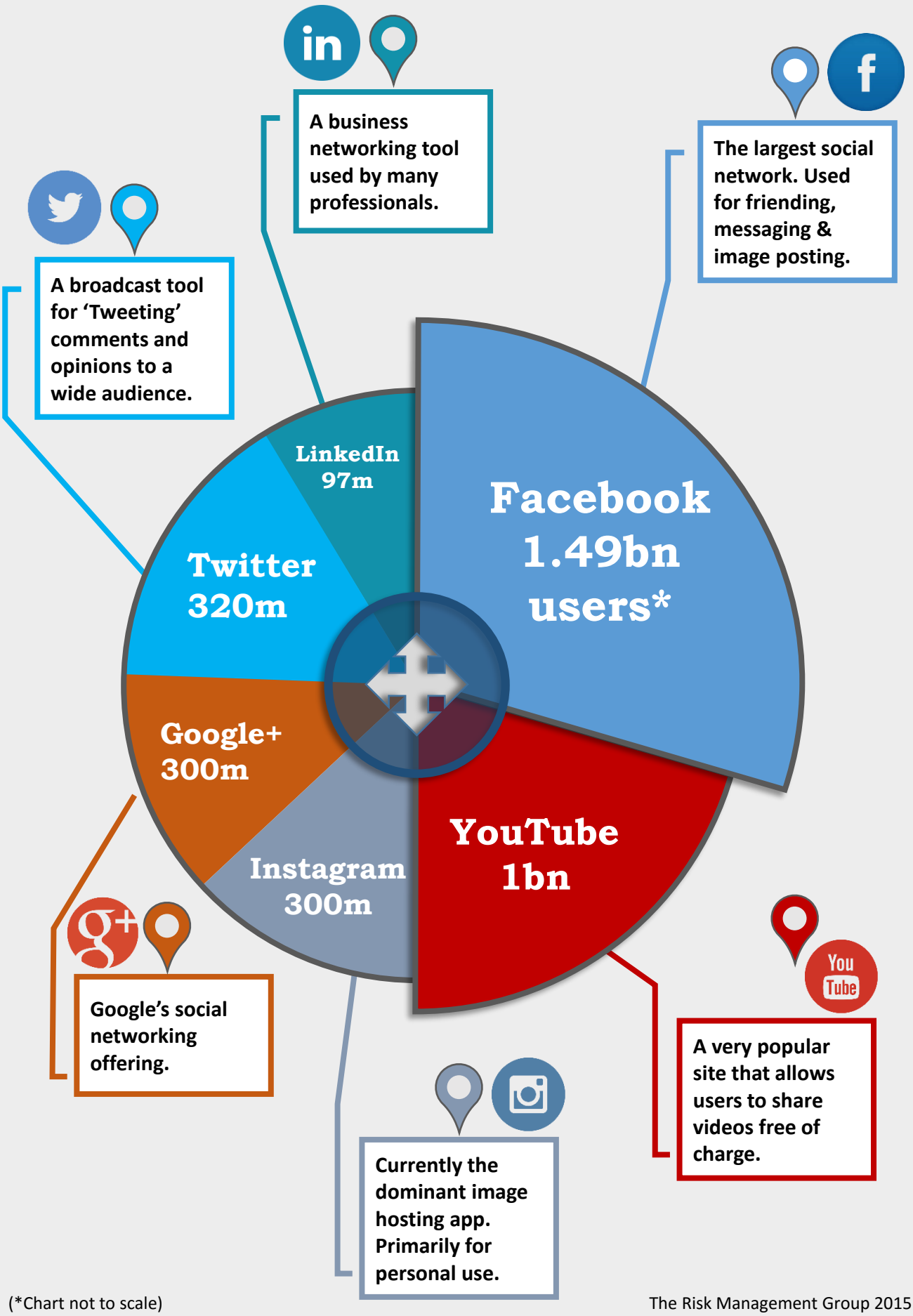
Issued by the National Policing DCG Futures Group
2015

# Secure Social Media

## Top 10 Do's and Don'ts

## 1. Prominent social media apps




(*Chart not to scale)



