Stay Secure Online 2016
A review of the privacy options currently 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.

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 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...

Find out all you can!

I have no choice.

About Eastern Online Bank...

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.

Hmmmm... here’s a guy...

Walkies later...

I’ll hang outside his office...

No walkies?
After several tries, she finally spots her man.

There he is!

The banker's is using a public WiFi hotspot during his break to send unencrypted emails to clients.

I'll use this WiFi hijacking toolkit...

Hacker girl uses a specialist toolkit to hijack the banker's WiFi connection.

Zap!

Bingo!!!
Back at home, Hacker Girl uploads the stolen emails and attachments to the crime gang...

Good first job, but we need his laptop?

Oh wow...

The gang wants more from her...

That's him!

Meanwhile, eOb clients have been defrauded and bank staff are being fired...

Nooo...

EOb hacked hundreds of jobs on the UK

I feel awful.

Hacker Girl has a chance encounter with her eOb target in the park. He looks very dejected.

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.
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”

<table>
<thead>
<tr>
<th><strong>Do</strong></th>
<th><strong>Don’t</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Use social media security settings.</td>
<td>1. Post personal details.</td>
</tr>
<tr>
<td>2. Turn off location services.</td>
<td>2. Use easily identified photos.</td>
</tr>
<tr>
<td>3. Secure your profile data.</td>
<td>3. Allow Apps to access your contacts or your location.</td>
</tr>
<tr>
<td>5. Use private browsing.</td>
<td>5. Save payment information.</td>
</tr>
<tr>
<td>6. Create a strong password.</td>
<td>6. Share your passwords.</td>
</tr>
<tr>
<td>7. Change your passwords regularly.</td>
<td>7. Leave devices logged on and unattended.</td>
</tr>
<tr>
<td>8. Use secure encrypted connections.</td>
<td>8. Use public WiFi for sensitive tasks.</td>
</tr>
<tr>
<td>9. Use only approved devices and networks.</td>
<td>9. Auto ‘check-in’ to hotspots or social feeds.</td>
</tr>
<tr>
<td>10. Search using a range of search engines, social feeds and languages.</td>
<td>10. Visit the profiles of persons of interest using insecure or personal accounts.</td>
</tr>
</tbody>
</table>
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 your IP address.

‘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.

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

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

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

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

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

Security Settings

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

Security: Login approvals

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.
Secure Facebook

Security: where you’re logged in

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

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

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
Secure Facebook

Privacy

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

Privacy Settings and Tools

<table>
<thead>
<tr>
<th>Who can see stuff?</th>
<th>Who can see your future posts?</th>
<th>Friends</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Review all your posts and things you're tagged in</td>
<td>Use Activity Log</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Limit the audience for posts you've shared with friends of friends or Public?</td>
<td>Limit Past Posts</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Who can contact me?</th>
<th>Who can send you friend requests?</th>
<th>Friends of Friends</th>
<th>Edit</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Who can look me up?</th>
<th>Who can look you up using the email address you provided?</th>
<th>Friends</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Who can look you up using the phone number you provided?</td>
<td>Friends</td>
<td>Edit</td>
</tr>
</tbody>
</table>

| 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.

2. Limit who can see your timeline.

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

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
Secure LinkedIn

Security: Profile photo & visibility

Restrict who can see your photo by selecting ‘Your connections’

Security: Archive of your data

Request your data 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'.
In 'Account' 'Third Party' section, you can view the apps you have authorised.

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.

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.

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.

DO NOT DATA SHARE
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.
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

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

Tweet location
- Add a location to my Tweets

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

Address book
- Manage your contacts

Personalization
- Do Not Track

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

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

Direct Messages
- Receive Direct Messages from anyone

Apply the Privacy settings as shown...
Password management

1. Now click here...
2. Choose a strong password* & change it frequently.

*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.

Time to open my password guessing app.
Notifications

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**

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.

**Manage your Apps**

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

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

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.

