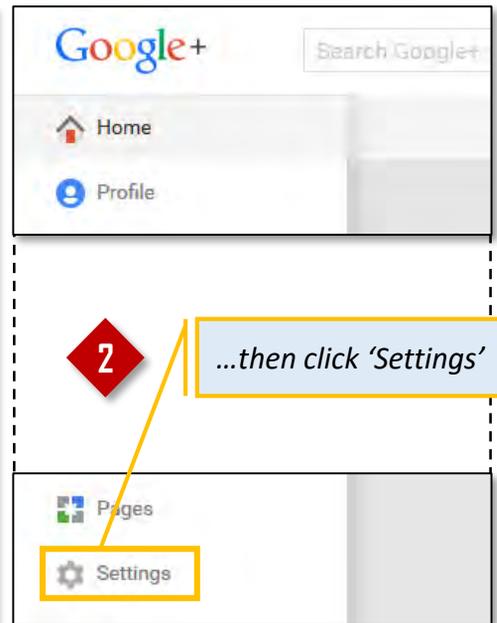
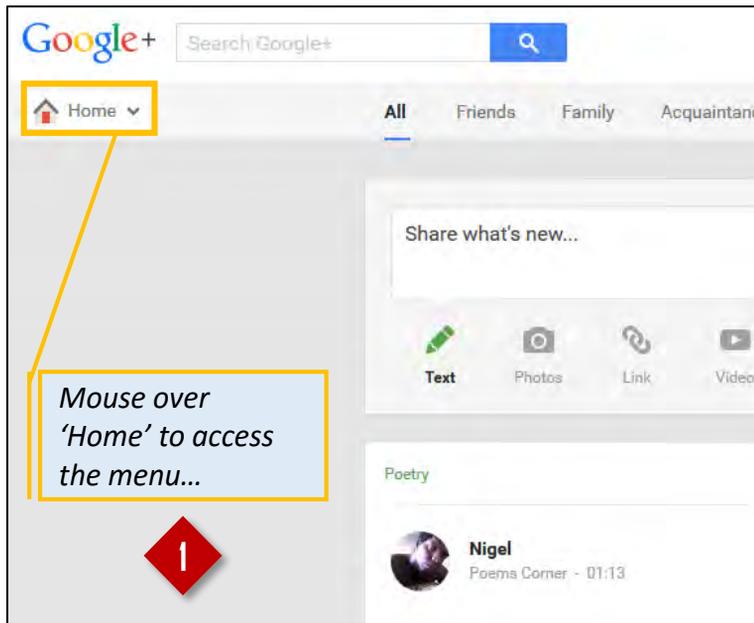
## Google+ 'Settings'

A screenshot of the Google+ Settings page. The page has a header with the Google+ logo, a search bar, and a 'Settings' dropdown menu. The main content area is divided into several sections: 'Who can interact with you and your posts', 'Shared Endorsements', 'Notification delivery', 'Manage subscriptions', and 'Receive notifications'. The 'Who can interact with you and your posts' section includes options for who can send notifications and who can comment on public posts. The 'Notification delivery' section shows email and phone notification settings. The 'Manage subscriptions' section has two checkboxes for updates. The 'Receive notifications' section has a dropdown menu for notification types. A yellow box highlights the top right of the page, and another yellow box highlights the bottom right of the page. A yellow arrow points from the top right box to the bottom right box.

**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'



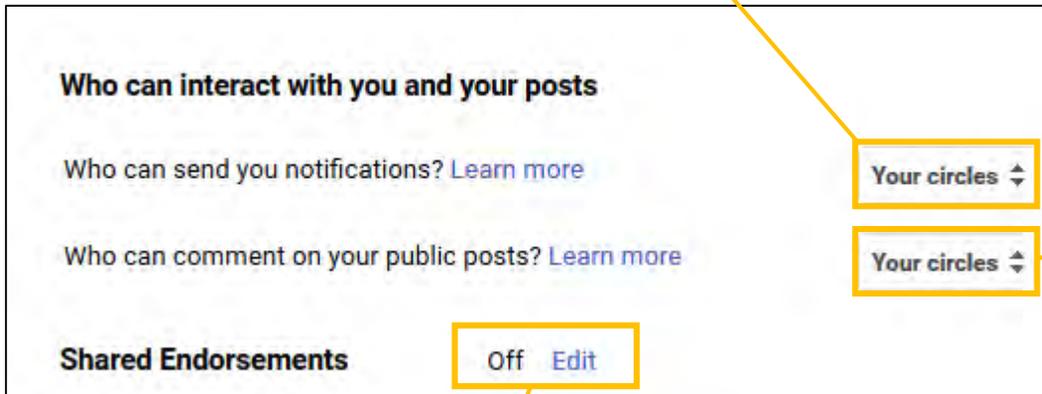
# Posts and Endorsements



Restrict who can send you notifications to 'Your circles' or 'Only you'.



Restrict who can comment on your posts.



Turn Shared Endorsements off to avoid being mentioned in Google Ads.



# 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.

3

*Turn off subscriptions.*

4

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

The screenshot shows the 'Notification delivery' section with an email field containing 'js123456@gmail.com' and a phone field with a dropdown arrow. Below is the 'Manage subscriptions' section with two unchecked checkboxes. The 'Receive notifications' section is expanded to show 'Photos' with sub-options: 'Tags you in a photo', 'Tags one of your photos', 'Suggests a profile photo for you', and 'Comments on a photo that you're tagged in'. To the right of these options is an 'Email' column with four checked checkboxes. The 'Hangouts' and 'Events' sections are partially visible at the bottom.

# 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

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

- Extended circles
- Public
- Your circles
- Only you
- Custom

Friends 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 shared with. [Learn more](#)

Cancel

Save

# Customise "Your circles"

**Click here.** 1

**Customise**

**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
- Family
- Acquaintances
- Following
- Book Reviewers
- Authors

**Think carefully about how widely you want to share your posts, photos and profile data.** 2

Cancel Save

Google Drive

**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.
- 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

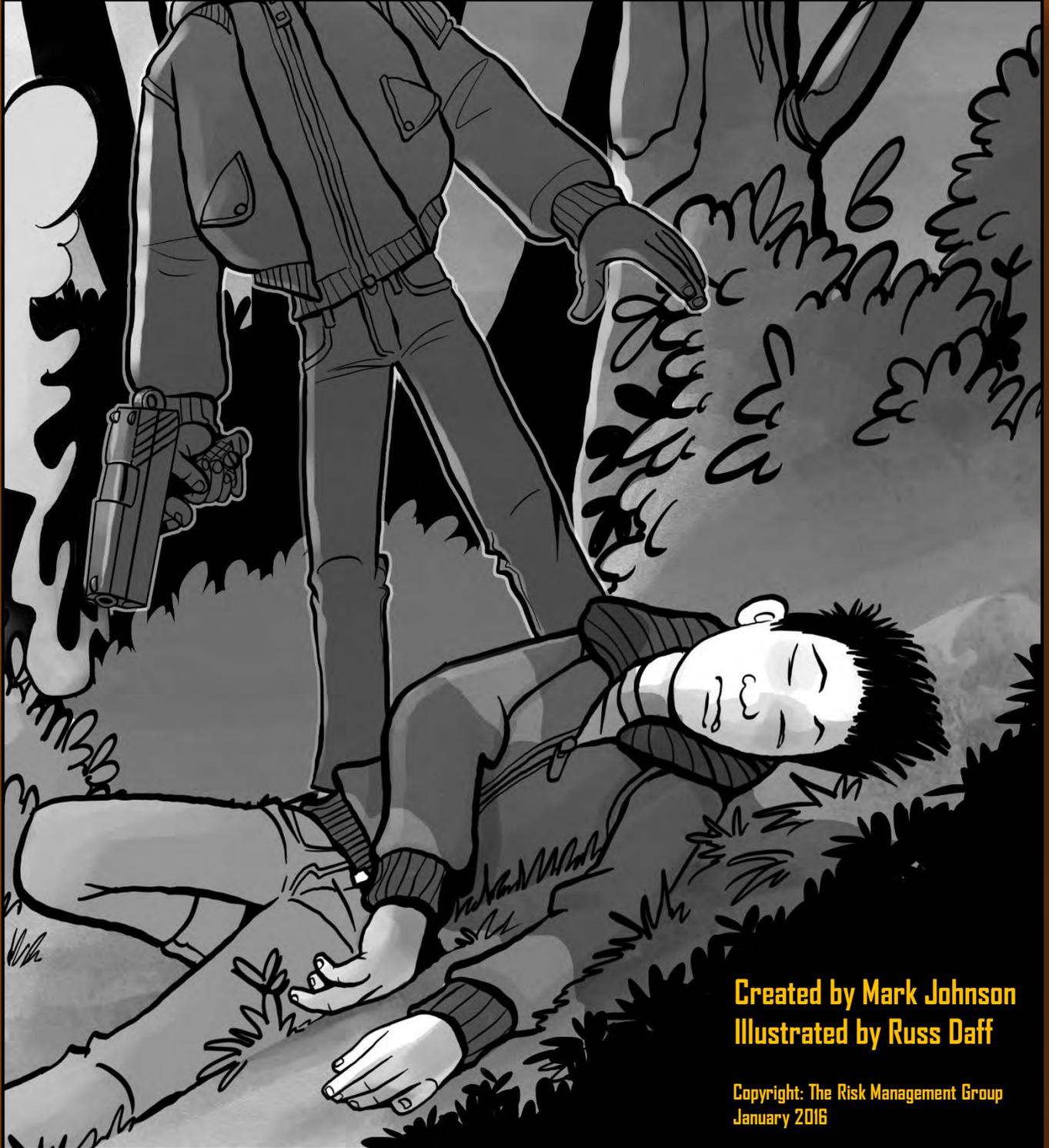
## Disable Google+

[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 1

# The Case of the Facebook Friends



**Created by Mark Johnson**  
**Illustrated by Russ Daff**

Copyright: The Risk Management Group  
January 2016



A CAR IS REPORTED ON FIRE IN A REMOTE LANE...

IT'S ON FIRE OUTSIDE!

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.

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.

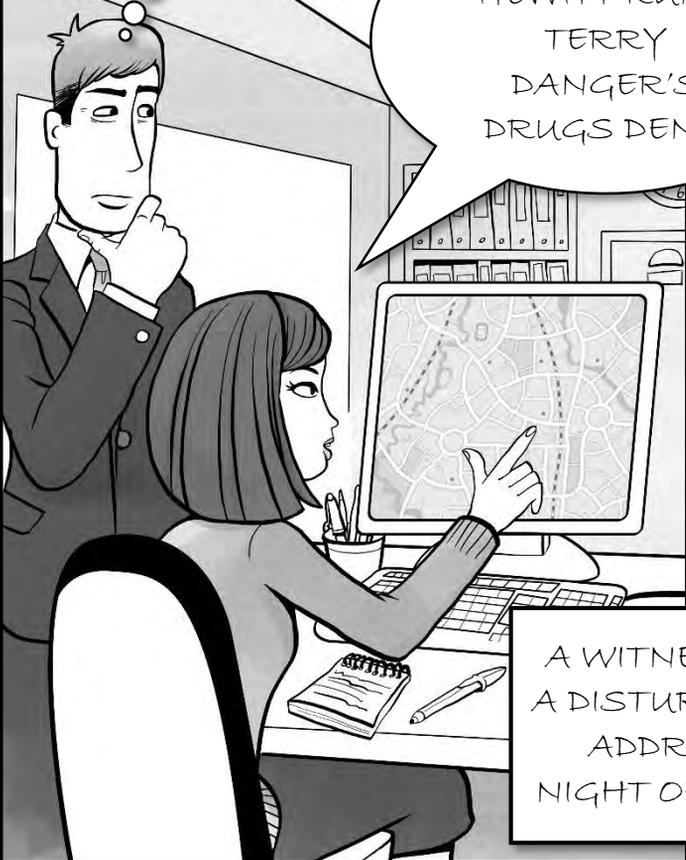


DANGER AND SMITH ALSO HAVE ANOTHER FRIEND IN COMMON ON FACEBOOK; ONE AMELIA HEWITT.



DID SMITH VISIT HER?

WE KNOW HEWITT RUNS TERRY DANGER'S DRUGS DEN...

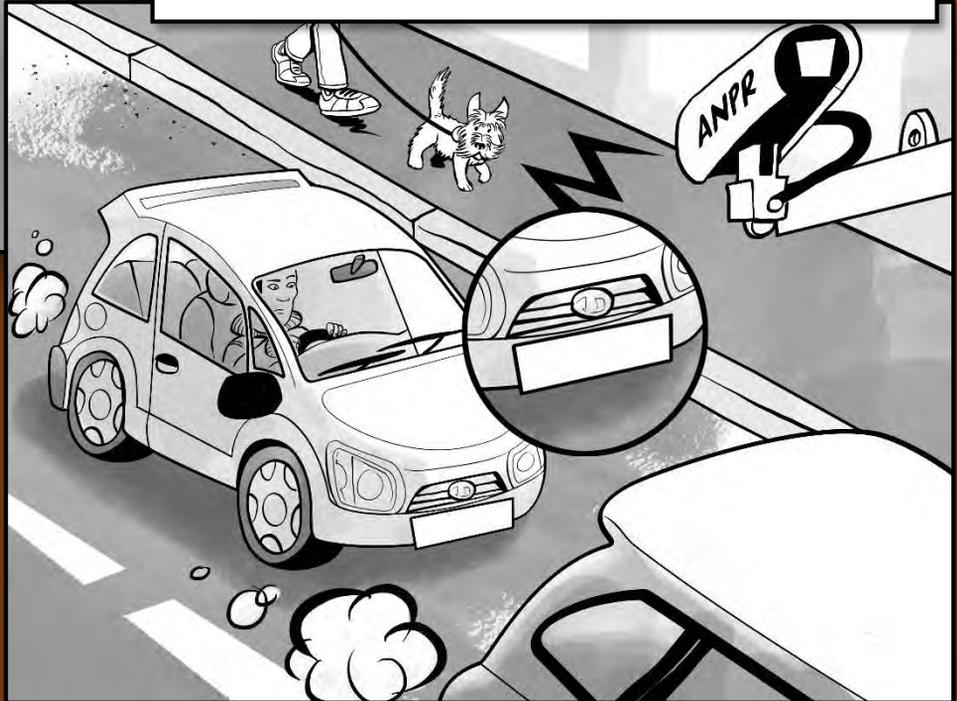


A WITNESS REPORTED A DISTURBANCE AT THE ADDRESS ON THE NIGHT OF THE MURDER.

ANOTHER CHECK OF SMITH'S CALL RECORDS CONFIRMS THAT HE MADE HIS FINAL CALL FROM THE VICINITY OF THE DEN...



AND AUTOMATIC NUMBER PLATE RECOGNITION DATA SHOWS SMITH'S CAR TRAVELLING ON A ROUTE THAT CONNECTS HIS HOME TO THE DEN...



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'.



GOODBYE,  
BOYO!

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

GOODBYE, MR  
DANGER!

ACCESS TO  
COMMUNICATIONS  
DATA, OPEN  
SOURCE  
INTELLIGENCE, AND  
DEVICE FORENSICS  
IS A KEY ELEMENT  
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.

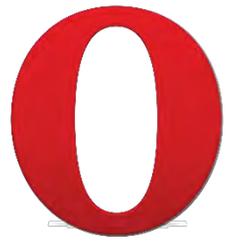


If you use the default browser settings on most browsers, all of your browsing activities may be logged on your device.

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

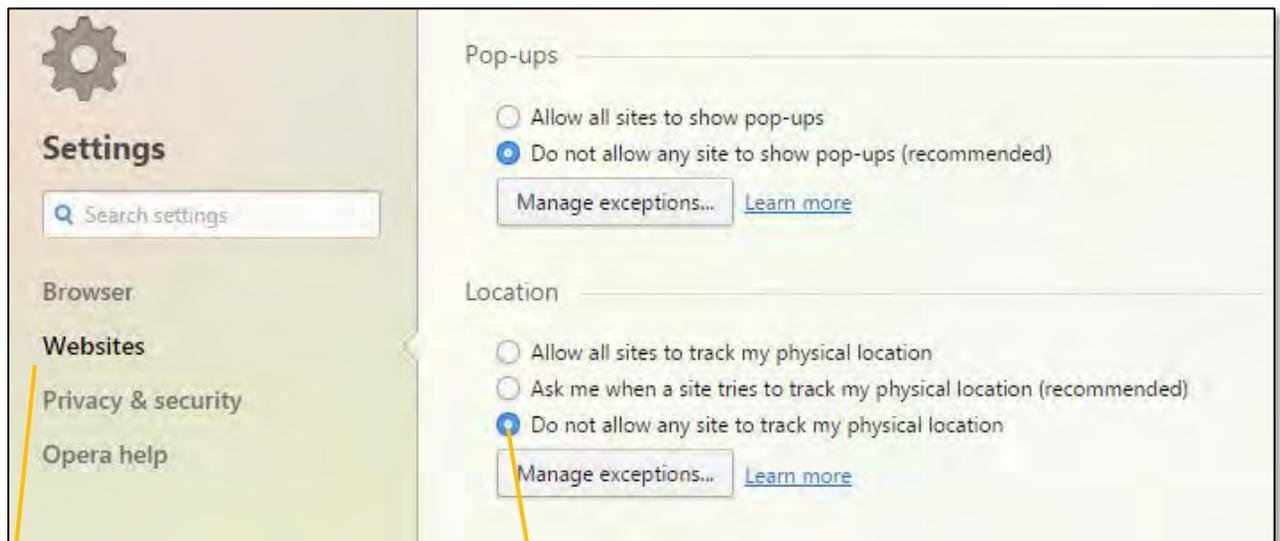


Note: all screenshots taken from the .com site. Mobile versions may have differing features.

## 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

The screenshot shows the Opera browser settings interface. On the left is a 'Settings' sidebar with a search bar and categories: Browser, Websites, Privacy & security (highlighted with a yellow box), and Opera help. The main content area is titled 'Privacy' and contains a 'Clear browsing data...' button (highlighted with a yellow box) and a 'Learn more' link. Below this are several checkboxes for web services, with 'Send a 'Do Not Track' request with your browsing traffic' checked. A section titled 'Want even more privacy?' features a shield icon and text about SurfEasy VPN. Below that is the 'Autofill' section with an unchecked checkbox for 'Enable auto-filling of forms on webpages' and a 'Manage Autofill settings' button. The 'Passwords' section is partially visible at the bottom.

