Public Safety Information on “SWATTING”

What is Swatting?

Swatting is false reporting an emergency to public safety by a person for the intent of getting a (“SWAT team”) response to a location where no emergency exists. The calling party will often report they are involved or nearby as a witness to a home invasion, active shooter, or hostage situation, attempting to muster the largest response possible. Often, the law enforcement response is substantial, with police confronting the unsuspecting victims at gunpoint, only to learn that there is no real emergency.

Those who attempt to cause a swatting incident use several techniques, including: caller ID spoofing, TTY relay technologies, and social engineering. These actors will often have a reasonable scenario and will sometime include personal information. These actors have various reasons; sometimes it is for “fun” and viewed as a prank to the actor, while other times it is used as retaliation against a real or perceived issue with the victim. Several public figures and celebrities have been the victims of swatting.

These calls come from two sources:

- Direct to the PSAP–Calls from spoofed devices with the caller directly providing information to a trained call taker.
- Relayed from a third party–Call from the caller to an untrained person at a relay service such as Telecommunications Relay Service, or even an innocent “Good Samaritan” using social media.

What do you do if you get a call?

Initially these calls cannot be differentiated from real incidents. The PSAP must process these calls as a normal call, following existing standard operating procedures (SOPs). Document all details about the call and caller.

As these are often in-progress calls, if the call taker is able to keep the caller on the line during the response, additional information can be gathered about the incident and caller. Asking specific questions and compare response to previously-supplied information may be useful.

Should the incident be identified as a possible swatting incident, local law enforcement will begin an investigation. PSAP staff should be ready to provide pertinent information on the call, including:

- Call recording (if a voice call)
- Call detail information from the 9-1-1 and telephone systems providers. Note: some system logs are purged after a short period and notifying these providers early may help to preserve evidence. Request info from each provider and work back through the path of call origination. This info may not be provided to the PSAP, but notifying the provider to capture the log information will assist the investigation.
- Gather info from call taker and any notes
- Cooperate in the investigation

What can you do to prepare?

Coordinate with your responding agencies. Understand the SOPs and on scene actions of the responders to the various types of calls, discuss the incidents where a major incident is reported with a single person reporting it. Discuss and determine the roles of each agency in the event of this type of incident.

Coordinate with your investigative agencies. Determine and document jurisdictions and roles and responsibilities of each agency. These can involve multiple agencies (incident site, PSAP, and caller jurisdictions, which may be out of state or even international).

Review PSAP and responder policies and procedures. Look for changes that may be needed to cover this type of incident. Include information on gathering and protecting evidence such as call taker notes and documents. Review roles, responsibilities, and/or SOPs for reporting and investigating swatting incidents.

Update and keep current your 9-1-1 and telephone service provider exigent circumstance contact info. This should include your current providers, but also consider access to the NENA Company Identifier program list. This list includes 24x7 contact numbers for all registered providers.

Update training to include information on Swatting. Include information on what swatting is, additional questioning techniques and how to handle the actions after the call.

Resources

Local Law Enforcement

Local telephone providers
- Exigent circumstance procedures and contacts

NENA Company Identifier Program
- http://www.nena.org/?page=CID2014

Federal Bureau of Investigation (FBI)
- Local FBI Office
- Cyber-Crimes Division
- Swatting info – http://www.fbi.gov/news/stories/2008/february/swatting020408
- InfraGard – https://www.infragard.org/

The Internet Crime Complaint Center (IC3)
- http://www.ic3.gov/default.aspx

U.S. Secret Service Electronic Crimes Task Forces (ECTFs).
- http://www.secretservice.gov/ectf.shtml

Federal Communications Commission (FCC)
- Public Safety and Homeland Security Bureau
- FCC 24/7 Operations Center
- phone: 202-418-1122
- email: FCCOPCenter@fcc.gov

- FCC Report “Caller Identification Information in Successor or Replacement Technologies”
- http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-11-1089A1.pdf

Dispatch Monthly - SWATing 911 Calls
- http://www.911dispatch.com/swating-911-calls/

9-1-1 Magazine – *Telephone Swatting: A New Look at an Old Problem*
- http://www.9-1-1magazine.com/Telephone-Swatting-A-New-Look-at-an-Old-Problem/

A resource provided in partnership with the National 911 Program.

May 2015