DO NOT CLICK UNLESS SURE!
Note: all screenshots taken from the Google.com site. Mobile apps may have differing features.

Google+ ‘Settings’

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

Scroll down the page for more settings options...

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.
To access ‘Settings’

1. Mouse over ‘Home’ to access the menu...
2. ...then click ‘Settings’

Posts and Endorsements

1. Restrict who can send you notifications to ‘Your circles’ or ‘Only you’.
2. Restrict who can comment on your posts.

Who can interact with you and your posts

Who can send you notifications? Learn more
Who can comment on your public posts? Learn more

Shared Endorsements

Off Edit

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.

   **Email:** js123456@gmail.com

   **Phone:** Add phone number

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

3. **Turn off subscriptions.**

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

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

   - 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

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

Manage apps & activities

Click to manage your apps and your activities log.

This is the most secure scenario.

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

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

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 for extended circles will see your +1s on posts and comments. People in your circles can view your activity. People you share with can view your activity.

Cancel Save
Customise “Your circles”

1. Click here.

When you share posts, photos, profile data and other things with “Your circles”, you’re sharing to all of your circles except the ones you’re just following. Think carefully about how widely you want to share your posts, photos and profile data.

2. Turn OFF automatic geolocation tagging and download permissions.

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

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

Location Settings

Set Location Sharing to OFF.

Disable Google

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

THE KILLER CAN’T HAVE ACTED ALONE. EVANS KNOWS HE NEEDS SOME EXPERT HELP.
DC Alison Kramer is Evans’ top investigator.

We’re definitely looking for two people...

First, I want to see the crime scene.

Kramer is an internet and communications specialist, but she knows the importance of physical evidence too.

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...

LOOK. THEY’RE FACEBOOK FRIENDS TOO.

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.
WE KNOW HEWITT RUNS TERRY DANGER’S DRUGS DEN…

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

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

DID SMITH VISIT HER?
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...

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!

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

Accessing Settings

1. Click here...
2. Then click here...

Location tracking

1. Select ‘Websites’...
2. Set to ‘Do not allow’ location tracking
1. Select ‘Privacy & security’...

2. Click Clear browsing data...

3. Decide what you want to clear and then click Clear browsing data.
Privacy & security

Settings

Privacy

- Clear browsing data...

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.

AutoFill

- Enable auto-filling of forms on webpages

Manage AutoFill settings

Passwords

- Offer to save passwords I enter on the web

Manage saved passwords

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

1. Deselect these options.
2. Select this option.
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

Access the menu as shown or press the Ctrl+Shift+Del keys to quickly clear your browsing history.
Take careful note of the site security badges displayed for each website you visit.
Accessing the Menu

Click here to access the menu...

Then select ‘Settings’
Accessing Advanced Settings

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.
Accessing Content Settings

Privacy

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

Set as shown to limit the data saved by cookies.

What has he been up to?
Control location tracking

Control which sites can track your physical location.

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...

How’s he going to explain that?
Content settings – Microphone & Camera

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...

Camera:
- Logitech QuickCam
- Ask when a site requires access to your camera (recommended)
- Do not allow sites to access your camera
- Manage exceptions...

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

Plugin access

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

Unsandboxed plugin access:
- 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...

Only expert users and administrators should adjust the other settings on this page.
Access ‘Clear browsing data’

1. 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

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

- Browsing history
- Download history
- Cookies and other site and plugin data
- Cached images and files
- Passwords
- Autofill form data
- Other
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

**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

1. Select ‘Search’...
2. Set this to ‘On’ for optimum search performance

Options - Privacy

1. Select ‘Privacy’...
2. Select to turn off tracking
3. Set to ‘Never remember history’
4. You can clear your current history (recommended).
Options - Advanced - General

- **Accessibility**
  - Set this to 'on'

Options - Advanced - Update

- **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

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.

Note: all screenshots taken from the .com site. Mobile versions may have differing features.
1. Select a ‘safe’ home page that does not imply any specific browsing habits.

