Ministry of Defence

Cyber Security
Location Services

Mobile devices and social media are great for finding restaurants and other facilities near you, and there are apps which help record your fitness activities, as well as the value of sharing photos with family and friends online. But are you sharing more than you intend to?

Simple points to remember:

1. Think about what you are posting online and review your privacy and security settings regularly.

2. Follow the rules for wherever you are – such as not using mobile devices.

3. We are all responsible for protecting all Defence assets, including information. Report any concerns about information you find online immediately.

What are location services?

In short, anything with location data attached to it – so obviously apps which show directions from where you are, but also digital photographs, fitness and online dating apps, some aspects of social media and even mobile games. And the list goes on …

Mobile devices "know" where they are by using Global Positioning Services (GPS) – that's great for apps which help you find your way around, but there can be a downside if you don't think about what you are posting and where you are checking in.

Photographs from mobile devices like smart phones, for example, include metadata which describes where and when a photograph was taken and even what device it was taken with. It's the digital equivalent of the captions we used to put in photograph albums or write on the back of the print (eg "Edinburgh Castle, 17 August 2006") – except that it's automatic, so you don't need to do anything, and more precise, so it records exactly where you were when you took the picture.

Fitness apps like Strava and MapMyRun will track your progress in training, identifying where and when you have cycled or run, and how you have performed against previous rides or runs – and how you have performed against others.

And of course there is the option of "checking in" at wherever you are to help your friends know where to find you.

All these are examples of what is called "geotagging" – attaching location data to what you are doing.

What is the Risk?

Publicly announcing where you are presents obvious risks to personal security. While you may be happy for your friends to know, unless your social media profiles are protected then anyone can see it, and you could be cyberstalked. And when you check in to that restaurant in Madrid, or post the photos you took on the beach in Thailand earlier today (and the metadata will give the date), then you might be unintentionally telling a thief that you aren't at home (and are unlikely to be tonight).

Pattern of life information can also be gleaned from checking in and fitness apps if you visit the same bar every Thursday evening, or run the same route every Tuesday lunchtime – and if your run starts and ends at a military location then anyone (including those with ill intent) would probably be right in guessing you have a connection with the military. There have been recent occasions when information on Strava.com not only showed routes starting and ending on bases, but also linked to Service personnel profiles and even to a unit club which listed its members (with photographs). This presents a clear risk to PERSEC.

OPSEC can also be compromised, for example when postings are made in theatre. It is not difficult for an adversary to search for photographs taken in an area and use these to identify facilities to target. The US military have admitted to being targeted as a result of geotagging, including from photographs posted by their personnel in theatre. The US Air

Force has claimed to have used information on social media to target an ISIS HQ.

So what can I do?

Think about what you are posting, including what you might be giving away inadvertently. Review your privacy and security settings for all sites and online apps and don't link everything back to a single social media profile (eg your FaceBook page).

- Don't assume that others want their details made public – this might be colleagues, club members or even family – and don't check them in or post their details without permission.

- Turn off the GPS facility on your device when you don't need it.

- Consider where you might be giving away pattern of life information that could put you or your colleagues at risk.

- Keep to any rules about not using mobiles devices or cameras at specific locations or on operations – the rules are there for a reason.

Remember that you are personally responsible for securely handling any assets, including information, entrusted to you. So think about the potential impact of information about Defence assets, including images and location data, on military and operational activities.

Get Safe Online has good advice to help you protect yourself against cyberstalking and an informative blog about keeping safe on social networking and with location services.

For more Information visit:
DI: Ministry of Defence > Policy and Guidance > Security
WWW: www.getsafeonline.org

For further information on Acceptable Use of Defence IT and Telecons, contact:
ISSSPP-JSP747enquiriesmailbox@mod.gov.uk

Reporting Cyber Issues:
If you have a cyber security concern at work report it to your TLB WARP, contact details for which can be found visiting:
DI: Ministry of Defence > JFC > Chief Information Officer > ISS > DAIS > JSyCC
If you think you have received a phishing email on DII then forward to SPOC-Spam(Multiuser)
If you cannot access DII or remember the detail of your TLB WARP call the SPOC on 188