TIMES DAILY www.TimesDaily.com

Oct 29, 2007

Police using technology

Law enforcement use social networking Web sites in the battle against crime

By Ambreen Ali,
Medill News Service

An attractive 20-something female pokes you on Facebook. You notice on her profile that she shares your passion for punk rock and grew up in the town where you went to college. You're intrigued, so you "poke" her back, giving her access to your profile.

What you don't know is the profile is run by the local police department. It's a virtual undercover cop, looking for access to your profile to find information that could implicate you in an investigation and give authorities access to your full name, phone number, list of friends, even where you work.

Web sites have been used by tech-savvy criminals for years as a way to recruit gang members and give signals to accomplices in robberies and bombings. But now, the everyday criminal has started leaving virtual footprints.

Online social networks, such as Facebook and MySpace, have provided unprecedented information about suspects: blogs that help explain criminal motivations, photographs of illegal activity, even posts by and to friends detailing where an individual was at a given time.

Russellville police used technology to try and development information for a case in which an adult man was trying to chat with an underage girl.

"We secured a search warrant and went into (the suspect's) e-mails to find some inappropriate messages that he had sent the victim," Lt. Scotty Lowery said.

Lowery said the case will be presented at an upcoming grand jury session for a possible indictment.

Florence police Deputy Chief Tony Logan said detectives were able to get information about a sex offender who had been trying to attract a potential victim by going online and looking at profiles.

"We try to use the technology just like the bad guys; you have to," he said.

"Technology has outpaced the law," Lt. Charles Cohen, of the Indiana State Police, told a group of 200 police officers at a suburban Washington conference on the use of social networking Web sites for criminal investigations.

Law enforcement officers say using these social networking Web sites is another tool in the battle against crime.

Lowery said the Web sites are good ways to find background on suspects or on potential victims.

"Some people will put their entire life story on their profiles, so it's there to check," he said.

Sheffield police Capt. Greg Ray said officers have used online social networks to check suspects for gang affiliation.

"We'll use every legal hook that we can, and I can see where this can be a useful tool for officers," added Muscle Shoals Police Chief Robert Evans.

Cops from all over the country caught up with the times at the Global Conference on Economic and High-Tech Crime in Arlington, Va., by learning how to collect evidence for investigations on suspects' profile pages.

Cohen loaded the MySpace page of a group that proclaims it hates cops as an example. If one of them goes so far as to kill a police officer, he said, this Web page can be used as proof of premeditation.

"The value of this information is that it shows intent to kill," he said. "This is the difference between lethal injection and life without parole or 30 years for murder."

Fans of detective thrillers will remember that the robber's role in a cops and robbers chase is to hide the trail he leaves behind. Why then are today's transgressors making their wrongdoings so public?

Sometimes the bragging is intentional. Michael Stefanone, assistant professor of communications at Buffalo University, studies the motivations for how people portray themselves online.

"If you boil away all of the technology and hype, just like 50 years ago, everybody more or less pursues attention," he said. "Attention is a form of social power."

Facebook started as a private network for college-age students, but has since opened up profile pages to Web searches and individuals not connected to universities. Users can control whether to prevent this default access.

Unlike MySpace pages, which users often create under pseudonyms, Facebook profiles are connected to verifiable e-mail addresses and users tend to use their full names, sometimes disclose where they work and even where they live.

Private profiles are only visible to friends, but the term is used loosely in this context: A "friend" could be anybody the user allows to access the Web page, including an undercover cop.

Private profile pages and messages can be accessed by serving warrants and subpoenas on MySpace and Facebook for access.

The companies can then lock a user out from changing or closing an account, or simply provide authorities a copy of the Web page and associated links, photos and private messages at a given time.

Regularly checking Web profiles requires time and money. Cohen's department uses analysts who monitor Web sites of interest hourly.

And if a criminal fears she is being monitored, a few clicks of the mouse can delete information forever.

Cohen's presentation concluded with a look at Second Life, an online virtual world where users can purchase virtual goods with real money. Linden dollars, the currency of this virtual world, can be used for money laundering since they can be exchanged for U.S. dollars.

"This is the future," he said.

So how will local authorities respond to crime in this virtual world?

Again, Cohen said, the law has not quite caught up: "This is something that has not been contemplated."

TimesDaily Senior Writer Tom Smith contributed to this report.