2. Set IE to start with the home page.

3. Set to delete browsing history on exit.

4. Now click ‘Settings’.
1. Select the ‘History’ tab…

2. Set this value to ‘0’.

3. Select the ‘Caches and databases’ tab…

4. Deselect this option.
Select the ‘Security’ tab...

Choose the security level that suits your role.
1. Select the ‘Privacy’ tab...

2. Choose the cookie setting that suits your role.

3. Select all three settings as shown (recommended).
Internet Options – Content

1. Select the ‘Content’ tab...

2. Click ‘Settings’...

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

4. Click ‘Delete AutoComplete history’.
Select the ‘Advanced’ tab...

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.
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

Network connections
- Wi-Fi
- Bluetooth
- Data usage
- More networks

Connect and share
- NFC: Allow data exchange when device touches another device.
- S Beam: Send files via NFC and Wi-Fi Direct.
- Nearby devices: Share your media files via Wi-Fi, Wi-Fi Direct, or using Mobile hotspot.
- Screen Mirroring: Share your device’s screen with another device.
Secure Android

My Device

Settings

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

2. Turn off hands-free mode unless required.
Secure Android

Lock Screen

1. Set a lock screen PIN

2. Set automatic locking and power key locking to ON

Screen security

Screen lock
Secured with PIN

Secured with PIN

Lock screen widgets
Customise your clock and personal message.

Camera shortcut

Additional information
On

Lock automatically
Screen will be locked in 5 seconds after screen automatically turns off.

Lock instantly with power key
Secure Android

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

Backup and restore

Back up my data
Back up application data, Wi-Fi passwords, and other settings to Google servers.

Backup account
Js123456@hotmail.com

Automatic restore
When reinstalling an application, backed up settings and data will be restored.
Secure Android

Location and Application management

1. Turn off location services, unless required.

2. Review your installed Apps and remove any unwanted ones.
Secure Android

1. Press to access Security management

2. Review your device administrators

3. Disable unknown sources

4. Consider encrypting your device & any SD cards, if permitted

Device administrators

Unknown sources
Allow installation of applications from both trusted and unknown sources.

Encryption

Encrypt device
Password required to decrypt device each time you turn it on.

Encrypt external SD card
Secure Android

Security

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

Request local policy guidance for each of these settings.

SIM card lock will prevent the switching of SIM cards.

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

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

Make passwords visible

Show password characters briefly as you type them.

Do not make passwords visible
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’!

Security update service

Security policy updates
Increase the security of your device by updating the security policy.

Send security reports
Send security reports to Samsung via Wi-Fi for threat analysis.

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’!
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
Secure Blackberry

**Holstering lock**

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

![Holstering lock interface]

**Encryption**

1. **Now select Encryption from the Security menu**

![Encryption interface]

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

PIN Caching

Next, select Smart Card from the Security menu

Deactivate PIN Caching

Select Parental Controls and consider whether to activate
Secure Blackberry

Firewall

1. **Select Firewall**

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

1. Locate the Settings icon on your device and press it.

2. Only use trusted, secure WiFi networks.

3. Turn Bluetooth off unless needed.

4. Turn Hotspot off unless needed.

**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.
Secure iOS 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

1. Return to ‘Privacy’ and scroll down to ‘Advertising’...

2. To limit the amount of data collected by Apple, turn ‘Limit Ad Tracking’ ON.

As applications request access to your data, they will be added in the categories above.

Diagnostics & Usage

Advertising

Limit Ad Tracking

Reset Advertising Identifier...

About Advertising & Privacy...
Secure iOS

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.
Secure iOS

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.
Secure iOS

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

Clear History and Website Data

Clearing will remove history, cookies and other browsing data.

History will be cleared from devices signed in to your iCloud account.

Cancel
Secure Smart Phone
Windows devices

Settings - Privacy

Access and set each option as shown in the following pages.
Secure iOS

Location services

Turn Location Services OFF unless required
Secure iOS

Location settings

Turn request indicator ON

Privacy Statement

Location request indicator

You’ll see this icon whenever an app requests your location. Geofence monitoring will not make the icon show up.

