Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-072325-2-PSA
July 23, 2025

In Real Life (IRL) Com: Violent Subset of The Community (Com) is a Rising Threat to Youth Online

The Federal Bureau of Investigation is warning the public about In Real Life (IRL) Com, one of three subsets of the growing and evolving online threat group known as The Com, short for The Community. The Com is a primarily English speaking, international, online ecosystem comprised of multiple interconnected networks whose members, many of whom are minors, engage in a variety of criminal violations. The members within IRL Com typically have a shared interest, ideology, or goal and work together, adding others to the group and splintering when necessary, to achieve their mission.

IRL Com, which initially stemmed from the subscriber identity module (SIM) swapping[1] community, includes subgroups that provide violence as a service (VaaS) and encompasses a range of violent crime. IRL services include shootings, kidnappings, armed robbery, stabbings, physical assault, and bricking. Services are posted online with a price breakdown for each act of violence. Groups offering VaaS advertise contracts on social media platforms to solicit individuals willing to conduct the act of violence for monetary compensation.

Much of the IRL violence within The Com arose from online conflicts in the SIM swapping community; however, the IRL violence has not only intensified but also expanded to other layers of The Com, emerging as its own market. IRL violence, or the threat of violence, is a tool to harass and intimidate targets. The spread of the VaaS market has led other layers of The Com to adopt similar methods of retaliation.

SWATTING AND IN REAL LIFE COM

IRL Com subgroups offer swat[2]-for-hire services via communication applications and social media platforms. Infighting among Com subgroups often leads to targeted swatting and doxing of members. IRL Com actors who offer these swatting services use platforms and technologies to obscure their true identities and are often paid in cryptocurrency.

---

[1] Subscriber identity module (SIM) swapping is a method in which a cyber criminal performs an unauthorized account takeover of a victim's wireless account held with the mobile phone carrier. This is accomplished by linking the victim's mobile phone number to a different SIM card within the same carrier's network but installed in a device the cyber criminal controls.

[2] Swatting is the act of reporting a false emergency situation with the intention of eliciting a law enforcement or SWAT response.

The goal of swatting differs among The Com subgroups. IRL Com groups use swatting as a way to earn money. The IRL Com groups also see swatting as a way of gaining credibility among members; the more attention a swatting incident gets, the more attention the member receives from the group. Additionally, leaders from IRL Com groups may use swatting to ensure members of the group remain obedient. When members of the IRL Com group disobey orders or refuse to comply with demands, the member or the member's family may become the target of swatting.

VICTIM REPORTING AND ADDITIONAL RESOURCES

If you or someone you know may be a victim of a crime using the tactics outlined above, the following resources may help:

- If it is an immediate, life threatening emergency, dial 9-1-1.
- Consult a health care provider who can provide an initial evaluation or referral to a mental health professional.
- Connect to a mental health resource who can help with health coping skills for intense emotions and help reduce the risk of a serious injury.
- The National Center for Missing and Exploited Children (NCMEC) provides a free service known as **Take It Down**, which helps minor victims, or adults who were victimized as minors, with removing or stopping the online sharing of nude, or sexually explicit content taken while under 18 years old. For more information, visit https://takeitdown.ncmec.org
- Contact your account providers immediately to regain control of your accounts, change passwords, and place alerts on your accounts for suspicious login attempts and/or transactions.
- Retain all of the information regarding the incident (i.e. usernames, email addresses, monikers, websites, platforms used for communication, names, photos, videos, etc.) and immediately report it to:
    - FBI's Internet Crime Complaint Center: www.ic3.gov
    - FBI Field Office: www.fbi.gov/contact-us/field-offices or 1-800-CALL-FBI (225-5324)
    - National Center for Missing and Exploited Children (NCMEC): 1-800-THE-LOST or https://report.cybertip.org/.