Cybercrime Prevention Flyer

CPF 0016-2020-CID361-9H **20 October 2020**

Protecting Children Online

The coronavirus pandemic increased the use of the internet among children through computers, smartphones, gaming systems, and other devices. Although many children are back to in-person learning, there are more kids online than ever before. The internet influences how children discover and interact with the world around them. Children go online to learn, play, and communicate.

Unfortunately, the internet is not always a safe place for children. Many criminals use the anonymity offered by the internet to prey on vulnerable children and teenagers. Masking their real identities and leveraging the curiosity of children when seeking victims, cyber predators and criminals use a variety of tactics and platforms to prey on unsuspecting children.

Understand the Risks:

Inappropriate Content

Children may encounter inappropriate content online that encourages unlawful or dangerous behavior. Inappropriate content can also leave children confused and unable to process what they have seen. Inappropriate content is different for every age and maturity level, but may include websites, posts, or pictures containing pornography, excessive violence, or hate speech. Many platforms provide a minimum age of use that can be used as a guideline to protect children from inappropriate content for their age.

Online Privacy

Online privacy protects children's online information such as name, address, passwords, phone numbers, and other personal information or PII. Personal information should not be shared online. Cybercriminals use the internet to collect information and may target children as children may willingly post or provide personal information. Cybercriminals use children's personal information to commit identity fraud and open credit cards, auto loans, utility services, or other accounts. Geographic locations and street address information should also be protected online as it can lead to criminals targeting your residence or unwanted contact from strangers. Geolocation tags on social media posts or photos give the exact location making it easier for criminals to locate the individual or residence.

Cyber Predators

Cyber predators are individuals who use the internet to connect with minors in order to take advantage of them sexually, emotionally, psychologically, or financially. Cyber predators manipulate children by developing trust and a friendship. Teens are more at risk to cyber predators than younger children as they may willingly talk to a predator online even though they know it is dangerous. Some teens turn to online dating or social groups, which can also make them more inclined to meet up with a predator in person.

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

Major Cybercrime Unit
U.S. Army Criminal Investigation Command

Cybercrime Prevention Flyer

Cyberbullying
Cyberbullying refers to harassment through the use of digital devices. Cyberbullying can cause emotional or physical distress in children. Cyberbullying can be done by spreading lies, posting embarrassing photos, and sending hurtful messages or threats. Cyberbullying most often occurs through social media, messaging platforms, gaming platforms, and cellphones. Preteens and teens are more likely to become victims of cyberbullying than younger children. Cyberbullying can cause depression, decreased self-worth, hopelessness, and loneliness. Preteen and teen victims of cyberbullying are at higher risk of self-harm and suicidal behaviors.

Online Scams
A variety of scams are carried out online. The most common online scam targeting children are free game advertisements and prize entries that ask for money or personal information. Other online scams targeting children include ads and auctions that offer items at cheap prices, but the items never arrive after sending a payment.

Phishing
Phishing is the use of emails or ads to trick children into clicking malicious links or attachments. Phishing emails and ads are often used to steal personal information by asking for verification of address or other personal information from seemingly reputable sites.

Accidental Malware Downloads
Malware refers to malicious software that disrupts, damages, or gains unauthorized access to a system. Malware can infect computers or other devices and is most often used to steal private information. Malware can also be used to steal credentials or give a cybercriminal access to the device. Kids are more likely to accidentally initiate malware when downloading games or other applications.

Children May Encounter Solicitations Through:
- Social media
- Email
- Texting
- Built-in chats on computer or video games
- Online forums, chat rooms, or message boards
- Software downloads
- Ads

Protect Your Children Online
Parental involvement is critical to help children use the internet safely.

- Talk to your children about their online activities.
- Get familiar with the technology platforms your child likes to use.
- Keep consoles and other devices in an easy to supervise location and be aware of other places where your child may be accessing the internet.
- Ensure children are using privacy controls when setting up accounts.
- Encourage your children to choose appropriate screen names.
- Set rules about what your children can share online.
- Talk to your children about giving out information online and to never give out personal information including passwords, home address, location, phone number, or email address.
- Teach children to ignore messages from strangers and to ask them who they are in contact with online.
- Teach children to never meet in person with someone they met online.
- Install antivirus on computers and mobile devices.
- Keep all software up to date.

- Ensure games and other applications are downloaded from official vendor application stores.
- Consider downloading parental control applications to block inappropriate content, monitor social networks, and monitor calls.

Signs Your Child May Be at Risk Online:

- Spending more time online, especially at night.
- Turning the computer monitor off quickly or changing the screen when you come into the room.
- Becoming overly upset when they are is not allowed on their devices.
- Receiving calls or text from callers you do not recognize.
- Taking extra steps to conceal what they are doing online.
- Receiving mail, gifts, or packages from people you do not know.

If you suspect your child has been victimized, contact your local law enforcement agency, the National Center for Missing and Exploited Children, the Internet Crime Complaint Center, or the Federal Trade Commission.

Resources

Protecting Kids Online – Federal Trade Commission
Parent's Guide to Internet Safety – Federal Bureau of Investigation (FBI)
Safety Pledge: Keep Kids Safer Online – National Center for Missing and Exploited Children
NetSmartz Digital Safety Lessons for Children – National Center for Missing and Exploited Children

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