Johns Creek

ALERT !!

September 15, 2015

The St. Johns County Sheriff's Office has reported a recent increase in the following crime and all residents are to take extra caution while on-line.

SWATting is the act of tricking an emergency service (via such means as hoaxing an emergency services dispatcher) into dispatching an emergency response based on the false report of an ongoing critical incident. **"Swatting"** is a prank often used by cybercriminals to harass a target by reporting nefarious activity like a hostage situation or active shooter at a person's location with the goal of getting a police SWAT team to respond and arrest them. It's not exactly a lighthearted prank, as sending in police officers who think they may encounter an armed suspect can be very dangerous.

Caller ID spoofing social engineering, TTY, prank calls, and phone phreaking techniques may be variously combined. 911 systems (including telephony and human operators) have been tricked by calls placed from cities hundreds of miles away or even from other countries. The caller typically places a 911 call ***(here in St. Johns County the calls were made to the non-emergency Sheriff's Office number)*** using a spoofed phone number with the goal of tricking emergency authorities into responding to an address with a SWAT team to an emergency that doesn't exist.

Examples of the types of calls made (from across the country) include:

- An unidentified Skype caller told police that he had shot his parents and was on a killing spree.
- A home was raided by local police after a call, purported to be from someone inside the house, said that there was a hostage situation at the residence. The caller had demanded a ransom of $20,000 and claimed they had planted explosives in the yard.
- 911 received a call claiming that his father had shot another family member with an assault rifle. A SWAT team attended the residence and discovered that it was a hoax.
- A 911 caller gave an address as his own and claimed: "I just shot my wife, so…I don't think I could come down there…She's dead, now…I'm looking at her…I'm going to shoot someone else, soon."
- An incident involved a 15-year-old boy from Naples, Florida who had his **X-Box** hacked by swatters who sent a message to the police saying he was stabbed and his family members were being held hostages.
- Another victim was playing an online game when a police team arrived at his house after they received a call, claiming to be from his daughter, saying he had shot his wife with a machine gun.

"People who make these swatting calls are very credible," an FBI Agent said. "They have no trouble convincing 9-1-1 operators they are telling the truth." And thanks to "spoofing" technology—which enables callers to mask their own numbers while making the victims' numbers appear—emergency operators are doubly tricked. Most who engage in swatting are serial offenders also involved in other cybercrimes such as identity theft and credit card fraud. They either want to brag about their swatting exploits or **exact revenge on someone who angered them online.** The FBI suggests making a police report about any swatting threats you receive online. Such threats typically come from the online gaming community, where competitors can play and interact anonymously. With a report on file, if a 9-1-1 incident does occur at your home, the police will be aware that it could be a hoax. **The FBI takes swatting very seriously**. Working closely with industry and law enforcement partners, the FBI continues to refine their technological capabilities and investigative techniques to stop the thoughtless individuals who commit these crimes. The bottom line is that swatting puts innocent people at risk.