CID

ARMY CRIMINAL INVESTIGATION DIVISION

3 September 2024

Cybercrime Prevention Flyer

Cyberstalking

As the result of a joint investigation between the Department of the Army Criminal Investigation Division – Cyber Field Office and the Federal Bureau of Investigation, a cyberstalker, an Army soldier, is now serving 27 months in federal prison.

From late 2017 through most of 2021, the soldier sent anonymous hateful and threatening messages to the victim, a former coworker, and the victim's family. The perpetrator escalated their actions by placing an electronic tracking device on the victim's vehicle and sent photos of the victim to businesses the victim patronized. The threatening messages eventually led to death threats.

Each year, as many as 7.5 million individuals experienced cyberstalking and nearly 6 million victims reported tracking technologies enabled the behavior. Approximately 4.5 million indicated cyberstalking was facilitated through portable electronic devices and of that group, many fell victim to malware or phishing efforts that subsequently resulted in unauthorized account access. Approximately 5 million victims reported personally knowing the perpetrator.

Cyberstalking is a stalking behavior involving persistent harassment through electronic communication services such as email, short message service (SMS) or text messages, social media, and other messaging platforms for electronic surveillance. Maintaining characteristics related to online harassment behavior, cyberstalking subjects victims to substantial emotional distress or reasonable fear of injury or death.

Examples of cyberstalking behavior include:

- Making threatening, deliberate statements in online message boards or forums that upset or inflict harm on the victim or their family (trolling).
- Posing as someone else to fuel and direct harassment toward the victim (inciting).
- Sending offensive, unsolicited images or sexting material (harassment).
- Threatening to reveal or expose private or explicit photos of the victim (revenge porn).
- Revealing or posting personally identifying information of the victim (doxing).
- Installing software that tracks the activities of the victim through an online medium (unauthorized use of a computer).

Recommendations

- Review privacy settings on your social media platforms. Verify the settings and shared information are at your comfort level.
- Review the devices you authorize to gain access to your account(s). Remove any unrecognized devices.
- Use strong passwords that leverage letters, numbers, and special characters.
- Update device, application, and operating systems.
- When possible, leverage multifactor or two-factor authentication on accounts.
- Avoid posting sensitive information to your social media accounts, including phone number, home address, banking information.
- Avoid “checking in” locations on social media.
- Deny friend request(s) from people you do not know personally or do not trust.
- Consider enabling an alerts function for searches of your name when new content appears on the internet.
- If you believe to be subjected to cyberstalking:
    - Do not engage further with the perpetrator.
    - Preserve any material that supports the complaint.
    - Contact your local police department.

Department of the Army Criminal Investigation Division: Report a Crime

FBI Internet Crime Complaint Center (IC3): File a Complaint

National Center for Missing and Exploited Children: CyberTipline (for victims under 18)

The Stalking Prevention, Awareness, & Resource Center (SPARC)

To receive Cyber Field Office Cybercrime Prevention Flyers, send an email to: CYDIntel@army.mil

CPF 0074-2024-CID461

Cyber Field Office
Russell Knox Building
27130 Telegraph Road
Quantico, VA 22134