Contact
DCGFutures@met.police.uk

**This document only describes the privacy options available to users.**

NPCC National Police Chiefs' Council

# 2. Ten social media "Do's and Don'ts"

## Do

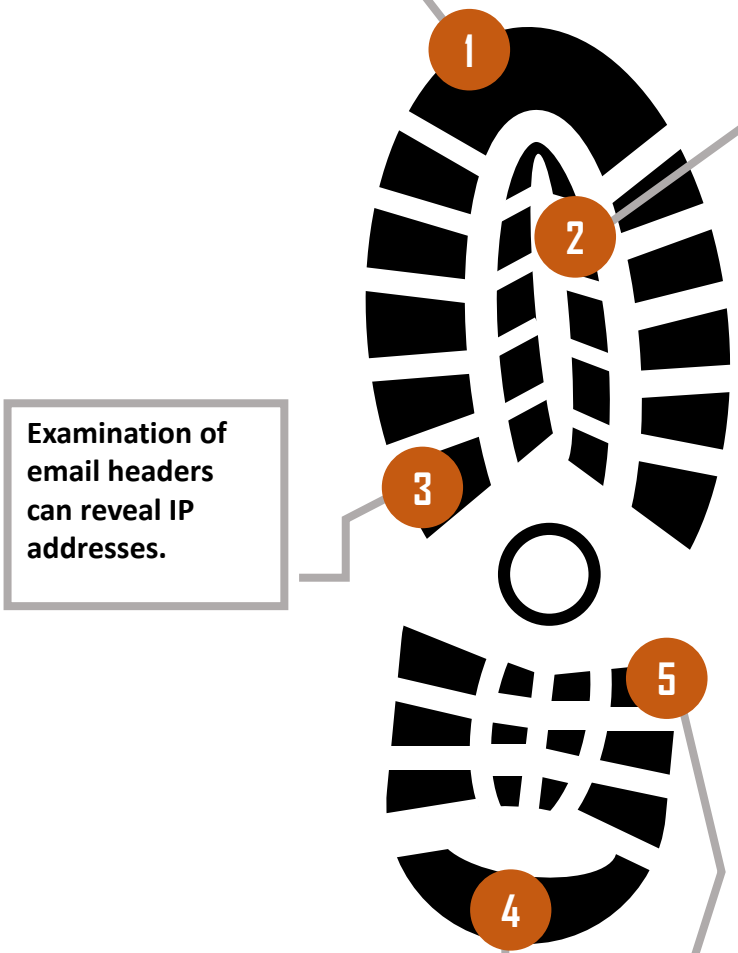
1. Use social media security settings.
2. Turn off location services.
3. Secure your profile data.
4. Limit your search 'footprint'.
5. Use private browsing.
6. Create a strong password.
7. Change your passwords regularly.
8. Use secure encrypted connections.
9. Use only approved devices and networks.
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.

# 3. Understanding your online footprint

The Risk Management Group 2015



1. Online activity is recorded by visited websites, or by spyware on infected devices.
2. Geo-location data, check in and travel updates on social media and other sites may be published online.
3. Examination of email headers can reveal IP addresses.
4. Insecure network connections, such as some public WiFi services, can expose users to interception.
5. '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!

# 4. How a criminal might investigate *you*...

Criminals search LinkedIn for anyone whose job title says 'intelligence' or 'investigator'.

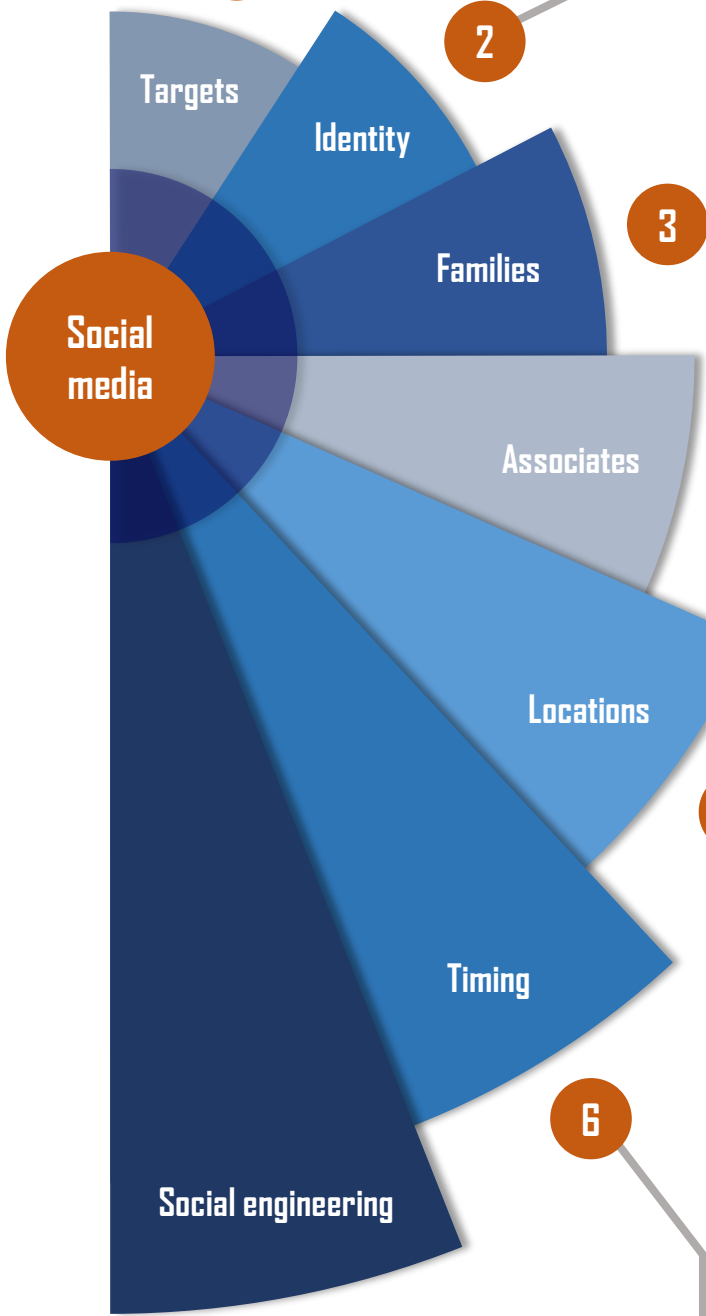
1

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

2

They check Facebook for family details and pages that might hold other intel.

3




4

Using LinkedIn, they connect with targets in order to view their connections.

5

If the target has location services turned on, criminals might find geo-tagged Tweets, images or posts.

6

Based on posts and geo-location intel, criminals can guess when a target is likely to be at certain locations.

7

Criminals might also attempt to trick their target into revealing sensitive information.

**If you are an investigator, you are also a target!**