## Clear browsing data

Obliterate the following items from: the beginning of time

- Browsing history
- Download history
- Delete cookies and other site data
- Empty the cache
- Saved passwords
- 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
- 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.

### HTTPS/SSL

Manage certificates... [Learn more](#)

2

### 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

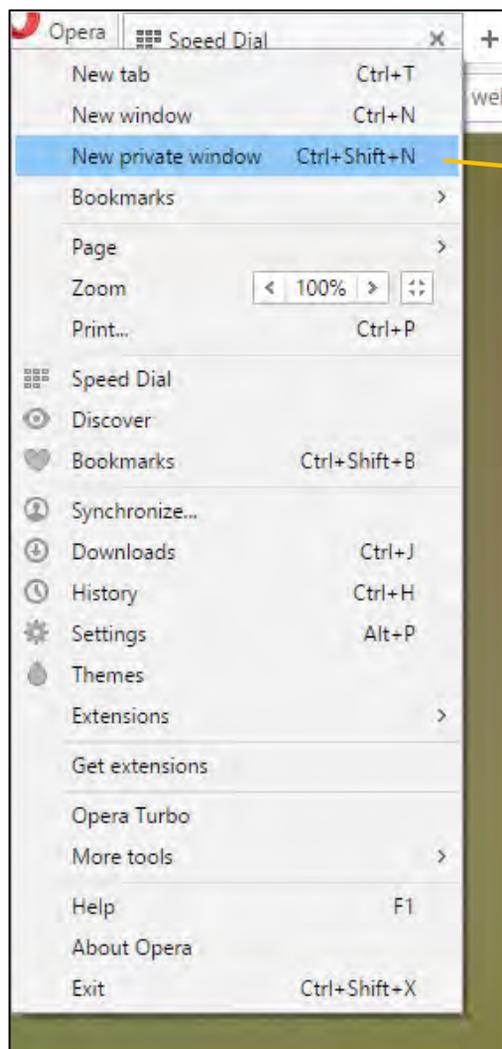
Manage exceptions...

All cookies and site data...

[Learn more](#)

Select this option.

# Private browsing



Click here.

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:

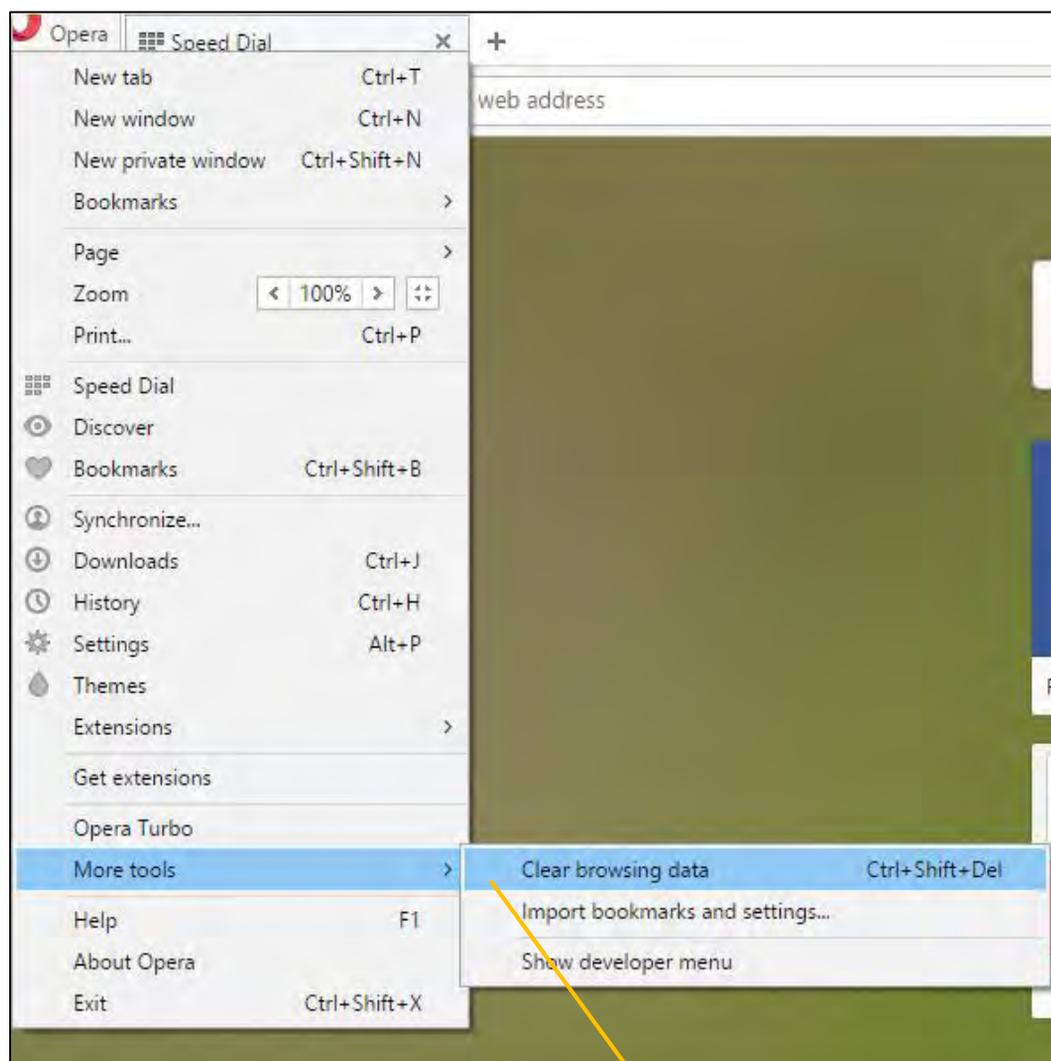
- browsing history
- items in cache
- cookies
- logins

A closed private tab or window cannot be recovered.



The last thing I want is someone reviewing all my searches... I always use private browsing.

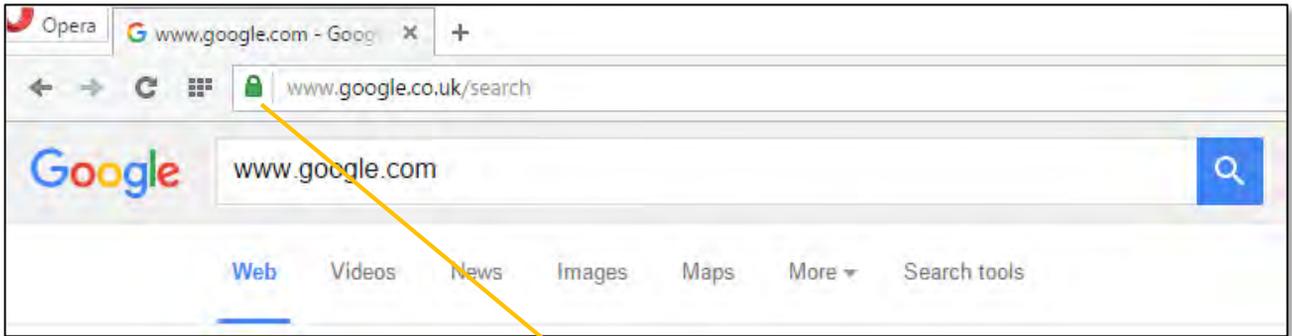
# Clear browsing data shortcut



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

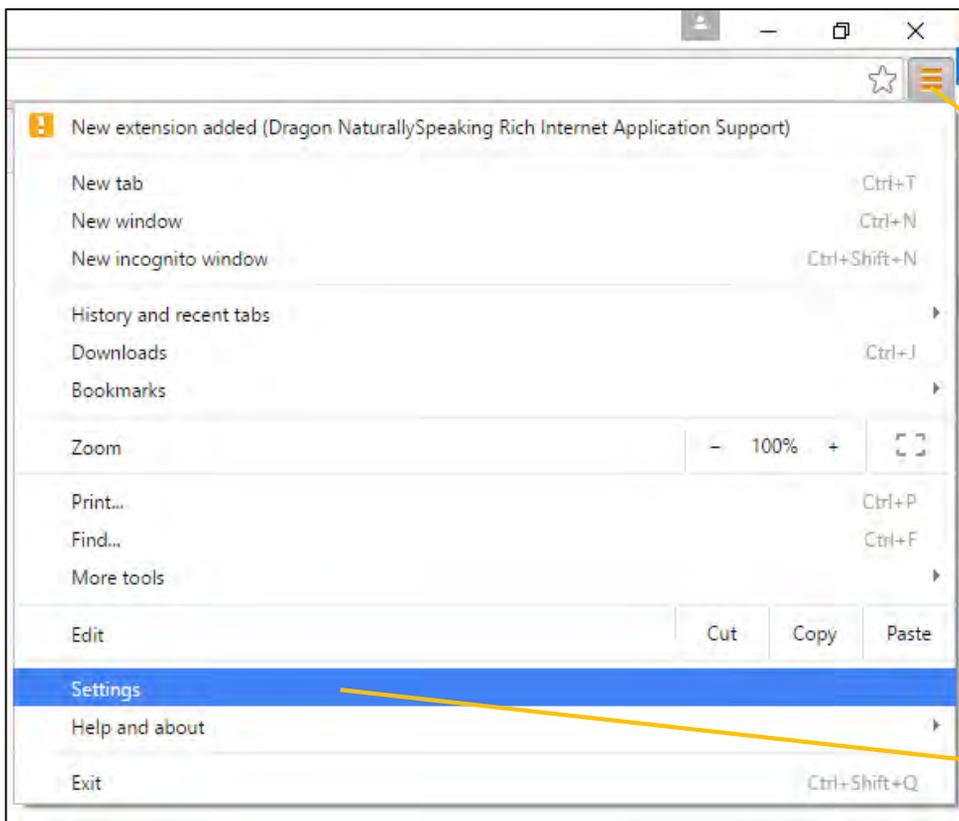
Take careful note of the site security badges displayed for each website you visit.



# Secure Chrome



## Accessing the Menu



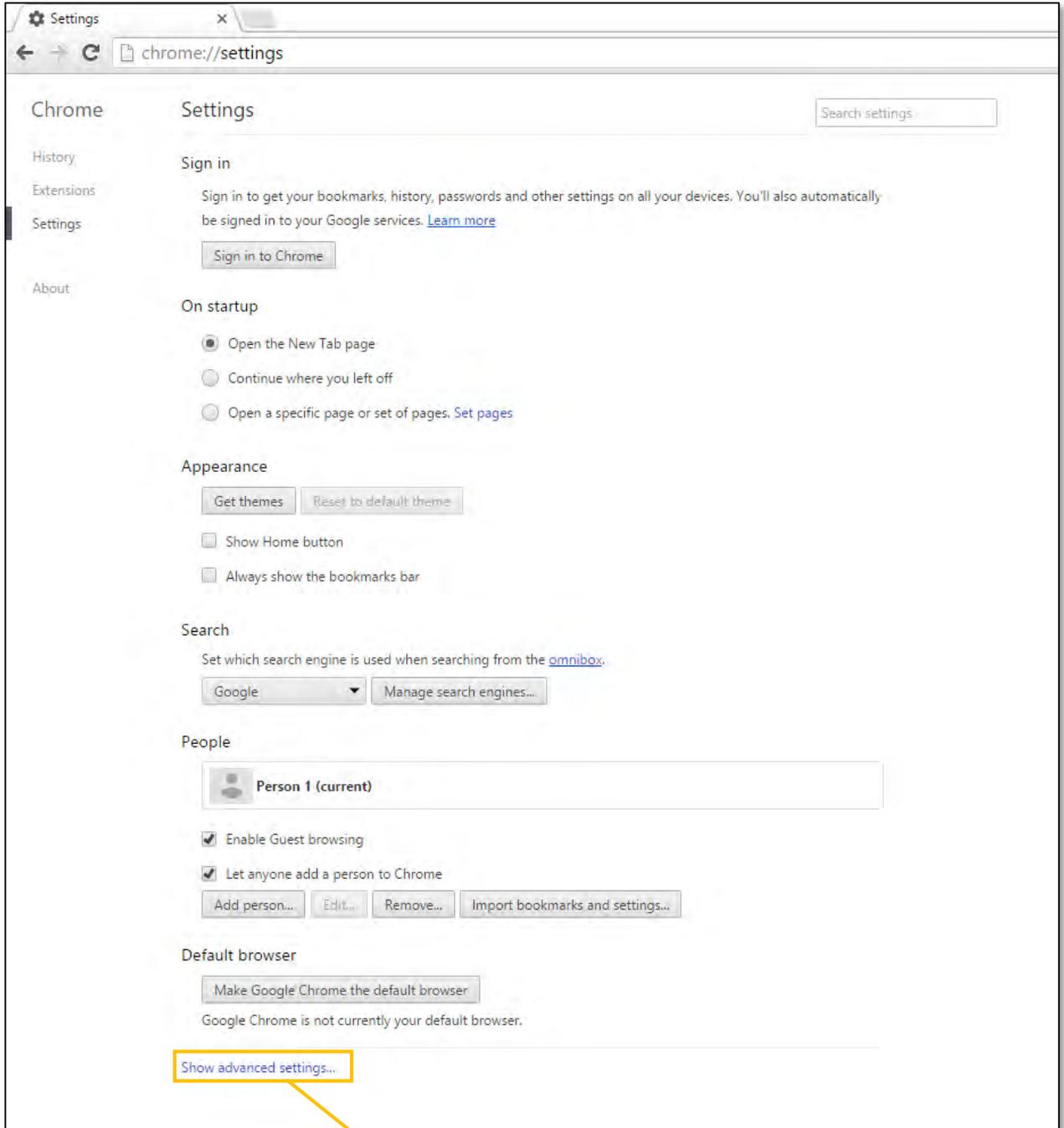
Click here to access the menu...

1

Then select 'Settings'

2

# Accessing Advanced Settings



The screenshot shows the Chrome Settings page. The left sidebar contains links for Chrome, History, Extensions, Settings, and About. The main content area is titled 'Settings' and includes a search bar. The sections visible are:

- Sign in:** A button labeled 'Sign in to Chrome'.
- On startup:** Three radio button options: 'Open the New Tab page' (selected), 'Continue where you left off', and 'Open a specific page or set of pages. Set pages'.
- Appearance:** Buttons for 'Get themes' and 'Reset to default theme', and checkboxes for 'Show Home button' and 'Always show the bookmarks bar'.
- Search:** A dropdown menu set to 'Google' and a 'Manage search engines...' button.
- People:** A profile card for 'Person 1 (current)', a checked checkbox for 'Enable Guest browsing', another checked checkbox for 'Let anyone add a person to Chrome', and buttons for 'Add person...', 'Edit...', 'Remove...', and 'Import bookmarks and settings...'.
- Default browser:** A button 'Make Google Chrome the default browser' and the text 'Google Chrome is not currently your default browser.'

At the bottom of the page, a yellow box highlights the link 'Show advanced settings...'. A yellow arrow points from this box to a red diamond icon containing the number '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
- Prefetch resources to load pages more quickly
- Automatically report details of possible security incidents to Google
- 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
- 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



Google Chrome may use web services to improve your browsing experience. You may optionally disable these services. [Learn more](#)

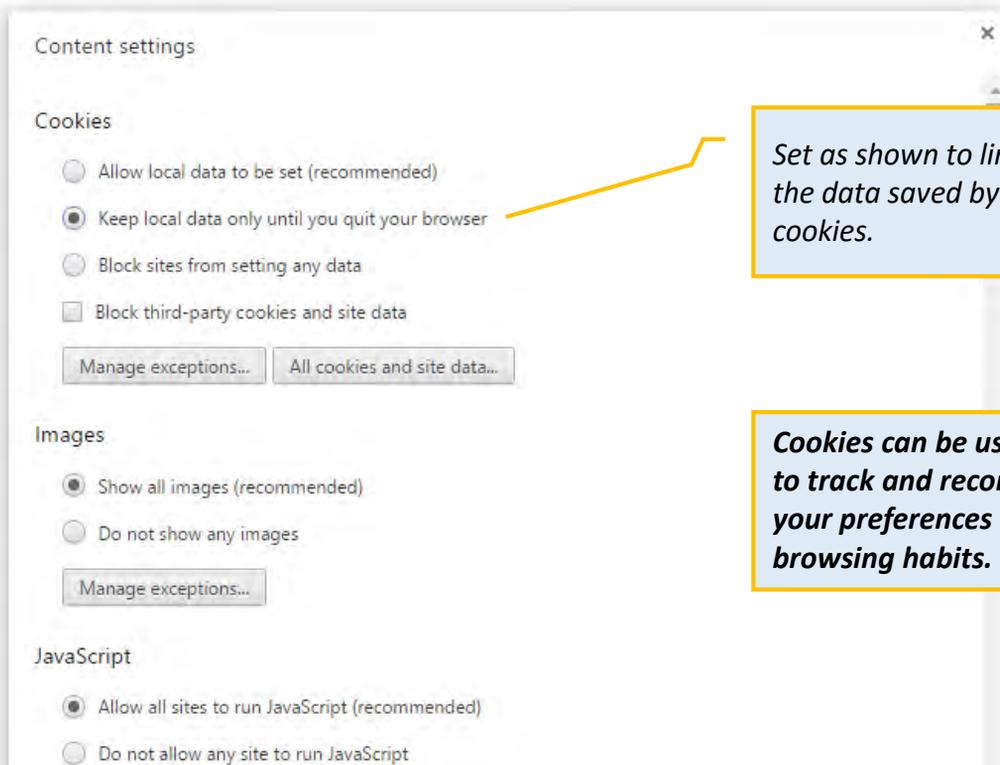
- Use a web service to help resolve navigation errors
- Use a prediction service to help complete searches and URLs typed in the address bar or the app launcher search box
- Prefetch resources to load pages more quickly
- Automatically report details of possible security incidents to Google
- Protect 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
- 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



