Report a crime to U.S. Army Criminal Investigation Command

Major Cybercrime Unit

27130 Telegraph Road
Quantico, Virginia 22134

Email

MCU Web Page

CID LOOKOUT
ON POINT FOR THE ARMY

"Do What Has To Be Done"

CPF 00008-2021-CID361-9H **1 April 2021**

Online Misconduct: Awareness and Reporting

Overview

Online misconduct is a term that describes unacceptable or improper behavior through the use of technology. It can include electronic communication that harms someone, typically by sending harassing, intimidating, humiliating, or even threatening messages. Online bullying, harassing email or text messages, embarrassing or degrading pictures posted to social media sites, and vicious attacking comments in chats or website communications are examples of online misconduct.

Be aware that harmful online communications can have legal consequences and that there are mechanisms for reporting online misconduct. While there is no Federal criminal statute called "online bullying," misuse of online communications, sending harassing or intimidating communications and images, or other online misconduct may violate existing Federal laws under the United States Code (U.S. Code or U.S.C.). The misconduct may also constitute violations of articles of the Uniform Code of Military Justice (UCMJ).

Offenses

When you become aware that someone is misusing technology to harm others, consider whether those harmful communications potentially fall under the following types of criminal conduct and applicable statutes:

Electronic Harassment: 47 U.S.C. § 223 makes it a crime to use a "telecommunications device" to knowingly send "any comment, request, suggestion, proposal, image, or other communication which is obscene or child pornography, with intent to annoy, abuse, threaten, or harass another person." Section 223 could apply if the offender initiated telephone calls (including VOIP calls) or texting with the intent to harass the victim.

Electronic Threats: 18 U.S.C. § 875 prohibits transmitting communications containing threats to kidnap or physically injure someone. It also criminalizes the actions of someone who, with intent to extort (receive anything of value), electronically threatens to injure the property or reputation of a person. Sextortion incidents (being tricked into providing sexual images and then being asked for money to not have the images published online) may fall under provisions of this law.

Stalking: 18 U.S.C. § 2261A prohibits a person, with the intent to kill, injure, harass, or intimidate someone, from using a computer (or other digital communications system), to engage in actions (course of conduct) reasonably expected to cause a person (or immediate family member, spouse, or intimate partner) substantial emotional distress.

Cybercrime Prevention Flyer

Child Exploitation / Child Sexual Exploitation: 18 U.S.C. § 2251, 2252, and 2252A, using a computer (a smart phone is a computer) to solicit, make, create, transmit, or receive child pornography is illegal. For these provisions, a child is anyone under the age of 18. 18 U.S.C. § 1462 makes it a crime to transmit obscene matters. 18 U.S.C. § 1470 criminalizes the transfer of obscene materials, to include digital images, to persons under the age of 16. Sending sexually explicit (graphic dirty talk) electronic messages to minors, or soliciting sexually explicit communications, also are criminal offenses.

Computer Misuse (Hacking): A person engaging in online misconduct may also commit violations of 18 U.S.C. § 1030, if, for example, the person exceeds authorized access to the computer or accesses the computer without authorization (i.e., hacks into an account or network) to send the harassing, intimidating, humiliating, or even threatening communication.

UCMJ: Military violations may concern Articles 88, 89, 91, 120b, 120c, 115, and 134 (all of which include the General Article provisions, Contempt, Disrespect, Insubordination, Indecent Language, Communicating Threats, Solicitation to Commit another Offense, and Child Pornography offenses), as well as other Articles.

Every nasty, hurtful, or embarrassing digital communication transmitted across digital communications is not a criminal offense. In fact, many communications, though offensive, may have speech protection under the First Amendment to the U.S. Constitution; however, as shown above, certain online misconduct violates Federal law.

Reporting Mechanisms

If you receive or experience offensive electronic communications – or become aware of others who do – report them. Commanders are responsible for maintaining good order and discipline within their organizations. Use your chain of command for reporting assistance.

Notify CID of online misconduct that involves death threats, child pornography or any sexually explicit communications involving messages or photos of minors, hacking, and stalking incidents. Contact your local CONUS CID office for domestic issues or the appropriate OCONUS CID office for overseas issues. To anonymously report crime, suspicious activity or threats, submit a tip from your computer, tablet or other internet connected device or you can submit a tip from your phone by downloading the CID Crime Tips mobile application. For reporting assistance, download the Crime Tips application brochure. If you require immediate assistance, call 911.

Notify the Military Police at your installation of all other online misconduct you believe is criminal. If you reside off-post and/or the incident is committed by someone not affiliated with the Army, contact your local police.

Additional Resources

For information about computer security and other computer-related scams, we encourage readers to visit the MCU website for the latest crime alert notices and crime prevention flyers.

To receive future MCU Cybercrime Prevention Flyers, send an email to: Subscribe CPF