Five Tips to Using Online Location-based Services Safely : AVG (AU/NZ)

Don’t Make it Easy for Criminals to Learn too Much About You

Across generations there have always been those who just don’t trust new technologies. It happened with radio, TV and more recently with the Internet. In the case of the latter, a little distrust would serve us well — especially when it comes to sharing information about ourselves on Facebook, Twitter, LinkedIn, Foursquare and other social media outlets.

As social networking continues to evolve, location-based services such as FourSquare and Facebook Places have developed. The evolution of social networking and geo-tagging means learning how to protect one’s online privacy becomes critical. Most people would be surprised to discover that when they upload a picture from their smart phones to Twitter, that picture is encoded with the latitude and longitude of the picture’s location. This data can then be used to match your geographic location with a business, home or other public place via Google Maps (see ICanStalkU.com).

Peter Cameron, Managing Director of AVG (AU/NZ), says: “By themselves, certain shared facts may seem harmless enough. But disparate pieces of ourselves can easily be assembled like puzzles to create holistic pictures of our daily lives. Don’t make it easy for criminals — follow these tips to protect yourself.”

1. Don’t post pictures online. If you must, make sure they can only be viewed by those you trust. There are privacy features on Facebook that will let you do this, but remember there is nothing to stop your contacts from copying and pasting pictures openly elsewhere.
2. If you want to share location or other personal info on Twitter, or you’re afraid of inadvertently giving away too much, create a separate network just for those you know and trust, and set the privacy setting to protected. But again, nothing prevents your contacts from publicly retweeting your updates.
3. For your larger online networks, always consider how someone might use posted info against you before you post. It is also a good idea to regularly look back on what you’ve posted to see how updates might be combined together to indicate where you live, work or go to school.
4. If you have a smart phone, disable the geotagging feature. But if you must use location-based services such as Foursquare, never “check in” from home as this will disclose your address.
5. Google yourself to see what others can find out about you online. Be sure to remove yourself from Spokeo and other aggregators of personal content.

Earlier this year we learnt about the so-called Bling-Ring, where some LA kids targeted celebs’ homes, robbing them of A$3.6 million worth of jewellery, artworks and designer clothes. Some of the celebrities burgled were Orlando Bloom, Megan Fox, Lindsay Lohan and Paris Hilton.

The teenage gang used Google Earth to locate and survey the homes and find ways in. For example, Paris Hilton lived in a gated community, but the kids found via Google Earth that there was a gully that went under a fence, and when they went and looked, found they could easily walk right in.

Then they simply watched Twitter until Paris announced that she was going out, and walked right up to her house. They found a key hidden near the door and returned to Hilton’s house five times.

“A little bit of extra care can help protect you from the baddies out there,” Cameron says. “After all, you wouldn’t hand out your address and personal details to strangers in the street, so don’t do it in the online world.”

AVG (AU/NZ) has a comprehensive range of security tips on its web site at http://www.avg.com.au/resources/security-tips/.

ENDS

About AVG (AU/NZ) Pty Ltd — www.avg.com.au

Based in Melbourne, AVG (AU/NZ) Pty Ltd distributes the AVG range of Anti-Virus and Internet Security products in Australia, New Zealand and the South Pacific. AVG software solutions provide complete real-time protection against the malware, viruses, spam, spyware, adware, worms, Trojans, phishing and exploits used by cyber-criminals, hackers, scammers and identity thieves. AVG protects everything important and personal inside computers — documents, account details and passwords, music, photos and more — all while allowing users to work, bank, shop and play games online in safety.

AVG provides outstanding technical solutions and exceptional value for consumers, small to medium business and enterprise clients. AVG delivers always-on, always up-to-date protection across desktop, and notebook PCs, plus file and e-mail servers in the home and at work in SMBs, corporations, government agencies and educational institutions.

Talk to Us

Siobhan MacDermott
AVG Technologies – Investor Relations

E-mail: siobhan.macdermott@avg.com
US Mobile: +1 415 299 2945
CZ Mobile: +420 725 695 132

For more detailed information please contact:

Lloyd Borrett AVG (AU/NZ) 03 9581 0807
Shuna Boyd BoydPR 02 9418 8100

Media resources, including logos, box shots, screen shots etc., are available online at: http://www.avg.com.au/media

Join the AVG Community for information, video content and pictures: http://www.flickr.com/photos/officialavg/sets/