*Set as shown to limit the data saved by cookies.*



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



# Control location tracking

## Content settings

### Location

- Allow all sites to track your physical location
- Ask when a site tries to track your physical location (recommended)
- Do not allow any site to track your physical location

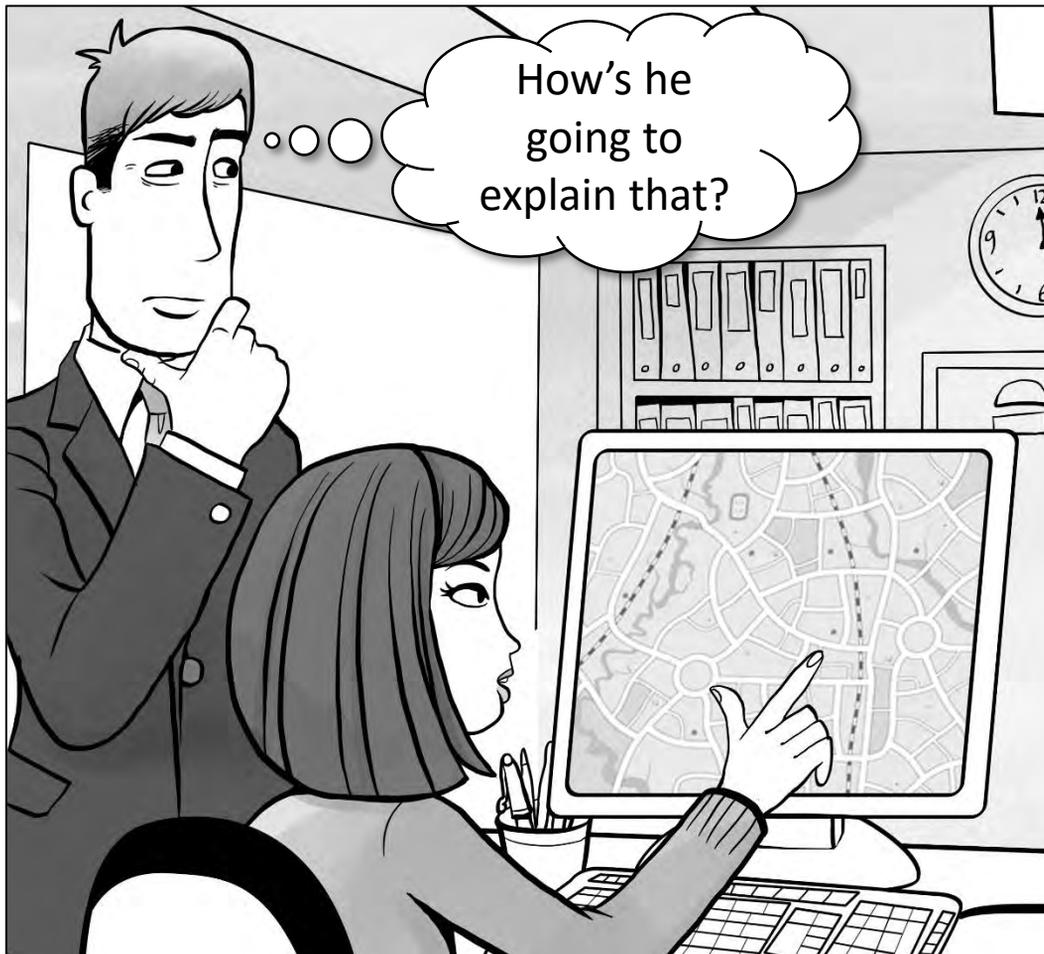
Manage exceptions...

### Notifications

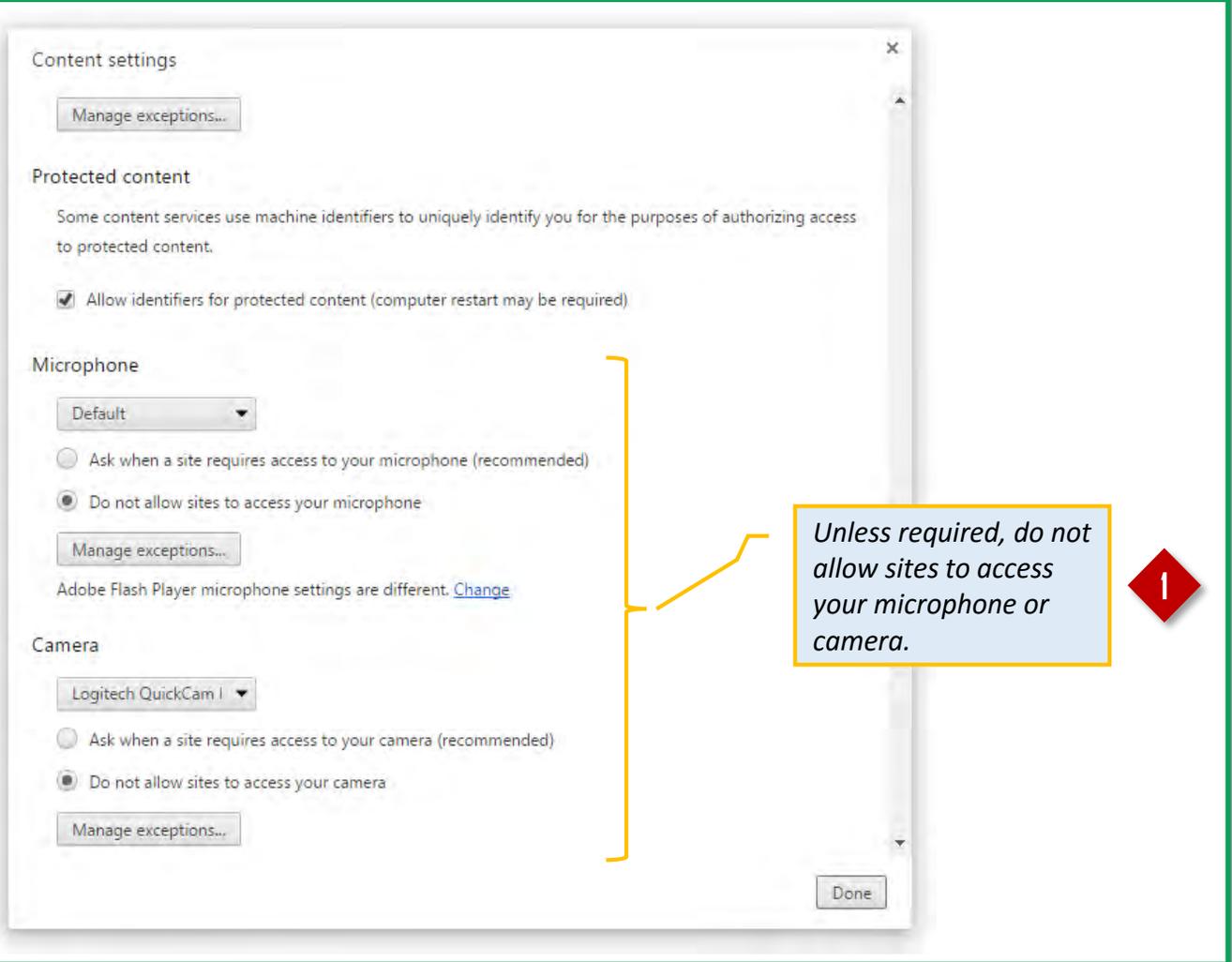
- Allow all sites to show notifications
- Ask when a site wants to show notifications (recommended)
- Do not allow any site to show notifications

Manage exceptions...

Control which sites can track your physical location.

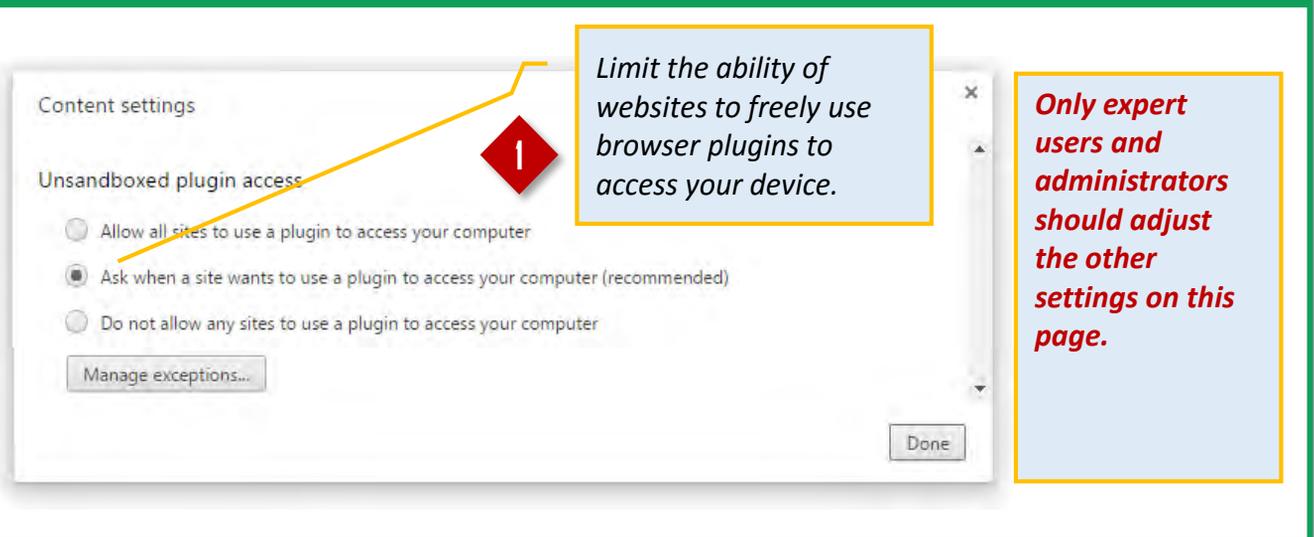


# Content settings – Microphone & Camera



The screenshot shows the 'Content settings' dialog box. Under the 'Microphone' section, the 'Do not allow sites to access your microphone' option is selected. Under the 'Camera' section, the 'Do not allow sites to access your camera' option is selected. A yellow bracket groups these two sections, with a callout box containing the text: 'Unless required, do not allow sites to access your microphone or camera.' A red diamond icon with the number '1' is positioned to the right of the callout box.

# Plugin access



The screenshot shows the 'Content settings' dialog box for 'Plugin access'. The 'Ask when a site wants to use a plugin to access your computer' option is selected. A yellow callout box with the text 'Limit the ability of websites to freely use browser plugins to access your device.' points to the selected option. A red diamond icon with the number '1' is also present. To the right, another yellow callout box contains the text: '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'*

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
- Prefetch resources to load pages more quickly
- Automatically report details of possible security incidents to Google
- 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
- 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](#)



*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.*



Clear browsing data

Obliterate the following items from: [the beginning of time](#)

- Browsing history
- Download history
- Cookies and other site and plugin data
- Cached images and files
- Passwords
- 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)

The screenshot shows the Google homepage in a Firefox browser window. The hamburger menu icon in the top right corner is highlighted with a yellow box. A red diamond with the number '1' and a callout box labeled 'Click here...' points to this icon. The menu is open, and the 'New Private Window' option, which features a mask icon, is highlighted with a yellow box. A red diamond with the number '2' and a callout box labeled 'Then click here to use private browsing (more secure)' points to this option.

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

4 Finally, access Options here

This close-up of the Firefox hamburger menu shows the 'History' and 'Options' options highlighted with yellow boxes. A red diamond with the number '3' and a callout box labeled 'Or here to review (and optionally clear) browsing history.' points to the 'History' option. A red diamond with the number '4' and a callout box labeled 'Finally, access Options here' points to the 'Options' option.



# Options - Advanced - General

Advanced

General Data Choices Network Update Certificates

**Accessibility**

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

**Browsing**

- Use autoscrolling

Set this to 'on'

# Options - Advanced - Update

Advanced

General Data Choices Network Update Certificates

**Firefox updates:**

- Automatically install updates (recommended: improved security)
  - 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

- Use a background service to install updates

**Automatically update:**

- Search Engines

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

# Secure IE

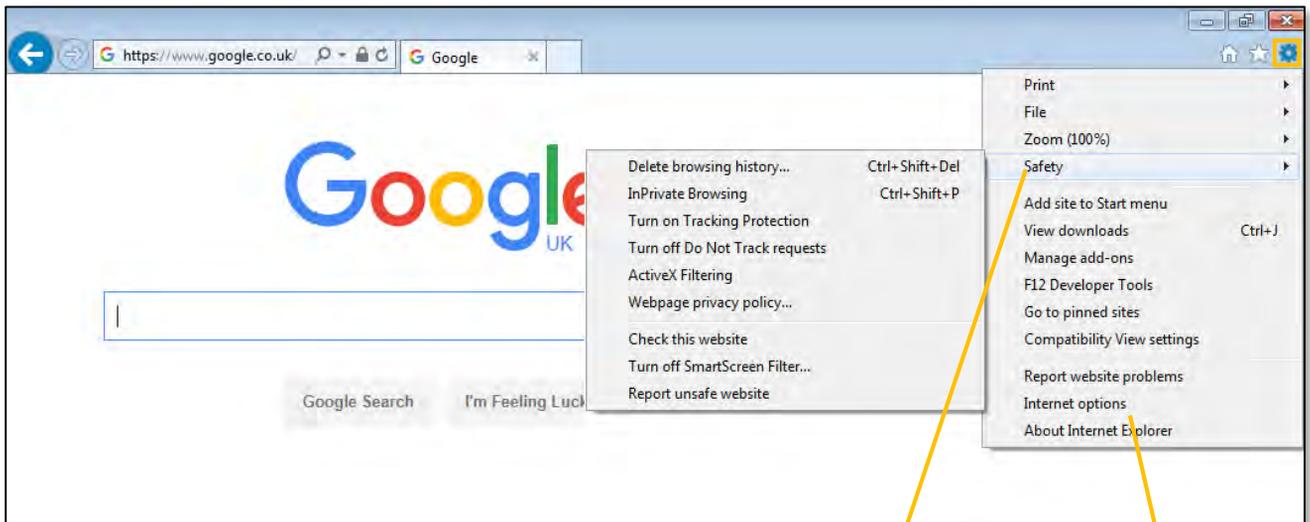


*Note: all screenshots taken from the .com site. Mobile versions may have differing features.*

## Accessing Safety Options & Settings



*Click to access the menu*

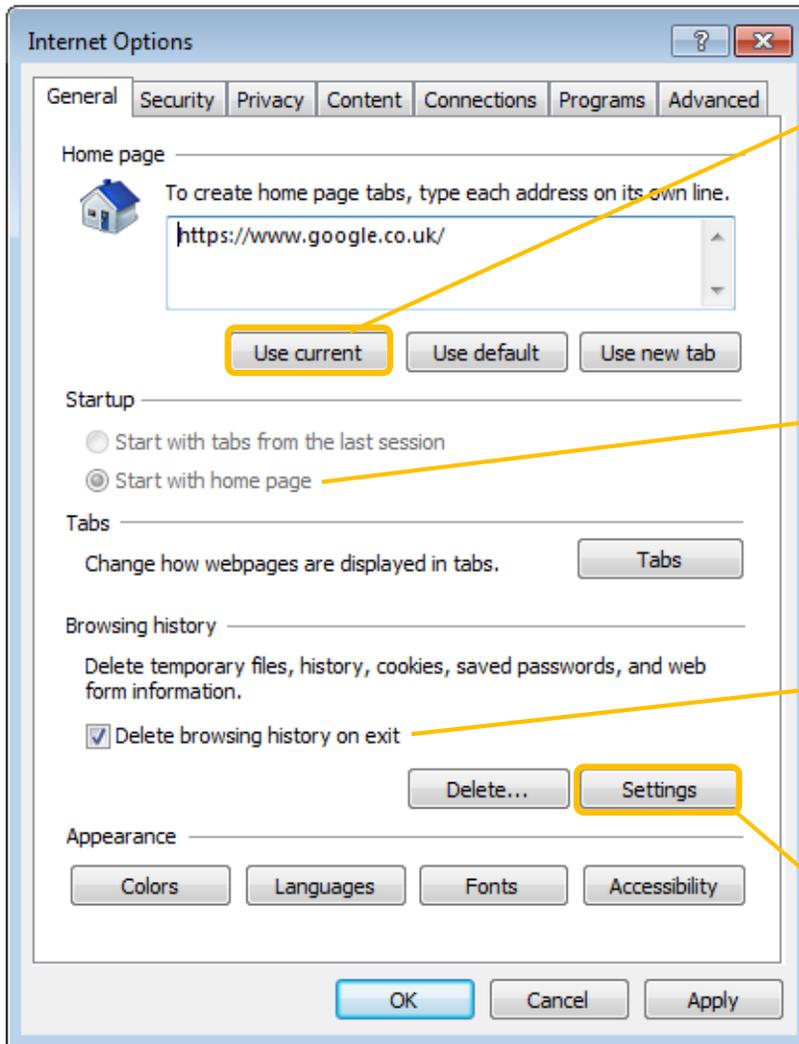


*Then select 'Safety' for a quick list of popular options*



*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.



Set IE to start with the home page.



Set to delete browsing history on exit.



Now click 'Settings'.



# Internet Options – General - Settings

The image shows two overlapping screenshots of the Internet Options dialog box. The top screenshot shows the 'History' tab selected, with an annotation pointing to it. The bottom screenshot shows the 'Caches and databases' tab selected, with an annotation pointing to the 'Allow website caches and databases' checkbox.

**1** Select the 'History' tab...

**2** Set this value to '0'.

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

**4** Deselect this option.

**Website Data Settings - History Tab:**

Specify how many days Internet Explorer should save the list of websites you have visited.

