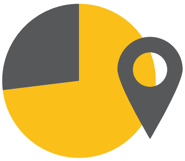
COUNTERINTELLIGENCE TIPS

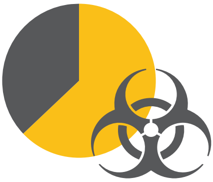
SOCIAL MEDIA SAFETY

Many social media and networking applications provide geolocation services to help identify potential matches in a particular area. Adversaries could easily use this capability to track or arrange a meeting with an unsuspecting target individual. To mitigate geolocation issues, almost all Social Networking Sites (SNSs) have a "check-in" component intended to facilitate meeting face-to-face. In most cases, you can disable this function on your device or limit it to sharing with friends or friends of friends.

In February 2015, IBM published a study that found:



73% of the 41 popular dating apps analyzed had access to users current and past geolocation information.



26 of the 41 (63% percent) dating apps analyzed on the Android mobile platform had either medium or high severity vulnerabilities (e.g., virus susceptibility, potential access to a phone's camera or microphone, unauthorized access to billing information, etc.)

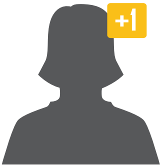
CREATE A SAFER PROFILE WITH SOCIAL MEDIA DOs AND DON'Ts

Consider the following best practices when accessing Social Media apps:

- Do not trust unsolicited messages that appear to be from trusted sources. Hackers regularly break into accounts or create persons to trick their targets into trusting them. Confirm the message's validity if it seems suspicious.

Know the Risk
Raise your Shield

- Create strong passwords.
- Phishing scams, viruses, spyware, and other unwanted software can spread through a Social Media network and infect workplace networks and compromise sensitive information.
- Status updates, photos, and comments can reveal more information than intended. Never post Personally Identifiable Information (PII) such as addresses, birthdates, phone numbers, or future plans, such as vacations or business trips. Even your comments or "likes" on a friend's site or a public site such as a TV show, car, or band may be seen by a terrorist or foreign intelligence service and allow them to target you.
- Be cautious of social networking service links to games, quizzes, and other applications that may access your information.
- Many smartphones geotag photos with metadata that reveal the exact location where the photo was taken. You should check account settings to ensure this information is not public.
- Limit requests to individuals you trust; never accept friend requests from someone you do not know, even if they are a friend of a friend. If possible, validate friend requests through other sources (e.g., phone, e-mail) before accepting them.
- Limit who can view your friend list.
- Go to your own page without logging in to the site to observe what a non-friend can see.
- When you add a Social Media site as your access point to other Internet sites, those services often ask for permission to access your friend list and other personal information. Understand that this can jeopardize your own information, as well as that of your friends.
- Although a Social Media site may be set up to quickly expire or delete messages (such as Snapchat), a foreign intelligence service can mine this information via "man-in-the-middle" attacks before it even gets to the provider. Assume that if you send it on the Internet, someone can get it and keep it **forever**. The interest in retaining your information goes up exponentially with your association with the government.
- Many foreign intelligence services "own the Internet" in their countries and would have a strong interest in your online behavior or any information you share while online.



INTERNET RESOURCES

OnGuardOnline.gov
Operated by the Federal Trade Commission (FTC), this site provides tips and technical guidance on cybersecurity issues as well as a guide for talking to children about Internet use.

StaySafeOnline.org
Offers resources on a variety of cybersecurity issues, including information on adjusting privacy settings on a number of popular platforms.