Terre Haute Police Department

“Swatting”

Public Service Announcement

What is Swatting?

Swatting is the practice of making hoax or prank calls to emergency services about ongoing critical incidents in order to fool them into visiting an address unnecessarily. The term comes from the use of SWAT (Special Weapons and Tactics) teams who respond to emergencies with specialized equipment such as firearms and door breaching tools.

Why “Swat”?

People use swatting as a tool to cause irritation, inconvenience or fear for their chosen victim. In some circumstances, being swatted can make the victim feel extremely anxious and can affect people’s general wellbeing and mental health.

Swatting can range from isolated incidents, intended to create rumors and/or get the victim into serious trouble, to sustained bouts of swatting attacks, where bomb squads are deployed and schools or businesses are evacuated multiple times. Sometimes, a group of swatters will target a particular individual or business and strategically make calls to the emergency services again and again regarding the same or different false emergencies with the purpose of creating maximum disruption to their target.

How Does “Swatting” Happen?

Most of the time, incidents of swatting will occur after someone has gained access to personal information such as your home address or place of work, using that information to fuel their harassment campaign. See below for some of the ways that a swatter can gain access to your information.

- **Location services** – On most devices and consoles, there is an option to use ‘Location services’ in which you allow the device or console to access your location in order to give you a more personalized experience while using it. Sometimes, when using the location services, your exact location will be visible to other users, making it easier for them to pinpoint your home address.
- **Doxing** – If someone’s information becomes public due to being doxed either by the perpetrator posting the information on different social media platforms or by distributing the information to other people, they are at risk of falling victim to swatting.

- **Sharing information** – It can be easy to share information with others when using the internet. But by sharing your home address with someone you don't know well enough, you are putting yourself and anyone else in your home at risk of being swatted.

What to do if you're "Swatted"

- **Remain calm** – Remember that law enforcement are responding to a serious emergency call. Authorities will respond better to a calm, friendly approach.
- **Cooperate** – Although you may be agitated, it's important that you cooperate with the local law enforcement. If they need to search your house or temporarily handcuff you, follow their instructions. They are on your side and once you explain what you think has happened, they will help you accordingly.
- **Report it** – In most states, swatting is taken very seriously. It is a waste of the emergency responders time and can result in the victim being seriously injured. If you are a victim to swatting, contact local law enforcement immediately.

Examples of "Swatting"

There have been several high-profile examples of how serious swatting attacks can be. These include:

Black Lives Matter Los Angeles

In August 2020, the home of Black Lives Matter activist Melina Abdullah was surrounded by Los Angeles police. The co-founder of Black Lives Matter Los Angeles livestreamed a situation that saw armed officers surround her home. It soon emerged that the incident was a swatting attack in which a caller reported a false hostage situation "to send a message."

Tyler Barriss

One of the most high-profile swatting cases involved Los Angeles resident Tyler Barriss making a false claim against Andrew Finch, in Kansas, in 2017. Barriss made a hoax call to emergency services, reporting Finch for killing a member of his family and holding two others hostage. Police arrived at Finch's house and shot and killed him. Barriss was arrested and given 20 years in prison.

Sergey Vovnendo vs. Krebs

In 2013, Ukrainian hacker Sergey Vovnenko sent heroin to the home address of cybersecurity blogger Brian Krebs via dark web site Silk Road and the U.S. Postal Service (USPS). The hacker attempted to get the blogger arrested for drug possession by sending him the drugs then reporting it when the package arrived at his address.

However, the plot failed and the hacker was later sentenced to 41 months in prison for his role in an unrelated international hacking conspiracy.

Notable “Swatting” Statistics

Putting a figure on swatting cases is difficult because swatting is not classified as a specific category in the crime statistics database of the Federal Bureau of Investigation (FBI). However, a former FBI special agent has revealed that swatting cases more than doubled from 400 in 2011 to over 1,000 in 2019.

How To Prevent “Swatting”

While the act of swatting itself is difficult to stop, there are steps users can take to avoid becoming a victim. This includes using a firewall to ensure web application security and preventing spoofing or Structured Query Language (SQL) injection attacks.

Simple processes and best practices users can take to prevent swatting include:

Privacy Settings

Users can prevent swatters from gaining access to their personal information by enforcing strict privacy and security settings on their devices and social media accounts. They should also take time to regularly check the safety and security settings on their email and social media profiles, especially when they get a new computer or mobile phone.

Switch Up Your Passwords

Regularly changing passwords, in addition to using strong, unique passwords for online accounts, is crucial to avoiding swatting attacks. This ensures that, even if an account gets compromised, the attacker will not be able to use the same password to access other accounts. As a result, it lowers the risk of swatters discovering users’ personal information.

Turn On Two-factor Authentication (2FA)

Using passwords alone is not enough to secure online accounts. Users should add an extra layer of security to their accounts by using 2FA, which requires them to verify their login activity by entering a code that is sent to their personal device.

Avoid Oversharing

Internet users need to avoid oversharing personal information on social media and public websites to prevent the threat of swatting. This prevents information like users’ home and work addresses from getting into the wrong hands. It is also important to be mindful of whether information shared on social media could be used by attackers to understand users’ location or piece together identity attacks.