Days to keep pages in history:

**Website Data Settings - Caches and databases Tab:**

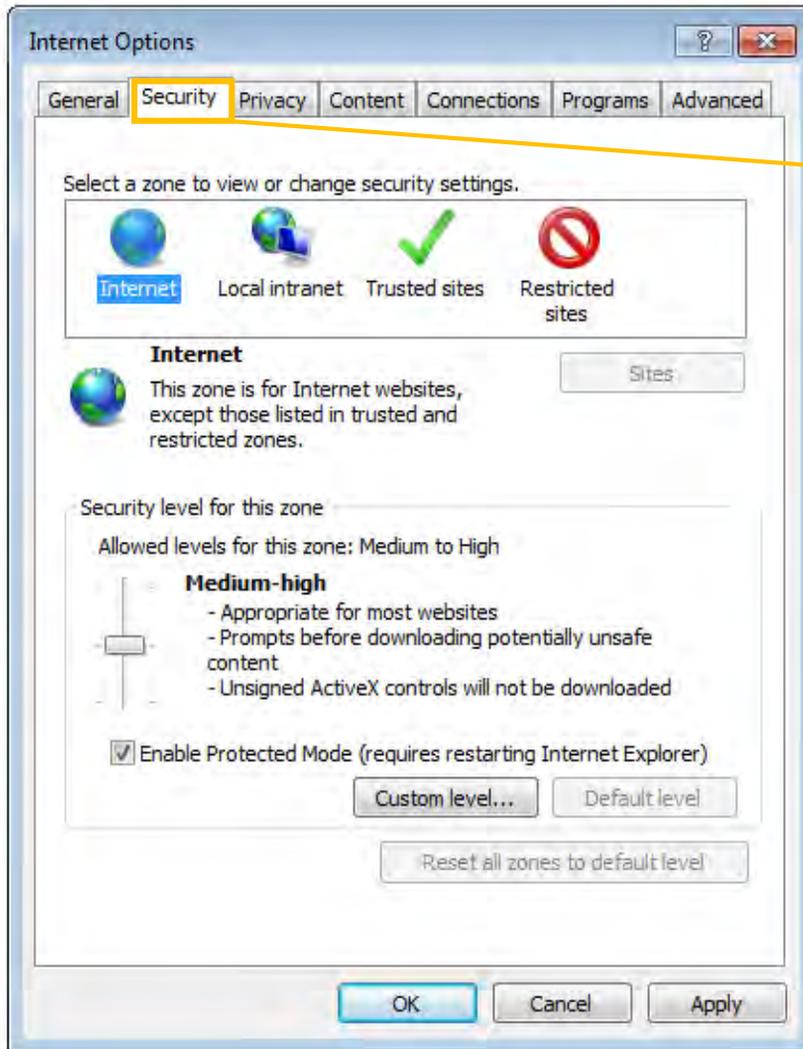
Allow website caches and databases

Notify me when a website cache or database exceeds:  MB

Website	File Storage	Data Storage	Exceed limit
windowsphone.com	4 MB	0 MB	N/A

Buttons: Exceed limit, Delete, OK, Cancel

# Internet Options – Security



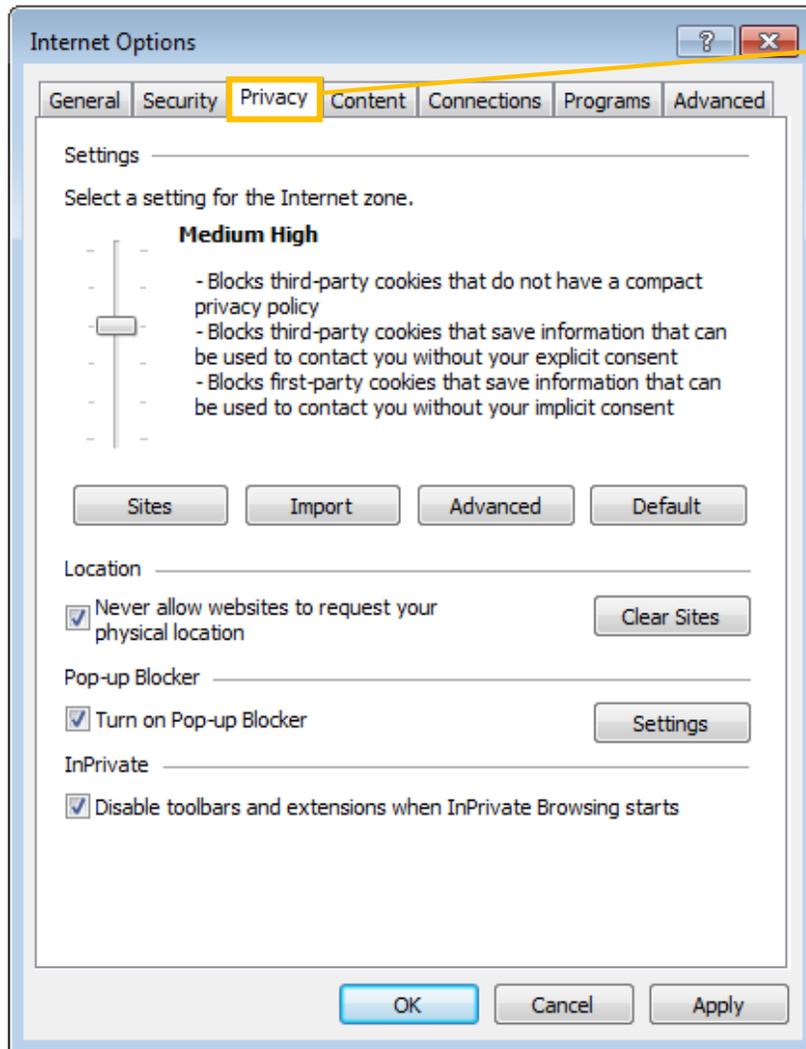
Select the 'Security' tab...



Choose the security level that suits your role.



# Internet Options – Privacy



Select the 'Privacy' tab...



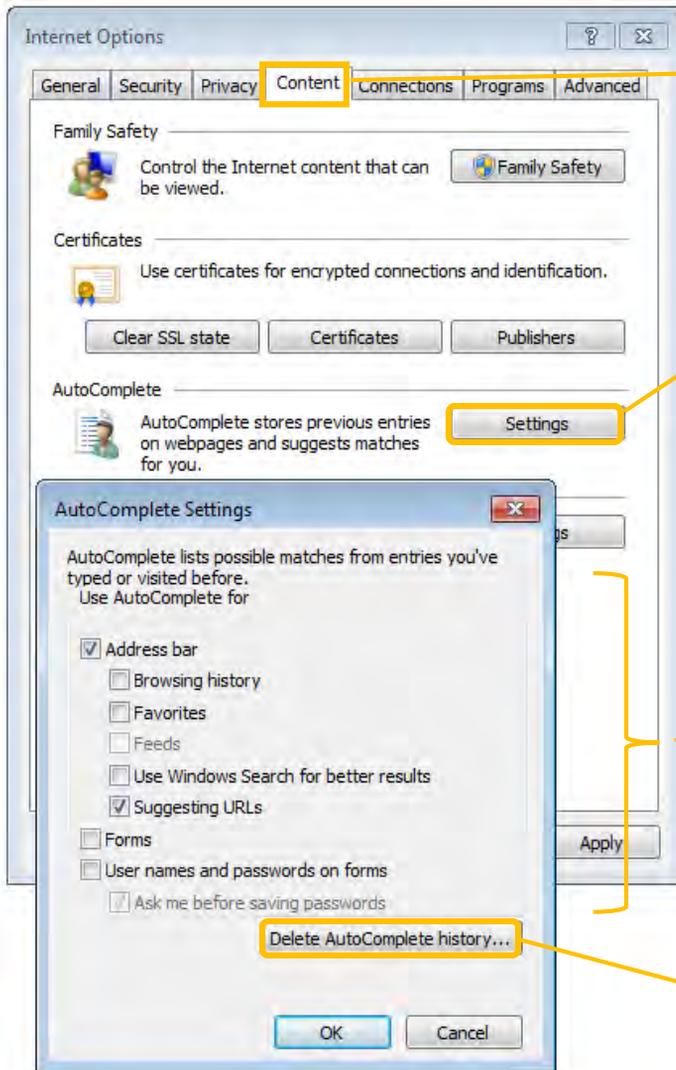
Choose the cookie setting that suits your role.



Select all three settings as shown (recommended).



# Internet Options – Content



Select the 'Content' tab...

1

Click 'Settings'...

2

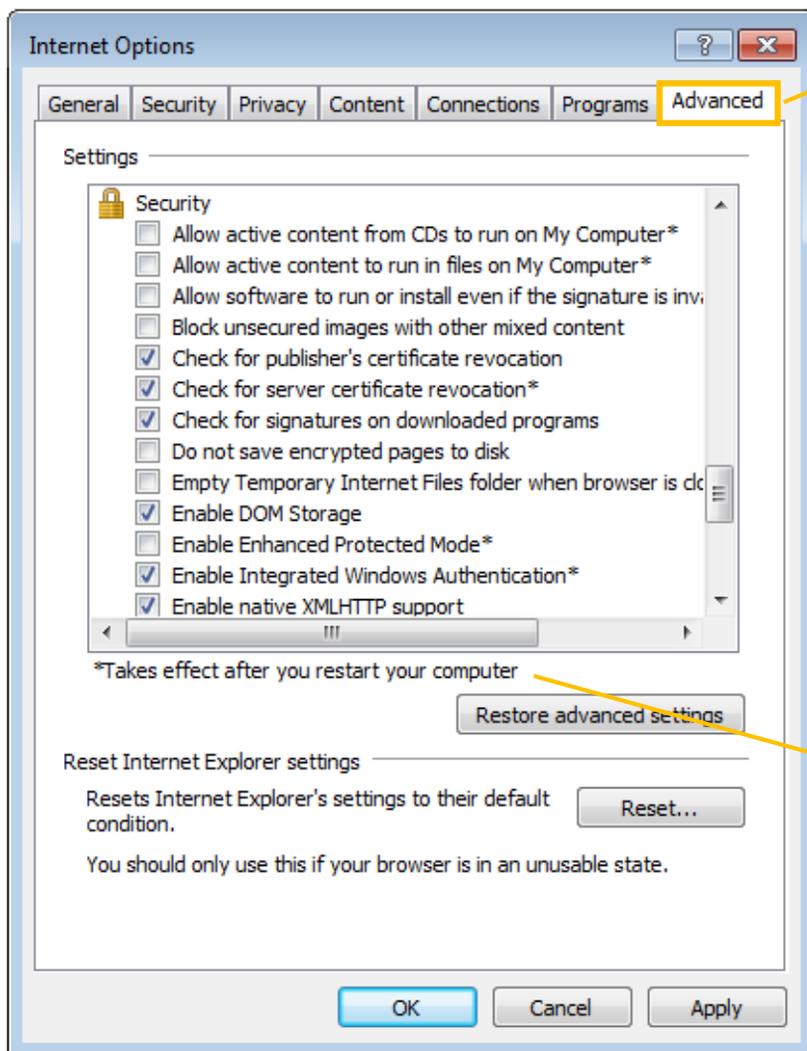
Choose the auto-complete settings that suit your role.

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.

3  
Restart your computer to make sure that all new settings take effect.

# 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.

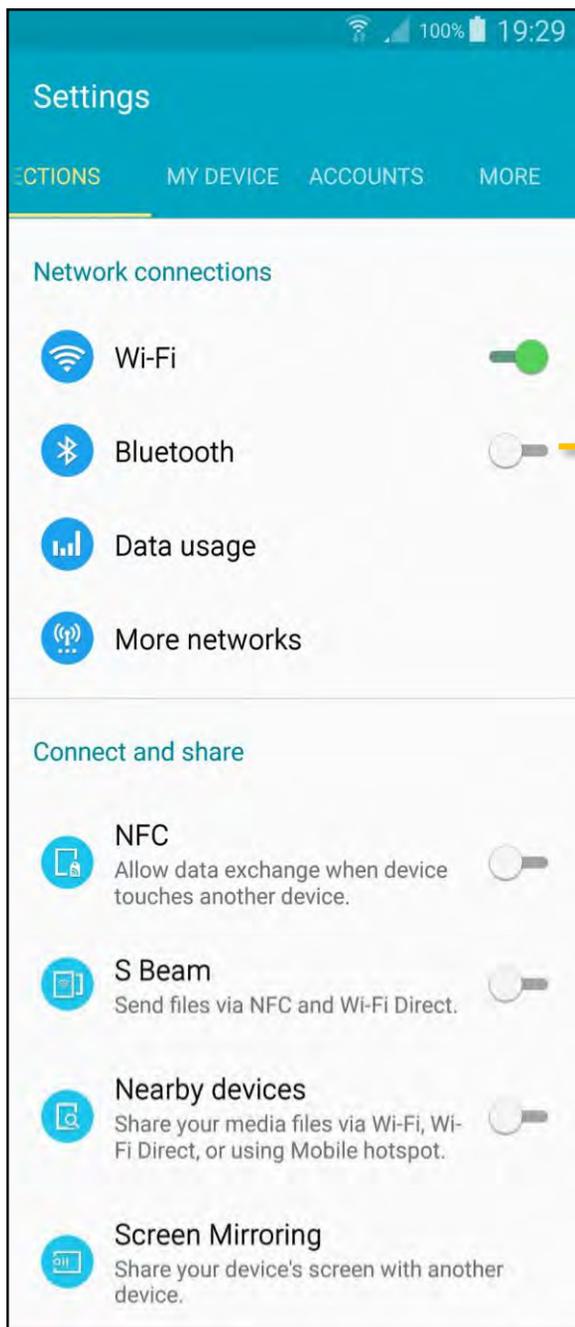
Contact information, messages, photos, social media feeds, location data and more can all be derived from a mobile device.

