

0004-15-CID361-9H

17 April 2015

Cyber Misconduct: Awareness and Reporting

Overview:

Cyber 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. Cyberbullying, 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 cyber misconduct.

Be aware that harmful online communications can have legal consequences and that there are mechanisms for reporting cyber misconduct. While there is no Federal criminal statute called "cyberbullying," misuse of online communications, sending harassing or intimidating communications and images, or other cyber 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 \(a\)\(1\)\(C\)](#) makes it a crime to anonymously use a telecommunications device (i.e., telephone, computer, or other electronic device used for communication) to harass a person; [47 U.S.C. § 223 \(a\)\(1\)\(E\)](#) prohibits initiating communications via a telecommunications device solely to harass the recipient.

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.

Cyberstalking – [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.

Obscenity – [47 U.S.C. § 223\(a\)\(1\)\(A\)](#) prohibits using a telecommunications device to make, create, or solicit, and transmit any obscene comment, request, suggestion, proposal, image, or other communication.



Contact Information:

Cyber Criminal Intelligence Program
27130 Telegraph Road
Quantico, Virginia 22134

Phone: 571.305.4482 IDSN 2401

Fax: 571.305.4189 IDSN 2401

E-mail:

usarmy.cciuintel@mail.mil

CCIU Web Page:

www.cid.army.mil/cciu.html



DISTRIBUTION:

This document is authorized for wide release with no restrictions.



Offenses (continued):

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 cyber misconduct may also commit violations of [18 U.S.C. § 1030](#), if, for example, he 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, and 134](#) (to include the General Article provisions, Contempt, Disrespect, Insubordination, Indecent Language, Communicating a Threat, 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 cyber 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. Utilize your chain of command for reporting assistance.

Notify CID of cyber 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 CID office (see www.cid.army.mil/unitsconus.html for domestic locations and www.cid.army.mil/unitsforeign.html for overseas), email Army.CID.Crime.Tips@mail.mil or call 1-844-ARMY-CID (844-276-9243). If you require immediate assistance, call 911.

Notify the Military Police at your installation of all other cyber 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 CCIU [website](#) for the latest crime alert notices and crime prevention flyers.



CCIU uses the Interactive Customer Evaluation (ICE) system. Please click on the ICE logo and take a moment to provide us with feedback.

Disclaimer: The appearance of hyperlinks in this Crime Awareness Flyer, along with the views and opinions of authors, products or services contained therein does not constitute endorsement by CID. These sites are used solely for authorized activities and information that support the organization's mission. CID does not exercise any editorial control over the information you may find at these link locations. Such links are provided consistent with the stated purpose of this flyer.