ALBUQUERQUE

President's Message

Dear Alumni:

Just wanted to check in with all of you to be sure that you are adjusting to our new normal, being mindful of social distancing, wash your hands frequently and for 20 seconds, finding new ways to connect with friends and families and most of all, being kind to one another.

If any member of the alumni association needs anything, please reach out to me.
Tim

April 1, 2020
Alert Number I-040120-PSA

Questions regarding this PSA should be directed to your local FBI Field Office.

Local Field Office Locations: www.fbi.gov/contact-us/fieldCyber

Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments

The FBI anticipates cyber actors will exploit increased use of virtual environments by government agencies, the private sector, private organizations, and individuals as a result of the COVID-19 pandemic. Computer systems and virtual environments provide essential communication services for telework and education, in addition to conducting regular business. Cyber actors exploit vulnerabilities in these systems to steal sensitive information, target individuals andbusinesses performing financial transactions, and engage in extortion.

As of March 30, 2020, the FBI's Internet Crime Complaint Center (IC3) has received and reviewed more than 1,200 complaints related to COVID-19 scams. In recent weeks, cyber actors have engaged in phishing campaigns against first responders, launched DDoS attacks against government agencies, deployed ransomware at medical facilities, and created fake COVID-19 websites that quietly download malware to victim devices. Based on recent trends, the FBI assesses these same groups will target businesses and individuals working from home via telework software vulnerabilities, education technology platforms, and new Business Email Compromise schemes.

Telework Vulnerabilities

The FBI advises you to carefully consider the applications you or your organization uses for telework applications, including video conferencing software and voice over

Internet Protocol (VOIP) conference call systems. Telework software comprises a variety of tools that enable users to remotely access organizational applications, resources, and shared files. The COVID-19 pandemic has led to a spike in businesses teleworking to communicate andshare information over the internet. With this knowledge, malicious cyber actors are looking for ways to exploit telework software vulnerabilities in order to obtain sensitive information, eavesdrop on conference calls or virtual meetings, or conduct other malicious activities. While telework software provid

es individuals, businesses, and academic institutions with a mechanism to work remotely, users should consider the risks associated with them and apply cyber best practices to protect critical information, safeguard user privacy, and prevent eavesdropping. Cyber actors may use any of the below means to exploit telework applications.

School Closings Due to COVID-19 Present Potential for Increased Risk of Child Exploitation

With our children home for the remainder of the school year and attending classes via the internet there is an increased risk of them being exploited. Please read the article below from the National FBI Citizens Academy and watch over our precious future.

The FBI is warning families and educators that due to school closings as a result of COVID-19, children will potentially have an increased online presence or be in a position that puts them at an inadvertent risk. Because of this, the FBI is seeking to help parents, teachers, caregivers, and children understand the dangers of online sexual exploitation and recognize signs of child abuse.

Please share this information with your Chapter's members, community partners, and local media. Questions regarding this release should be directed to your local FBI Field Office.

BACKGROUND

Online sexual exploitation comes in many forms. Individuals may coerce victims into providing sexually explicit images or videos of themselves, often in compliance with offenders' threats to post the images publicly or send the images to victims' friends and family.

Other offenders may make casual contact with children online, gain their trust, and introduce sexual conversation that increases in egregiousness over time. Ultimately this activity may result in maintaining an online relationship that includes sexual conversation and the exchange of illicit images, to eventually physically meeting the child in-person.

In order for the victimization to stop, children typically have to come forward to someone they trust-typically a parent, teacher, caregiver, or law enforcement. The embarrassment of being enticed and/or coerced to engage in unwanted behavior is what often prevents children from coming forward. Offenders may have hundreds of victims around the world, so coming forward to help law enforcement identify offenders may prevent countless other incidents of sexual exploitation.

Abuse can occur offline through direct contact with another individual. During these uncertain conditions, where time with other adults and caregivers has increased immensely, parents/guardians should communicate with their children about appropriate contact with adults and watch for any changes in behavior, including an increase in nightmares, withdrawn behavior, angry outbursts, anxiety, depression, not wanting to be left alone with an individual, and sexual knowledge.