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



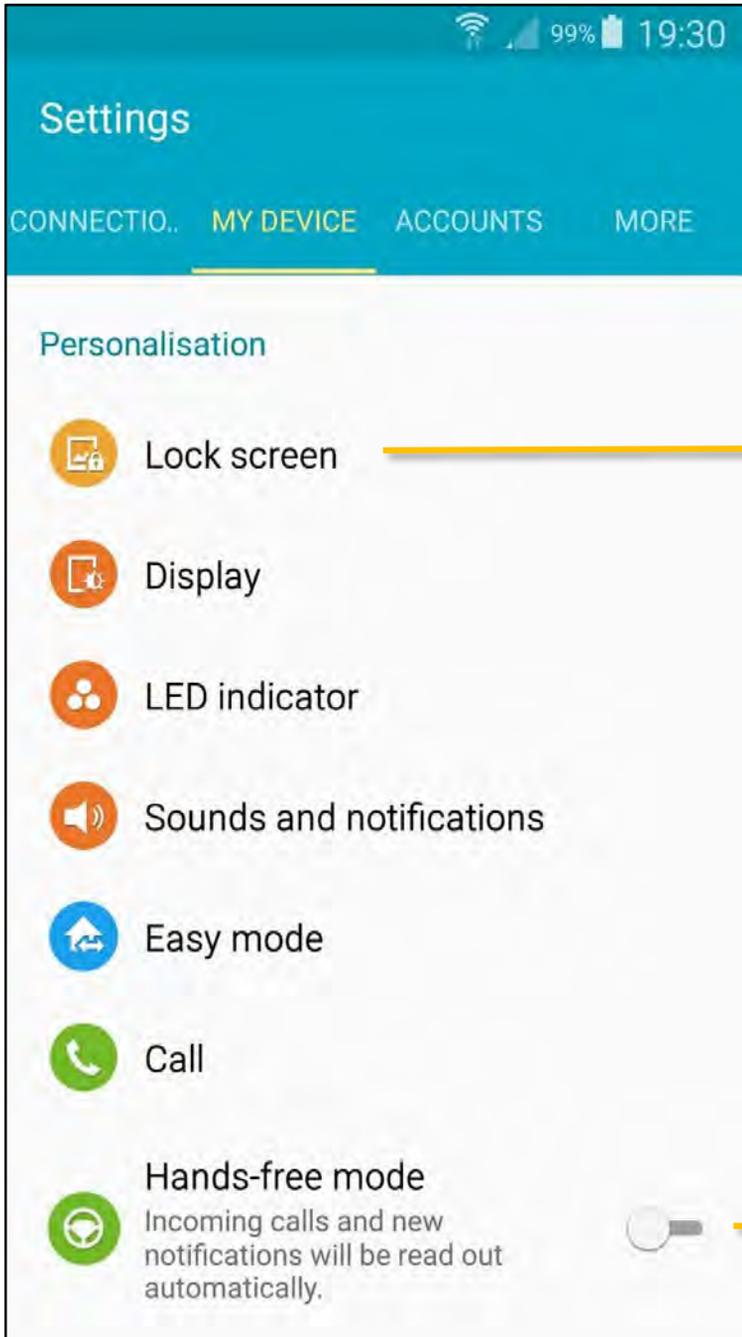
1

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

2

*Turn off Connect and Share options unless essential*

# My Device



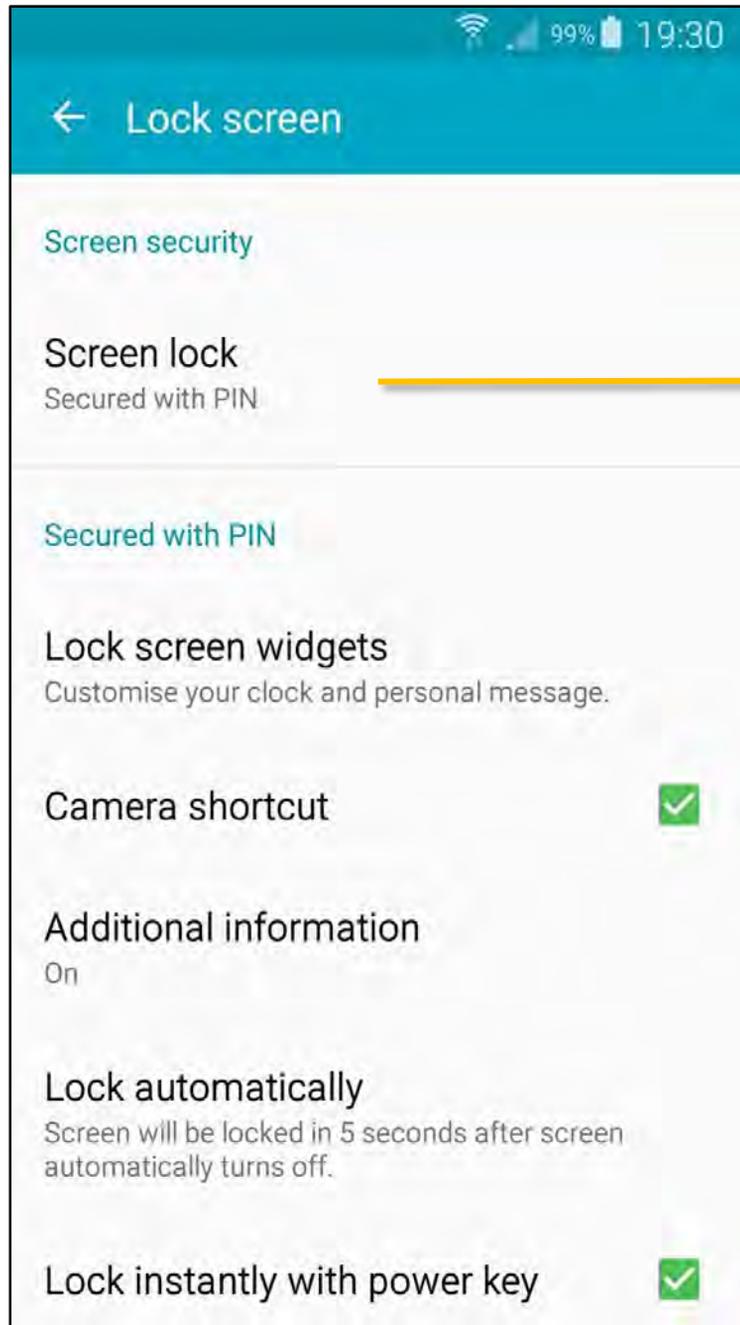
1

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

2

*Turn off hands-free mode unless required*

# Lock Screen



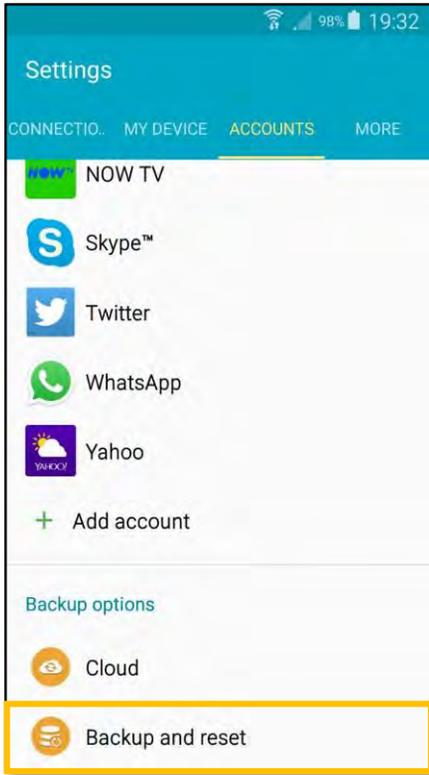
1

Set a lock screen PIN

2

Set automatic locking and power key locking to ON

# Backup options

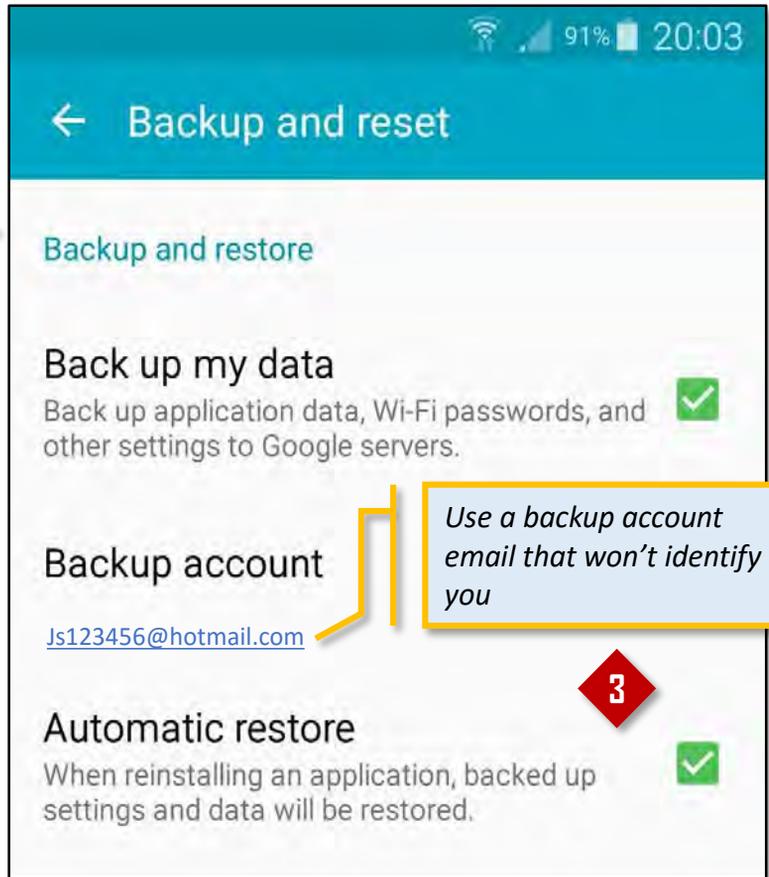


1

*Press to access Backup options*

2

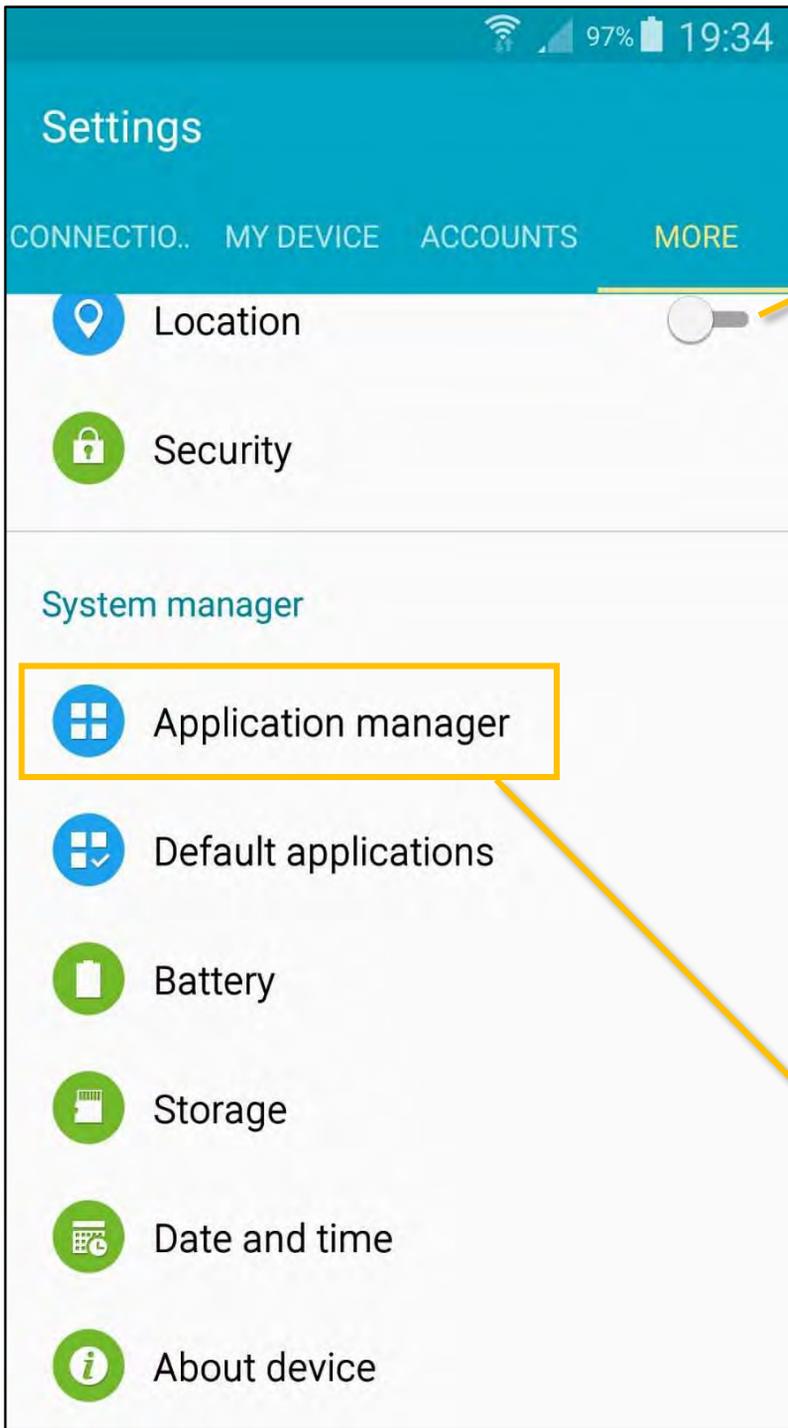
*Set appropriate backup and restore settings, based on your role*



3

*Use a backup account email that won't identify you*

# Location and Application management



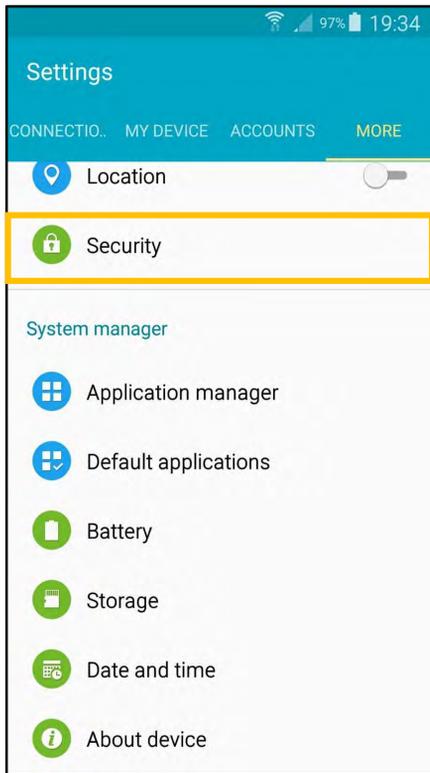
1

*Turn off location services, unless required*

2

*Review your installed Apps and remove any unwanted ones.*

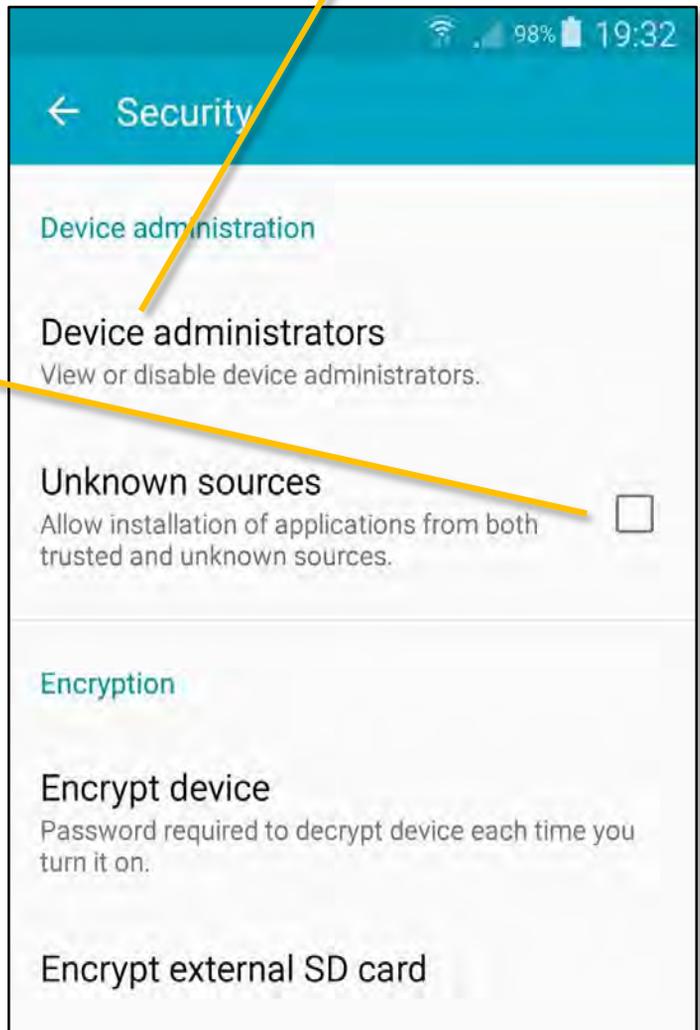
# Security



*Press to access Security management*



*Review your device administrators*



*Disable unknown sources*



*Consider encrypting your device & any SD cards, if permitted*



# 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

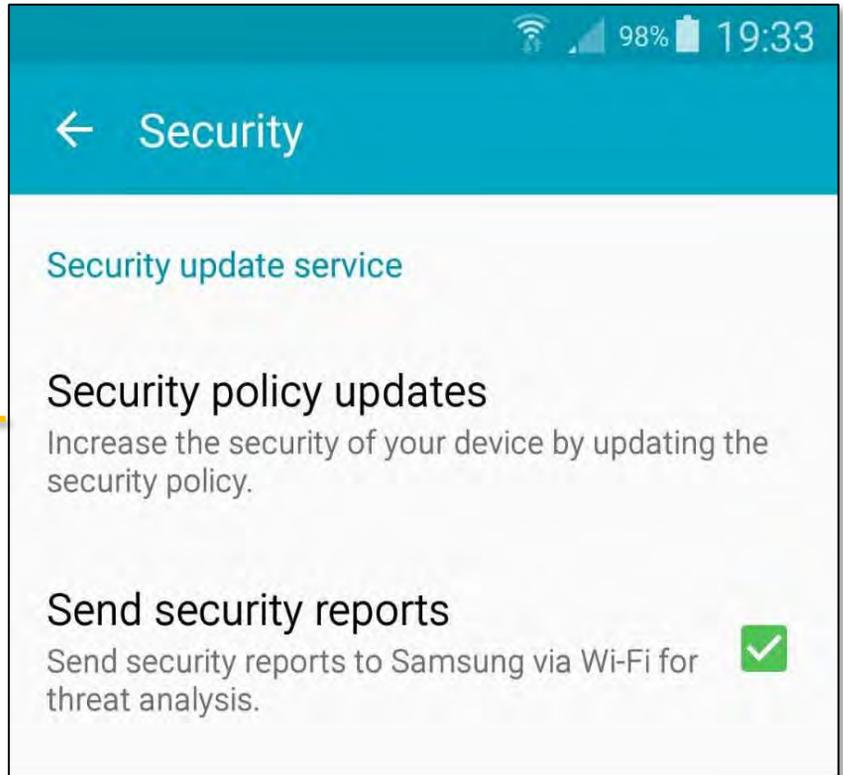
Do not make passwords visible

The screenshot shows the 'Security' settings page on an Android device. The status bar at the top indicates 98% battery and the time 19:33. The page title is 'Security' with a back arrow. The settings listed are: 'Find My Mobile', 'Remote controls' (Off), 'SIM change alert', 'Go to website' (http://findmymobile.samsung.com), 'SIM card lock', 'Set up SIM card lock', 'Passwords', and 'Make passwords visible' (with a checkbox). Yellow callout boxes and lines connect the text on the left to the corresponding settings on the right.

# Security updates



Ensure that your security policies are up-to-date



These days, smartphones hold loads of sensitive data.

Some people just don't see the risks, but I guess 'smart phone' doesn't always equal 'smart user'!



# Secure Smart Phone Blackberry

## To access Security settings



*Enter the Options menu and then select Security*



## Password



*Select Password from the Security menu*



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



# Holstering lock



*Set the device to auto-lock when holstered.*



# Encryption



*Now select Encryption from the Security menu*



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



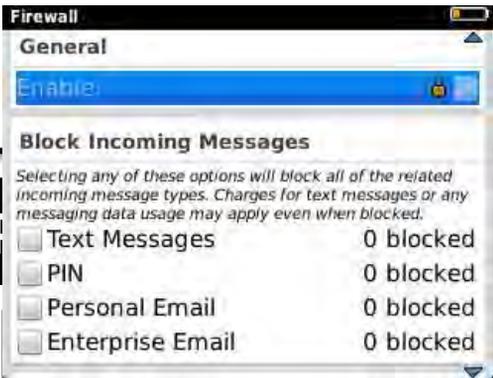
# PIN Caching



Next, select Smart Card from the Security menu



Deactivate PIN Caching



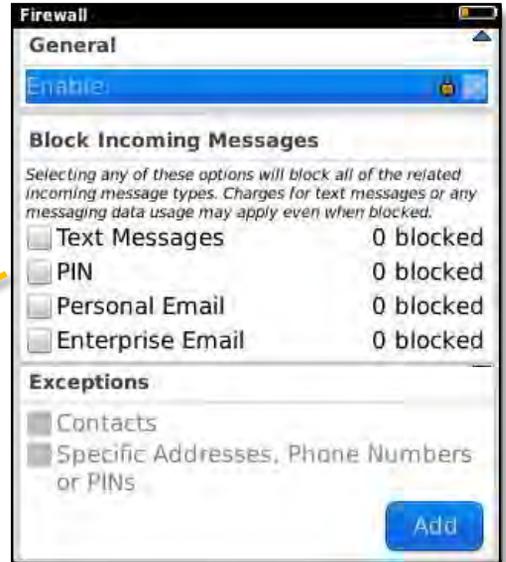
Select Parental Controls and consider whether to activate