Show icon

Geofence monitoring

A geofence is the boundary around a place of interest to you. Location services can monitor geofences to tell your apps when you’re entering or leaving them.

Current status: not tracking geofences

Turn Geofence monitoring OFF
**Find my phone**

You can ring, lock, erase, locate or send apps to your phone from WindowsPhone.com.

- Save my phone’s location periodically and before the battery runs out to make it easier to find

**Privacy Statement**

**Set the saving of phone location OFF**
**Secure iOS**

**Advertising ID**

- **SETTINGS**

  **advertising id**

  Advertising ID
  Off

  Resetting your advertising ID makes it harder for apps to connect your past activities with your future ones.

  - reset your advertising ID

  Privacy Statement

---

*Set Advertising ID to OFF*
Feedback

Send phone usage feedback to help improve Microsoft and partner products and services.

Send feedback
Off

Privacy Statement

Set Feedback to OFF
App permissions

You can control what permissions apps have access to on your phone.

- Calendar
- Camera
- Contacts
- Messaging
- Microphone

Manage App permissions as shown in the following pages
Secure iOS

Backup

Backups help you guard against mishaps by saving important information to the cloud.

What gets backed up?

apps+settings
backup off

text messages
backup off

photos+videos
auto upload off

Carefully consider what, if anything, you want to backup to the Cloud
Hacker Girl Episode Two

Will you be my friend?
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!

GOOD. BANKER WAS NOT FIRED...

GET HIS LAPTOP FOR ME.

BUT HOW???

BE HIS FRIEND. GET CLOSE!

I’LL NEED TO MEET HIM...

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

SHE IS PLANNING. GREAT!

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

HMMMM... MAYBE.

YES BOSS. OF COURSE SHE DO IT. IF NOT, SHE KNOWS - BYE, BYE!

MEANWHILE, THE GANG MAKES AN OVERSEAS CALL.
ACKER 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...

THERE HE IS AGAIN!

HE DOESN'T EVEN KNOW I EXIST!

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...

Try harder or... you know what!

Oh boy... Hmmm... music. I wonder...

Hacker Girl decides to try a different approach.
SEARCH ON FACEBOOK REVEALS THAT THE BANKER LIKES AN INDIE MUSIC BAND CALLED THE HOWLING MONKIES...

OMG... SERIOUSLY?

A QUICK TRIP TO THE SHOPS PRODUCES RESULTS...

THEY ACTUALLY STOCK THIS?

THAT LUNCHTIME HACKER GIRL ACCIDENTALLY DROPS THE CD...

OOPS!

LET ME...
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...
DO YOU WANT TO SEE SOME PICS OF MY DOG?

WOW! SHE LIKES DOGS TOO??

I LOVE DOGS!

YOURS IS SO CUTE!

YOURS IS BEAUTIFUL!

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

Now click the ‘My Account’ button.

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

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

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

3. Click ‘Try It’.

4. Enter the code you receive via SMS.

5. Click ‘Next’.
Secure Gmail

Configure 2-step verification

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

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

Finally, you will see this confirmation dialogue.

Backup verification options will be listed below the confirmation text.
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.

Settings

MY ACCOUNT

Name
Username
Birthday
Mobile Number
Email
Password
Login verification
Notifications
Snapcash

ADDITIONAL SERVICES

Manage

WHO CAN...

Contact me
View My Story
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

<table>
<thead>
<tr>
<th>ACCOUNT ACTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear browser data</td>
</tr>
<tr>
<td>Clear Conversations</td>
</tr>
<tr>
<td>Restore purchases</td>
</tr>
<tr>
<td>Blocked</td>
</tr>
<tr>
<td>Log Out</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>ACCOUNT ACTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear browser data</td>
</tr>
</tbody>
</table>

Are you sure you want to clear browser 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.