RECOMMENDATIONS

Parents and guardians can take the following measures to help educate and prevent children from becoming victims of child predators and sexual exploitation during this time of national emergency:

Online Child Exploitation

- Discuss Internet safety with children of all ages when they engage in online activity.
- Review and approve games and apps before they are downloaded.
- Make sure privacy settings are set to the strictest level possible for online gaming systems and electronic devices.
- Monitor your children's use of the Internet; keep electronic devices in an open, common room of the house.
- Check your children's profiles and what they post online.
- Explain to your children that images posted online will be permanently on the Internet.
- Make sure children know that anyone who asks a child to engage in sexually explicit activity online should be reported to a parent, guardian, or other trusted adult and law enforcement.
- Remember that victims should not be afraid to tell law enforcement if they are being sexually exploited. It is not a crime for a child to send sexually explicit images to someone if they are compelled or coerced to do so.

Child Abuse Awareness

- Teach your children about body safety and boundaries.
- Encourage your children to have open communication with you.
- Be mindful of who is watching your child for childcare/babysitting, playdates and overnight visits.
- If your child discloses abuse, immediately contact local law enforcement for assistance.
- Children experiencing hands-on abuse may exhibit withdrawn behavior, angry outbursts, anxiety, depression, not wanting to be left alone with a specific individual, non-age appropriate sexual knowledge, and an increase in nightmares.

VICTIM REPORTING

Reporting suspected sexual exploitation can help minimize or stop further victimization, as well as lead to the identification and rescue of other possible victims. If you believe you are-or someone you know is-the victim of child sexual exploitation:

- Contact your local law enforcement agency.
- Contact your local FBI field office or submit a tip online at tips.fbi.gov.
- File a report with the National Center for Missing & Exploited Children (NCMEC) at 1-800-843-5678 or online at www.cybertipline.org.

When reporting, be as descriptive as possible in the complaint form by providing as much of the following as possible:

- Name and/or user name of the subject.
- Email addresses and phone numbers used by the subject.
- Websites used by the subject.
- Description of all interaction with the subject.
- Try to keep all original documentation, emails, text messages, and logs of communication with the subject. Do not delete anything before law enforcement is able to review it.
- Tell law enforcement everything about the online encounters-we understand it may be embarrassing for the parent or child, but providing all relevant information is necessary to find the offender, stop the abuse, and bring him/her to justice.

OTHER RESOURCES

- More information about the FBI's guidance on sexual exploitation and protecting your kids.
- FBI urges vigilance during COVID-10 pandemic.
- Updated information on the coronavirus from the CDC.

Mark your calendars for the following:

March 18, 2020	2020 Citizens Academy Begins-POSTPONED
March 26, 2020	Mandalay Bay Presentation-POSTPONED
April 10, 2020	Breakfast with SAC Langenberg-POSTPONED
June 15-18, 2020	Washington, DC and Quantico Trip
August 19-21, 2020	National Conference, Milwaukee, Wisconsin
August 27, 2020	Pulse Nightclub Presentation

Membership Reminder:

Those of you that have already renewed your 2020 Gold Shield Membership, a sincere thank you for your continued service and support with the FBIACAAA!

If you have not renewed or maybe even never been a member, we request you please consider renewing or becoming an FBIACAAA Gold Shield Member! In addition to supporting the mission and objectives of the FBIACAAA! To pay your dues online, follow this link. If you prefer to send a check, please send it to: PO Box 92142, Albuquerque, NM 87199.

We have a wonderful event schedule planned for 2020, and events exclusive for Gold Shield Members only. Gold Shield Member events include:

- The opportunity to join SAC James Langenberg at a bi-annual informal breakfast to discuss current areas of interest and ask questions.
- Participate in a private tour of FBI Headquarters in Washington, DC as well as the FBI Academy in Quantico, VA.
- Additional special guest speakers throughout the year.
- You will be sent special invites at the discretion of the SAC throughout the year as opportunities arise.

We hope you will consider joining us as Gold Shield Member for $50 and supporting FBIACAAA in 2020!
See what's happening on our social sites.

Mission

The Albuquerque Citizens Academy Alumni Association is a community-based and supported organization, distinct and separate from the FBI. The association is expected to project a positive image of the FBI in the communities, identify crime problems affecting specific communities, and establish the exchange of information between the FBI and the community.