# Firewall



Select Firewall



Decide whether to block any message types



# Firewall



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



# Secure Smart Phone

## iOS (iPhone/iPad) devices

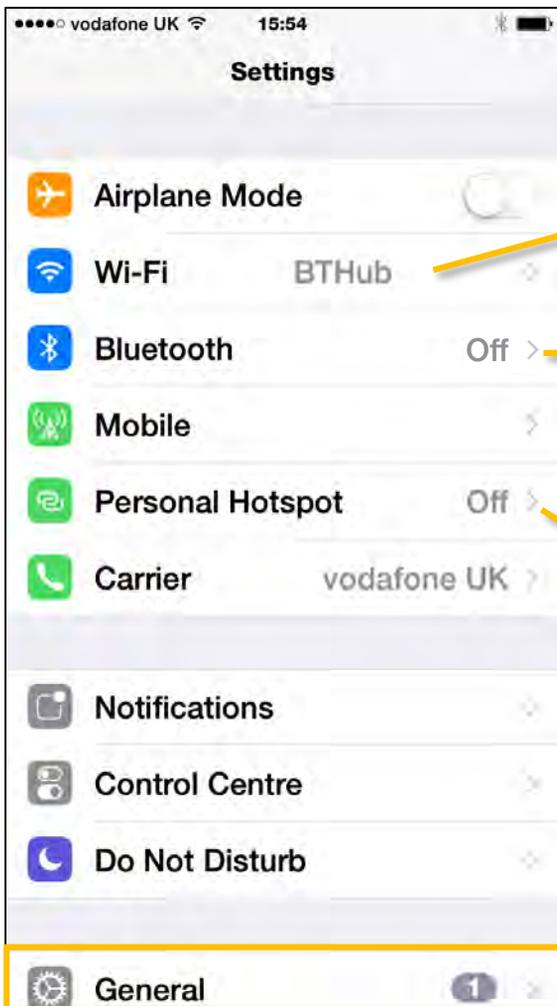


### To access Settings



Locate the Settings icon on your device and press it

1



Only use trusted, secure WiFi networks

2

Turn Bluetooth off unless needed

3

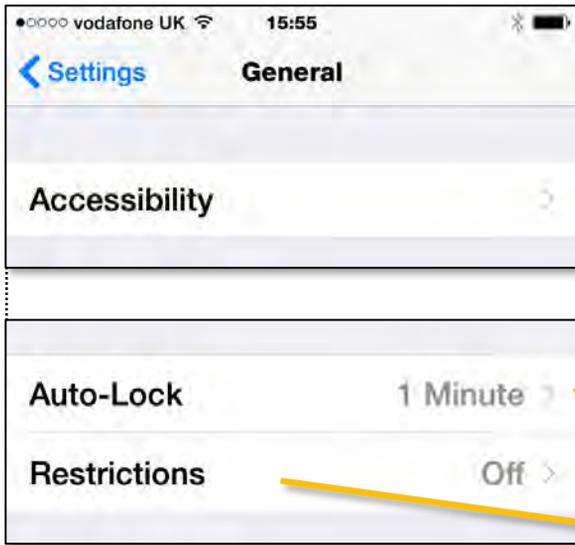
Turn Hotspot off unless needed

4

Now press the 'General' menu option

5

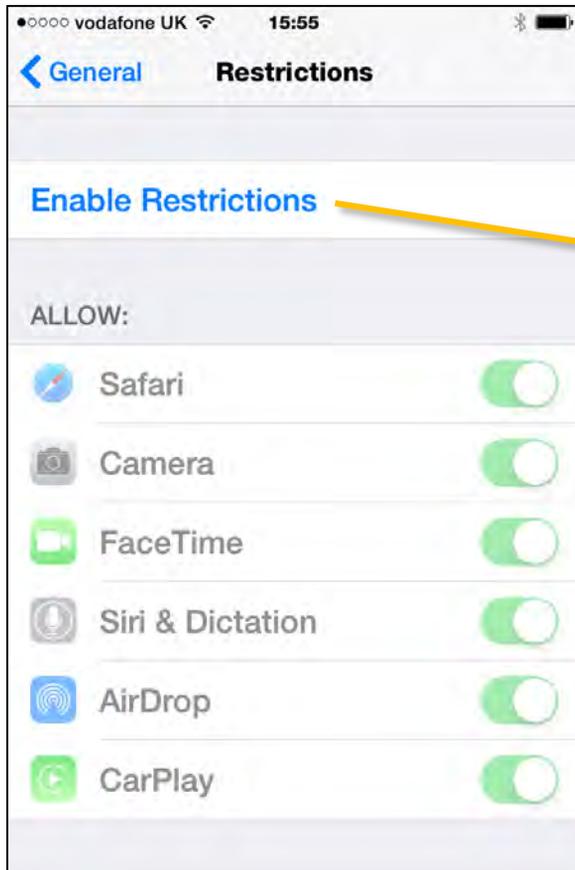
# Auto-Lock



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

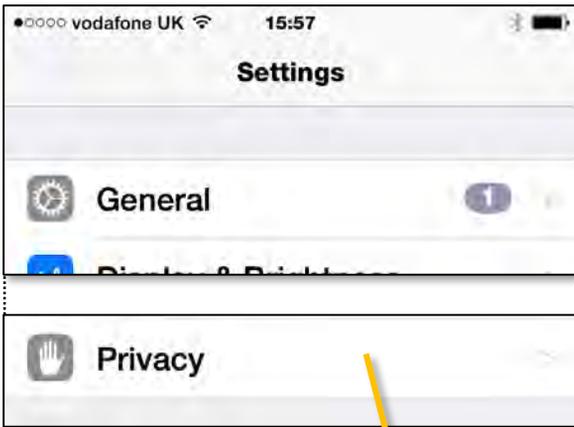


1  
Press 'Enable Restrictions' if you want to restrict access to specific applications.

You will be asked to select a Restrictions Password.

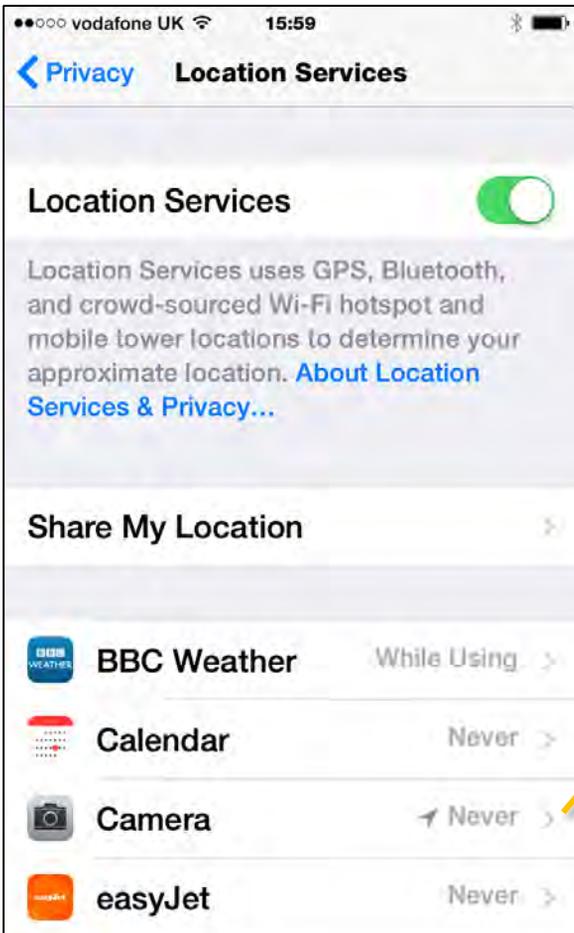
2  
Disallow access to those applications you do not want other users of your device to use. You can also do this on any iOS device you have given to a child or other vulnerable person.

# Privacy - Location Services



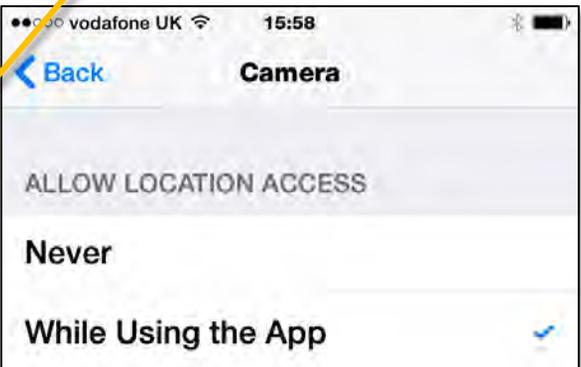
Return to 'Settings' and select 'Privacy'

Then select 'Location Services'

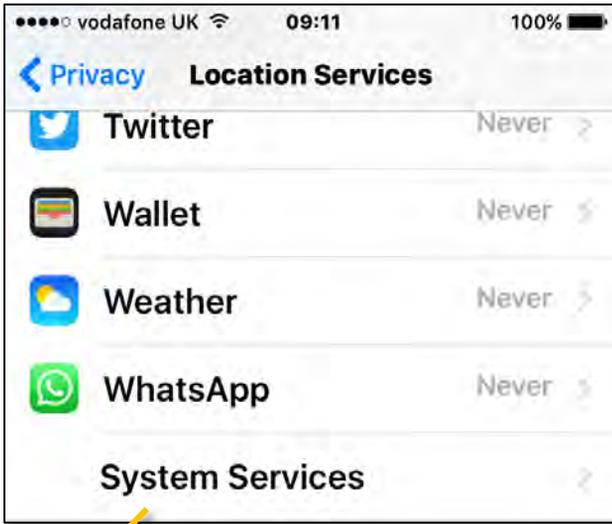


Turn Location Services **OFF** for maximum security (recommended)

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



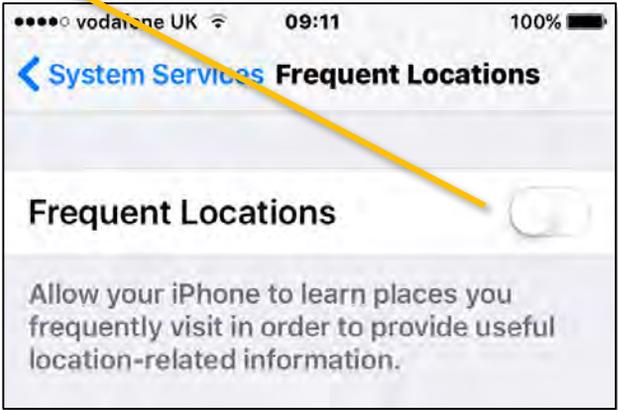
# Privacy – Frequent Locations



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

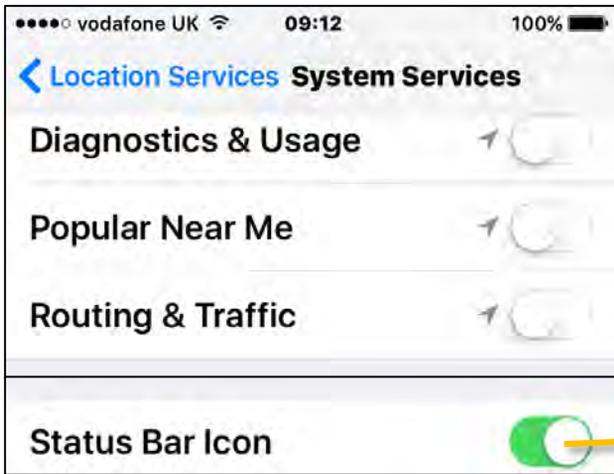
2

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

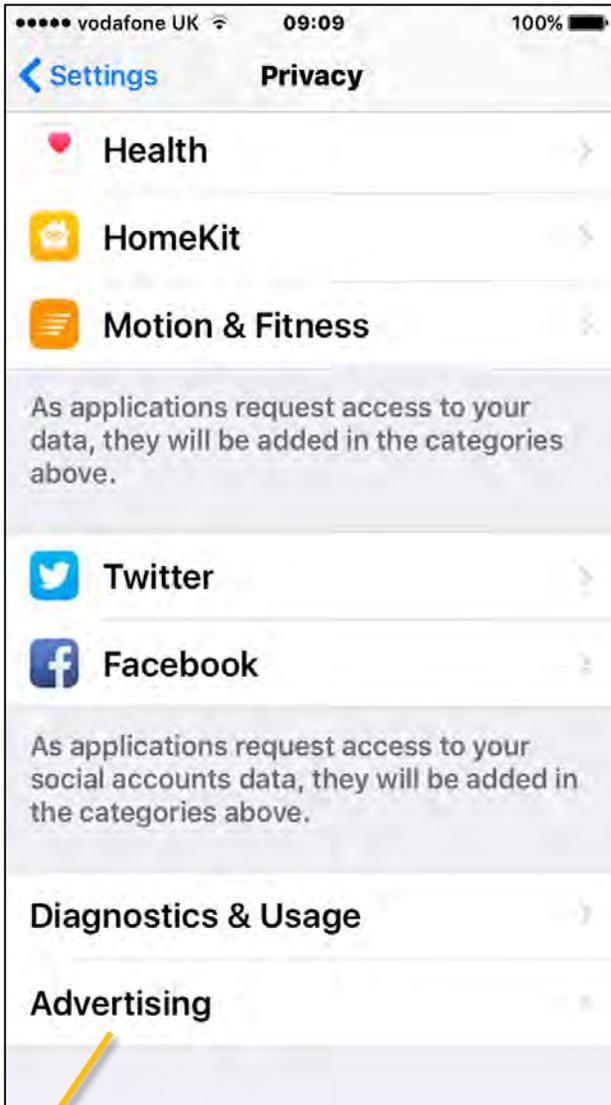


3

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.



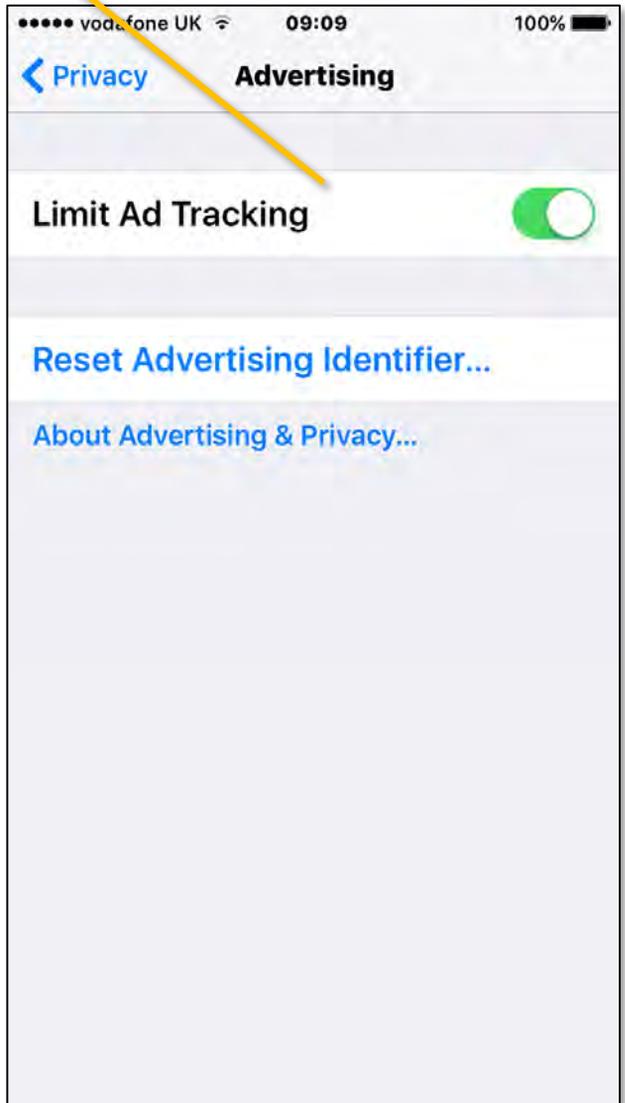
# Privacy – Ad Tracking



*Return to 'Privacy' and scroll down to 'Advertising'...*

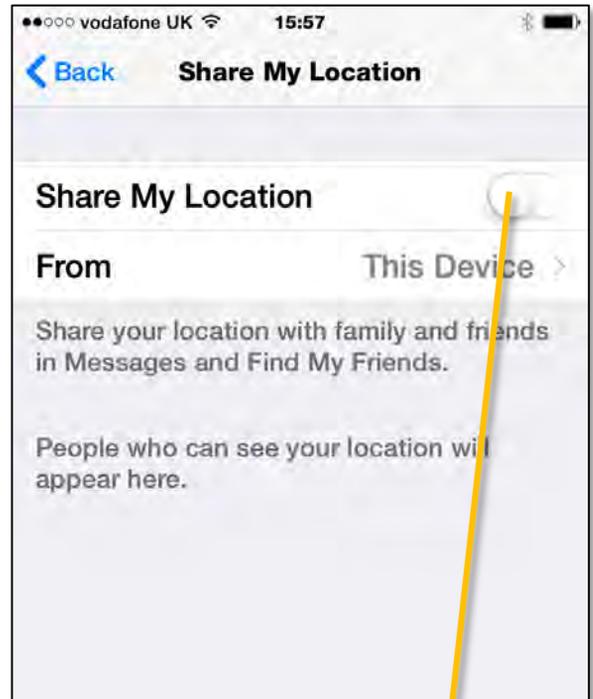
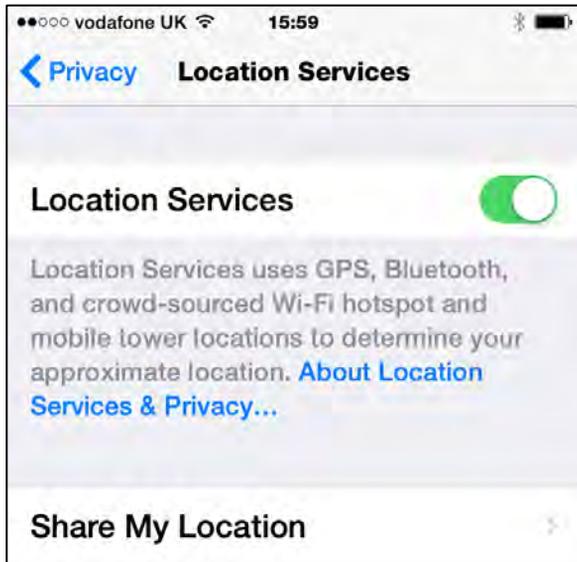


*To limit the amount of data collected by Apple, turn 'Limit Ad Tracking' ON.*



# Share My Location

Share My Location



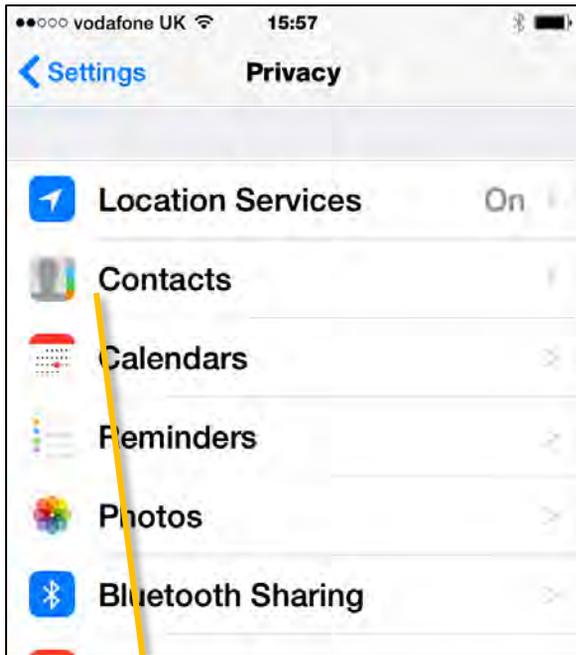
Set *Share My Location* to **OFF**.



