U.S. Army Information Technology Agency (ITA)

Strategic Communication Message, December 3, 2010, ITA, Pentagon, Washington, DC

Creating Connections

Cyberchasing & Geotagging – The Dangers of Posting Your Physical Location Online

ITA is pleased to provide this information update as part of our commitment to support your information assurance efforts. This holiday season, as you travel and have family gatherings, you may be tempted to stay current with your online friends and post photographs and videos of your time away from home. Or you may have recently started using a social networking site that encourages you to 'Check In' to various physical locations just as your friends have. The purpose of this bulletin is to raise awareness regarding cybercasing which is a term used to describe how criminals can make use of geographical information that you post online to mount a real world attack on you or your home when you are away.

Most smartphones now contain the GPS technology which automatically adds geographical data to the images and videos that you capture using your phone. This feature, known as Geotagging, is available by default and most users are not aware of its presence and that it can be turned off. Therefore, you are posting the exact location of where you are currently located when you post an image of yourself on holiday for hackers to see. Additionally, you are announcing to would be attackers that you are currently away from home.

Another way cyber attackers can stalk your movements is if you use a social networking site that has application that allows you to 'Check In' to a physical location. This social networking tool is quickly gathering momentum and is another way that users inadvertently post information about their whereabouts to hackers. The Places Application on Facebook is an example of this feature, and has been the target of terrorist activity in the South West Asia region when used by British forces using mobile phones. Foursquare, Gowalla, Yelp, BrightKite, Where.com, Booyah and Loopt are all examples of location based social networking sites where the information that you post online can be used by hackers in cybercasing attacks.

How can you protect yourself?
You can take measures to protect yourself by understanding the GPS features available on your smart phone and make sure that it is turned off when you capture photographs and videos which you post online. Do not use location based social networking sites to announce your whereabouts to the world. This can place yourself, your family or your home at risk. Another way to protect yourself is to simply wait until you return from your vacation to post your photos online. This way, you are not announcing to would be burglars that your home is unattended when you are away.

ITA ESS-P delivers monthly information assurance awareness updates as a service to our customers.

Respectfully,
ITA Information Assurance
NIPR: ITAIA@conus.army.mil; SIPR: ITAIA@hqda-s.army.smil.mil
ITA's website: http://ita.army.mil

Reference: AR 25-2, Para. 2-8(g)
Classification: UNCLASSIFIED
Caveats: NONE