

Bad guys can learn plenty from those photos you post

.....
By Steve Johnson SAN JOSE MERCURY NEWS

SAN JOSE, Calif. — Whipping out your smartphone to snap and post online pictures of yourself and your kids relaxing at home — or perhaps that pricey new TV you just hung on your rec-room wall — is like throwing chum to a sea of hungry sharks.

That's because smart-phone images can be deciphered to reveal precisely where the photos were taken, which security experts say could lead burglars and other criminals directly to your front door. Similarly, they add, posting images from vacation sites or your workplace could invite crooks to ransack your house while you're away.

“That can be sharing a bit too much,” said Con Mallon, senior director of mobility for the security firm Symantec. “They can then put the location of where you are now and where your

house is into a maps program and work out how much time they have to pay a visit while you're out.”

Smartphone photos are embedded with “geotags” containing the latitude and longitude. This data isn't visible to the naked eye. But when deciphered with the help of photo-sharing websites, various apps or other methods, those coordinates can enable someone using Google Maps to identify the precise spots depicted in the images.

That also makes the technology useful, for example, for someone with scads of photos who can't otherwise remember where some of them were taken. And sharing geotagged photos online has become so commonplace that many people hardly give it a second thought.

“I'm OK with it,” said 25-year-old Roilo Escalada of Santa Clara, Calif., who is studying kinesiology at San Jose State and occasionally posts pictures with his iPhone. “I don't have any stalkers. I feel safe.”

But geotagged photos have posed unanticipated problems for even the most computer-savvy people.

That includes John McAfee, founder of the antivirus software company that bears his name. After McAfee eluded Belize authorities, who were seeking to talk to him as a “person of interest” in the 2012 shooting death of his neighbor, his location was revealed when a photo of his Guatemalan hideout was posted online.

Some Web commentators say that concerns about geotagged smart-phone photos are unwarranted, noting that millions of people routinely post them without being victimized. Nonetheless, the National White Collar Crime Center, a

nonprofit organization that helps police combat economic and tech-related crimes, has cautioned that placing such pictures on the Internet can be dangerous.