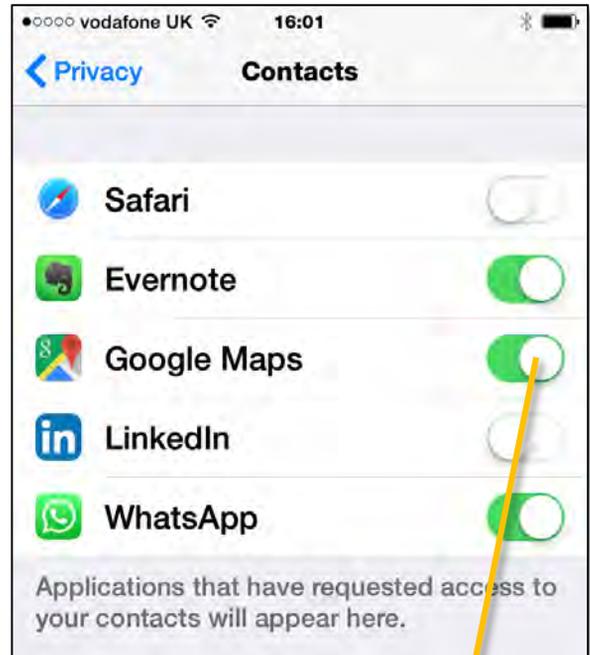
I was able to track the banker's location because he:

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

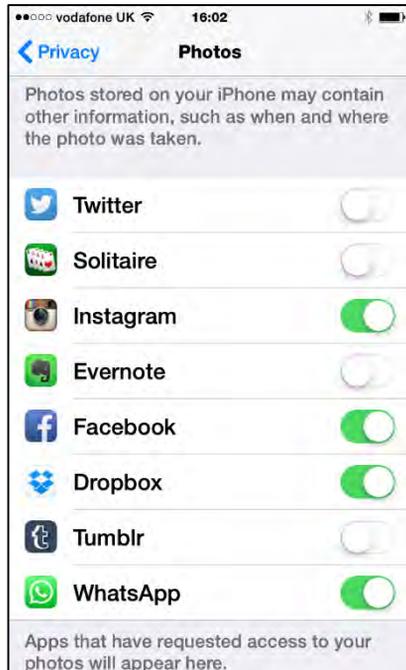
# Contacts



**1** Return to Settings/Privacy and select 'Contacts'.

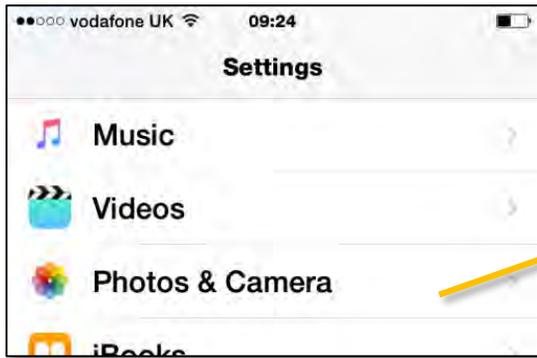


**2** Decide which Apps genuinely need to access your contacts list. Turn the others OFF.



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

# Photos and Camera

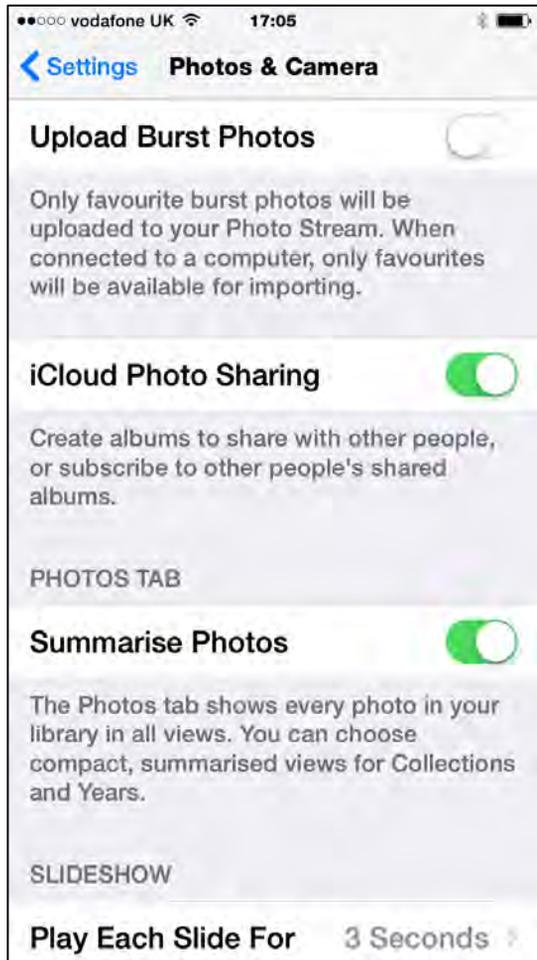


1

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



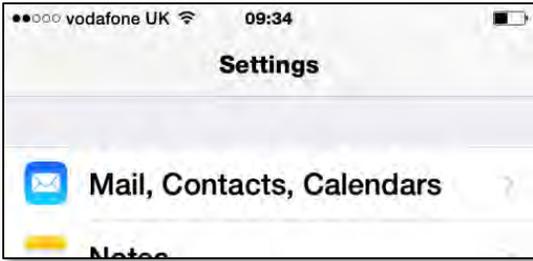
Off = safer



Off = safer



# Safari Browser



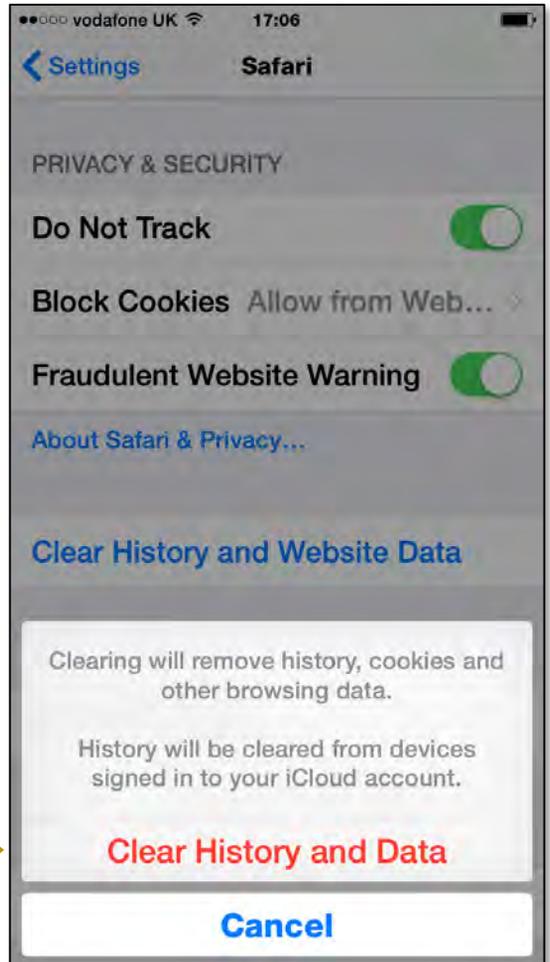
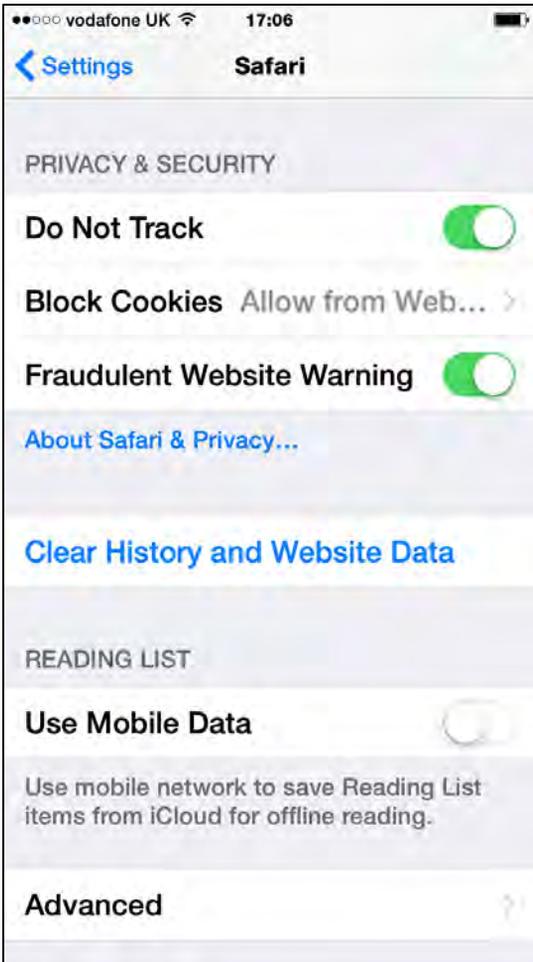
1

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



2

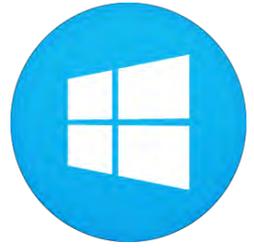
Tell websites not to track you, then clear your history and website data regularly to remove browsing history and cookies.



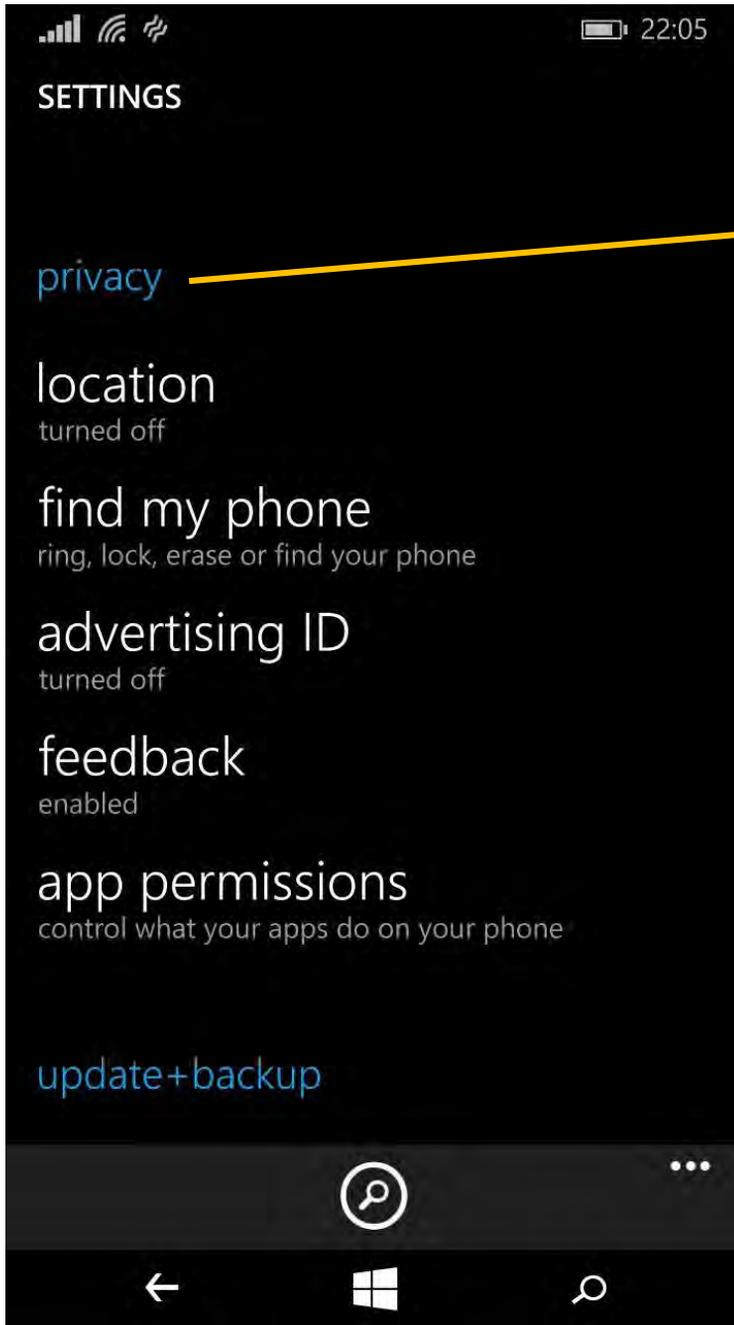
Regularly

# Secure Smart Phone

## Windows devices



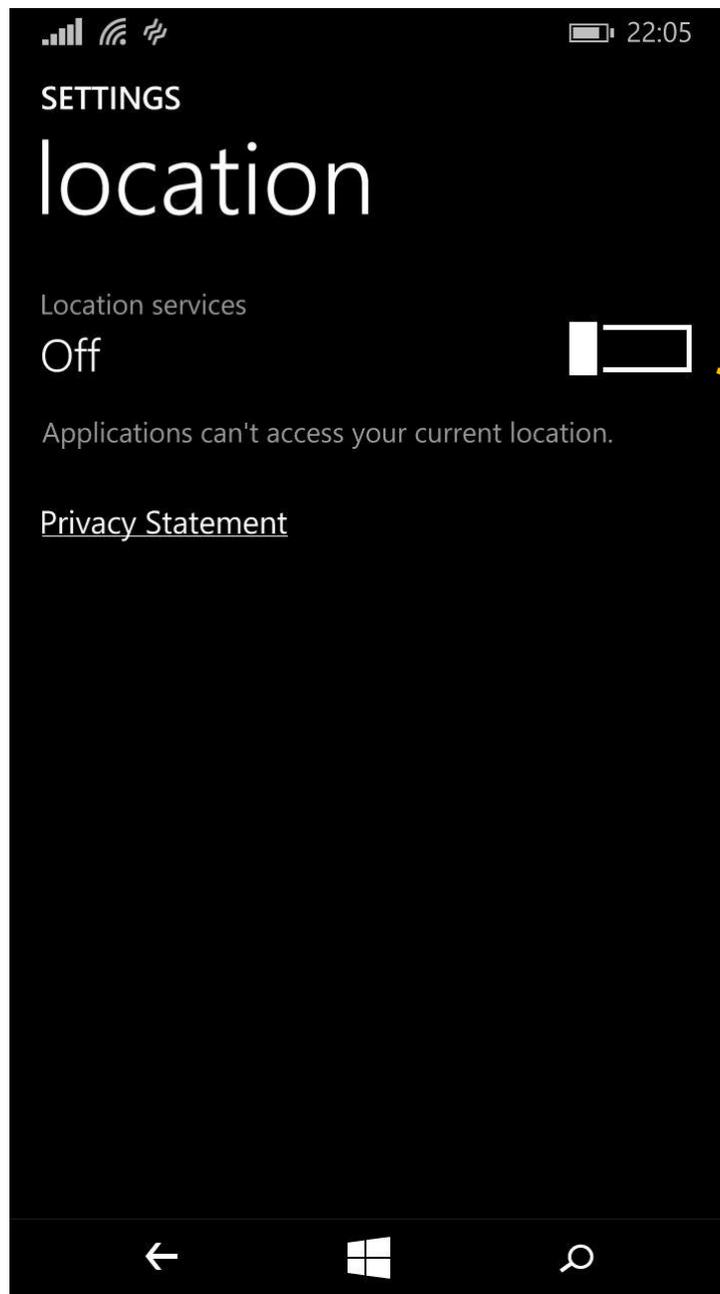
### Settings - Privacy



*Access and set each option as shown in the following pages*



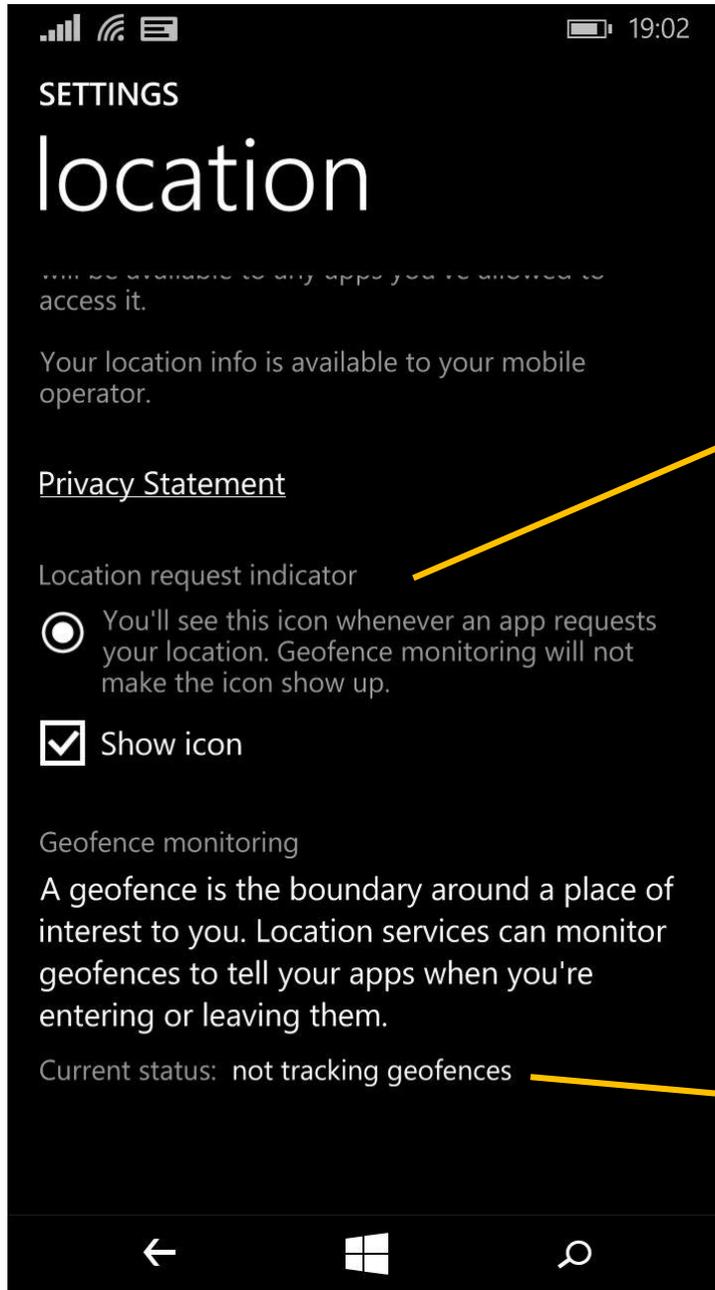
# Location services



*Turn Location Services OFF unless required*



# Location settings



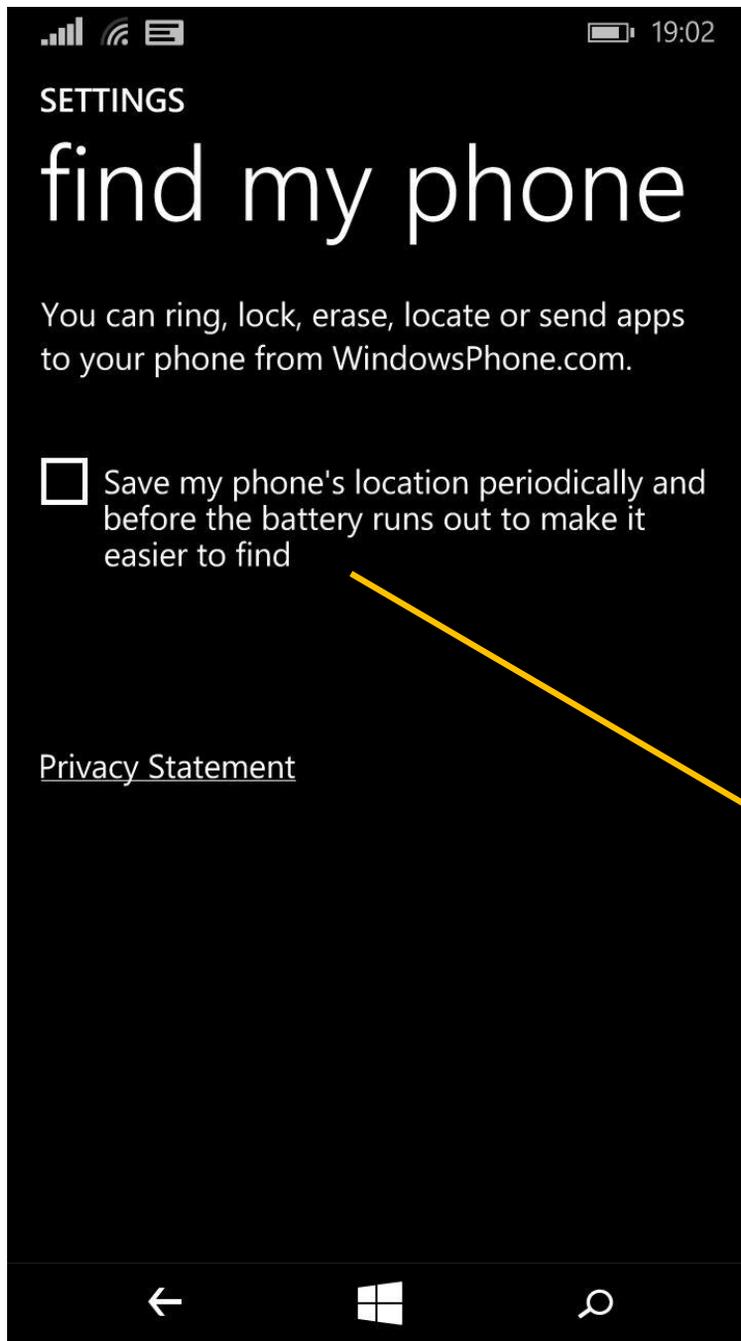
Turn request indicator ON



Turn Geofence monitoring OFF



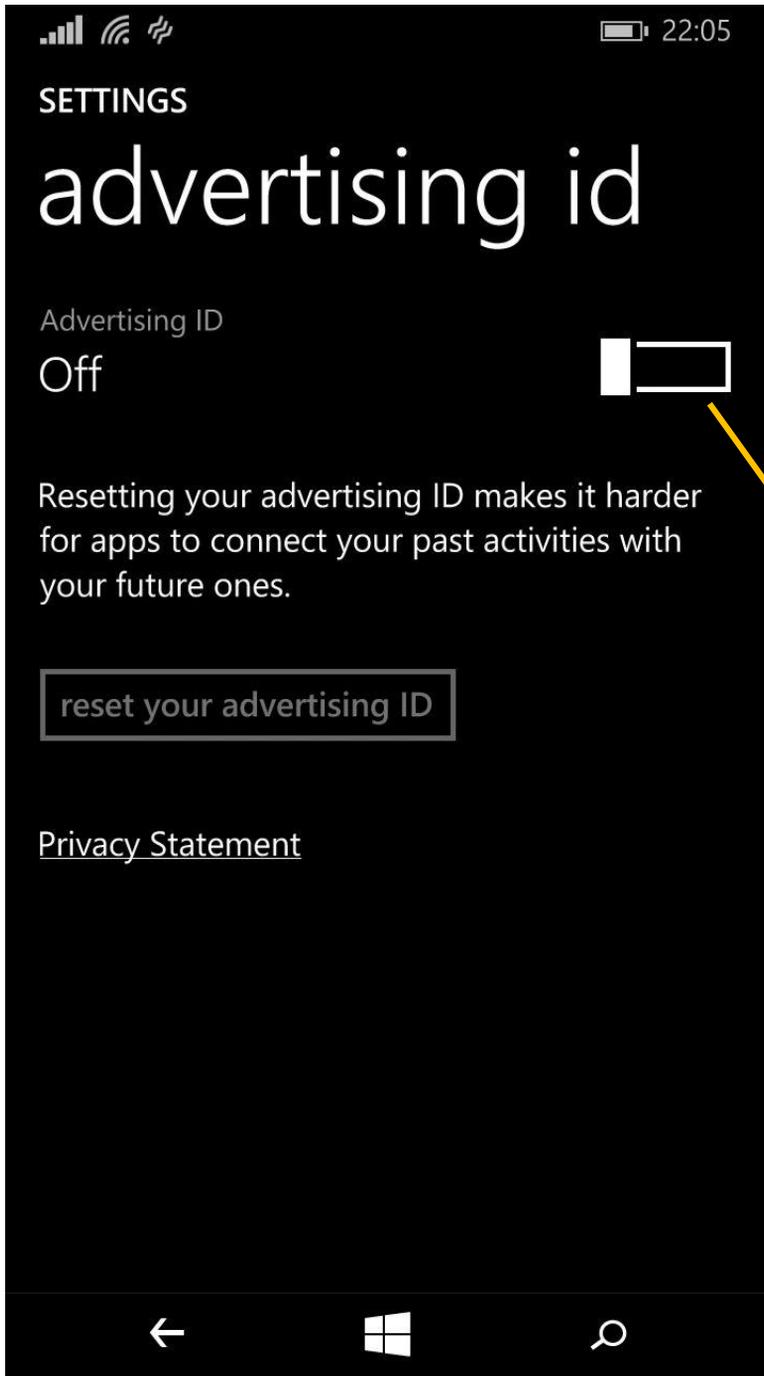
# Find my phone



*Set the saving of  
phone location OFF*



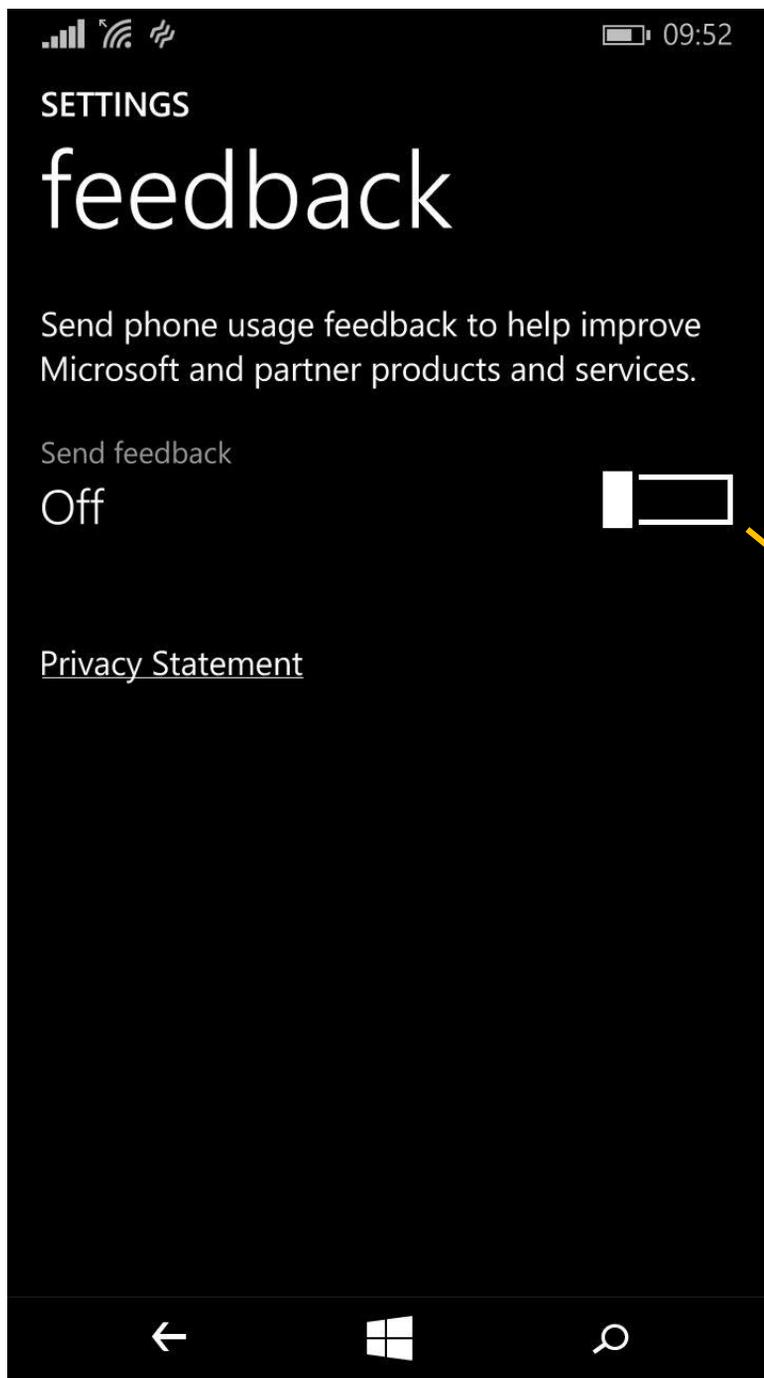
# Advertising ID



*Set Advertising ID to OFF*



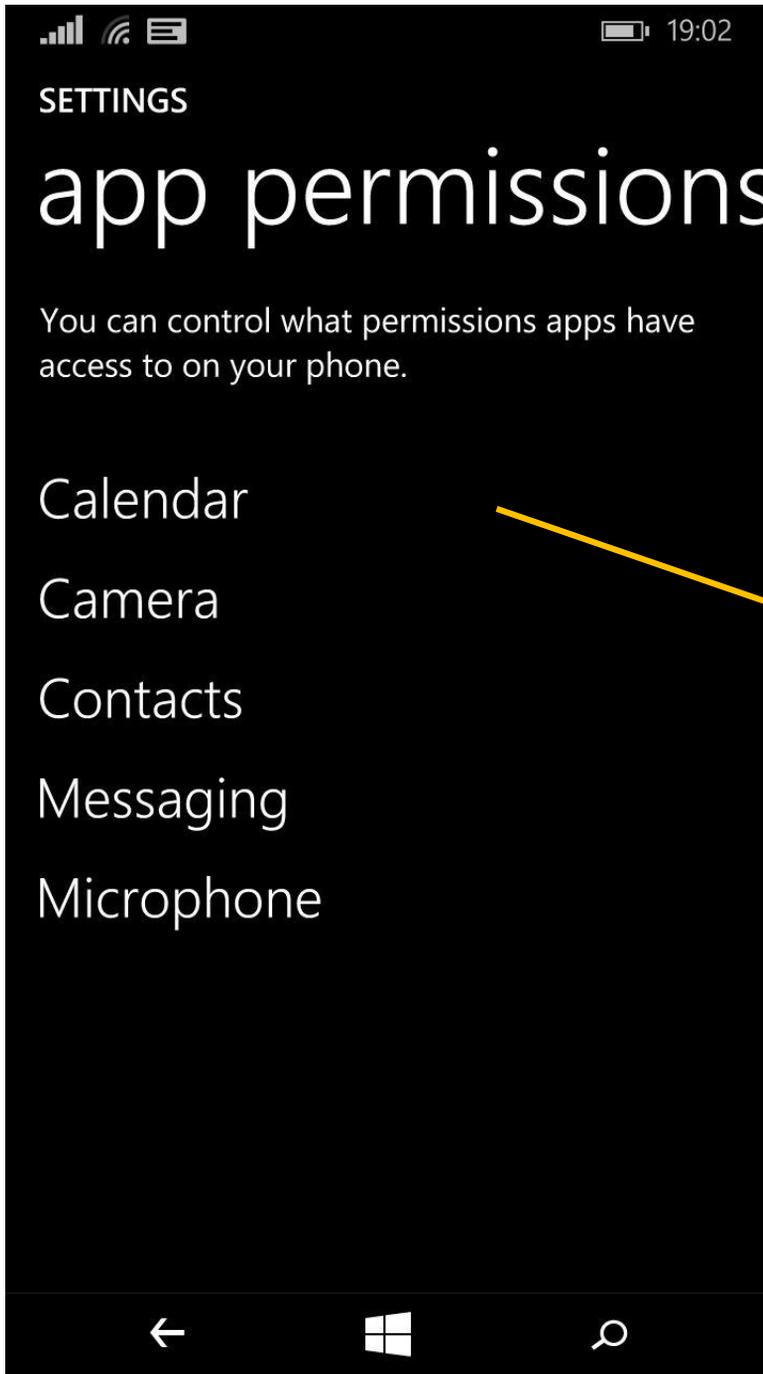
# Feedback



*Set Feedback to OFF*



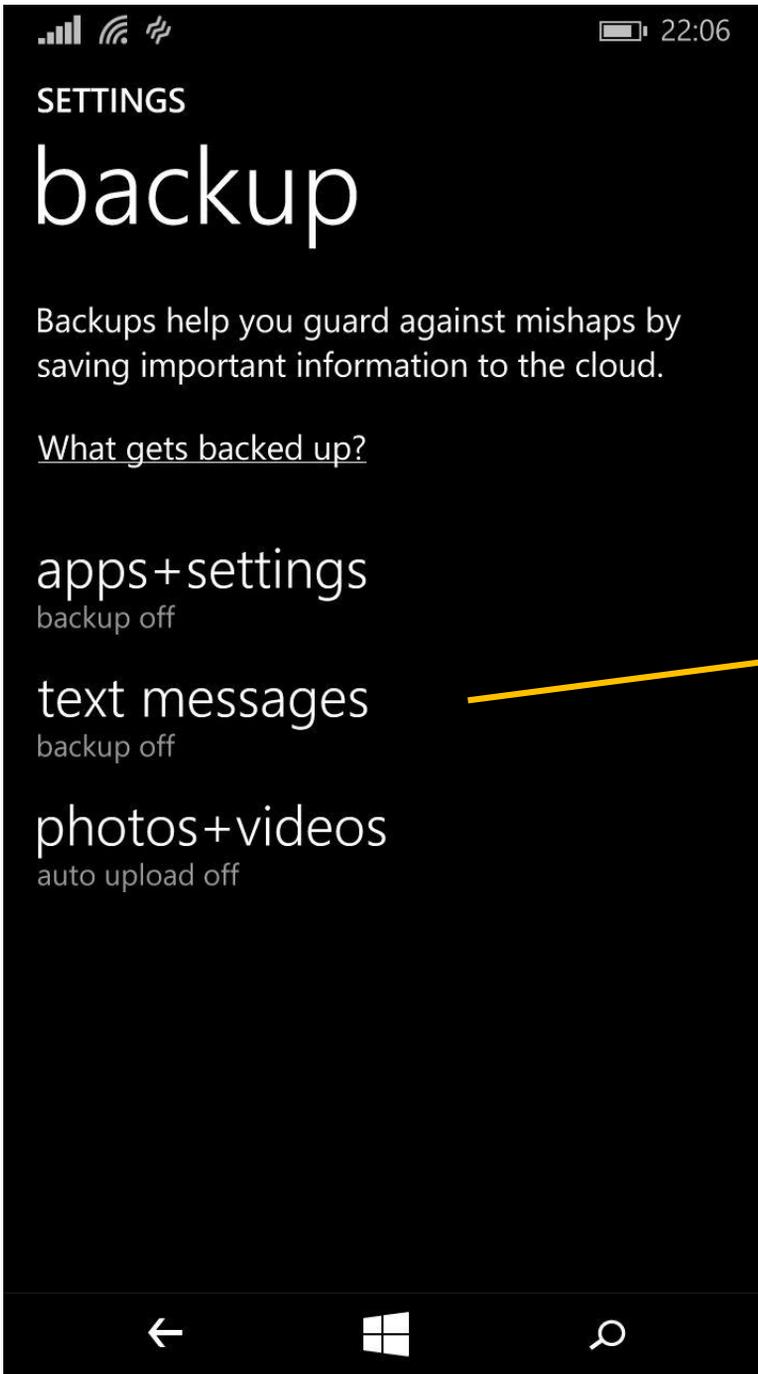
# App permissions



*Manage App permissions as shown in the following pages*



# Backup



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



# Credits

---



**Conceived and commissioned by Andrew Beet, National Policing DCG Futures Group**

**Written and produced by Mark Johnson, TRMG**

**OSINT Consultant, Esti Medynska, TRMG**

**Artwork supplied by Russ Daff and Nic Brennan, TRMG**

## 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.