School Safety Newsletter

Volume 7, Issue 6 January 2020

## FY2019 STOP School Violence Grant Program

Open December 31, 2019 and Closes March 3, 2020

Description: The FY 2019 Student, Teachers, and Officers Preventing (STOP) School Violence Grant Program is designed to improve school security by providing students and teachers with the tools they need to recognize, respond quickly to, and help prevent acts of violence. The program's objective is to increase school safety by implementing training and school threat assessments and/or intervention teams to identify school violence risks among students; technological solutions such as anonymous reporting technology that can be implemented as a mobile phone-based app, a hotline, or a website in the applicant's geographic area to enable students, teachers, faculty, and community members to anonymously identify threats of school violence; or other school safety strategies that assist in preventing violence.

For more information and to apply, visit: https://bja.ojp.gov/funding/opportunities/bja-2020-17313

## DuPage Regional Office of Education Awarded Bureau of Justice Assistance Grant

DuPage Regional Office of Education was awarded a three-year $400,000 Student Teachers Officers Preventing (STOP) grant by the Bureau of Justice Assistance to initiate a countywide mental health training program in 2018.

To see the article, visit: https://www.dupageroe.org/news/dupage-regional-office-education-awarded-bureau-justice-assistance-grant

## Department of Justice, Community Oriented Policing Services Grant

Currently Open and Closes March 11, 2020

https://cops.usdoj.gov/grants

The DOJ provides funding directly to law enforcement agencies to hire and/or rehire career law enforcement officers in an effort to increase their community policing capacity and crime prevention efforts. In FY 2020, agencies may request the number of officer positions necessary to support their proposed community policing strategy. Please keep in mind that there is a minimum 25 percent local cash match and a 12-month retention requirement for each officer position funded. The COPS Office will fund as many positions as possible for successful applicants; however, the number of officer positions requested by an agency may be reduced based on the availability of funding and other programmatic considerations. (1) Hire new officers, which includes filling existing officer vacancies that are no longer funded in your agency's budget. (2) Rehire officers who have already been laid off from any jurisdiction as a result of state, local, or Bureau of Indian Affairs (BIA) budget reductions. The rehired officers must be rehired on or after the official grant award start date as it appears on your agency's award document. Documentation must be maintained showing the dates that the positions were laid off and rehired. (3) Rehire officers who are (at the time of application) currently scheduled to be laid off by your jurisdiction on a specific future date as a result of state, local, or BIA budget reductions. Grantees will be required to continue funding the positions with local funding until the dates of the scheduled lay-offs. The dates of the scheduled lay-offs and the number of positions affected must be identified in the CHP application.

CHP grants can be used to hire and or rehire School Resource Officers. Please note that the COPS Office

*Protecting our future through information sharing*

### In This Issue

## Department of Justice, Community Oriented Policing Services Grant (Continued)

requires that the officer(s) deployed into the SRO position(s) spend a minimum of 75 percent of their time in and around primary and/or secondary schools, working on youth-related activities. The time commitment of the funded officers must be above and beyond the amount of time that the agency devoted to the schools before receiving the grant. There must be an increase in the level of community policing activities performed in and around primary or secondary schools in the agency's jurisdiction as a result of the grant.

## United States Bans TikTok on Military Devices, Signaling Growing Concern About App's Chinese Roots

December 31, 2019, Drew Harwell and Tony Romm

https://www.washingtonpost.com/technology/2019/12/31/us-army-bans-tiktok-military-devices-signaling-growing-concern-about-apps-chinese-roots/

The U.S. Army has banned the use of the popular video app TikTok on government-issued phones, following guidance from the Pentagon and highlighting growing tensions over the app's Beijing-based parent firm. Army spokeswoman Lt. Col. Robin Ochoa told Military.com in an interview released this week that the app was "considered a cyber threat" and not allowed on government-issued devices. Army spokeswoman Lt. Col. Crystal X. Boring told The Washington Post on Tuesday that the service branch was adhering to directions from the Defense Department, which flagged the app for "potential security risks."

The measure follows a similar ban from the U.S. Navy and a "cyber awareness" message earlier in December from the Defense Department that urged the Pentagon's roughly 23,000 employees to uninstall the app because it could potentially expose personal data to "unwanted actors." A Pentagon spokesperson, who requested anonymity because they were not allowed to speak publicly about the issue, said the threat is related to potential loss of personally identifiable information but would not provide further detail. TikTok did not immediately respond to a request for comment.

The Army's ban and the rare notice from the Pentagon, which does not generally issue policy measures on individual social media services, reflects deeply rooted doubts throughout Washington about TikTok and its Chinese parent, ByteDance. Some of their suspicions stem from criticisms raised by TikTok's former employees, who told The Post earlier this year that the company in the past restricted videos in alignment with Chinese rules on acceptable speech.

In response, TikTok has sought to rebut lingering privacy, security and censorship concerns. It says it stores U.S. users' data in Virginia with a backup in Singapore, for example, and doesn't apply Beijing's strict content guidelines in the United States. But those assurances have hardly satisfied lawmakers, some of whom had planned to grill the app's leader, Alex Zhu, on a trip he planned to make to Washington in December but ultimately canceled, citing scheduling conflicts.

In October, Senate Minority Leader Charles E. Schumer (D-N.Y.) and Sen. Tom Cotton (R-Ark.) asked U.S. intelligence officials to investigate the app for national security concerns, fearing that Chinese spies could gain access to American users' personal data. Sen. Marco Rubio (R-Fla.), meanwhile, requested his own national security probe, which threatens to unwind the merger that made TikTok possible in the first place. And Sen. Josh Hawley held a hearing this year with an eye on TikTok and its content moderation rules, responding to concerns that it limits what U.S. users see in line with Beijing's demands. The company declined to testify at the session, drawing a sharp rebuke from the Missouri Republican. Military-related hashtags tend to be popular on TikTok: Videos mentioning #army have 10.6 billion views, for example, and those tagged as #military have more than 826 million views. Anyone can append those or other labels to the content they upload, but pages for each of those hashtags do include scores of clips of people dressed in military fatigues or referencing their time in the service.

The Defense Department has recommended that service members "be wary" of the apps they download and to research the developers' ownership for "any suspicious foreign connections." Uninstalling TikTok "will not prevent already potentially compromised information from propagating, but it could keep additional information from being collected," the agency told military officials, according to a statement from a Defense Department spokesman. In a transparency report released this week, the company said it responded to 298 legal or emergency requests for information on users from 28 countries in the first half of the year, including 107 from India and 79 from the United States. TikTok also said it received 28 requests from government bodies in nine countries to remove content deemed a violation of local laws, and removed or restricted 25 accounts in response. TikTok said it "did not receive any government requests to remove or restrict content" or any "legal requests for account information" from China.

## Monthly Webinars!

First Wednesday of Every Month

at 10 am

(Except January, July, and August).

## Next Webinars

**Wednesday, February 5, 2019**

Each webinar has a round table discussion at the end. Questions are always welcome!

To participate, you must be a vetted member. For more information please email

isp.schoolsafety@illinois.gov

# TikTok Sued For Collecting Kids' Data Without Consent

January 6, 2020, Farron Cousins

https://trofire.com/2020/01/06/tiktok-sued-for-collecting-kids-data-without-consent/

A TikTok class action filed in Illinois federal court claims that the popular video app collects data from children under the age of 13 without consent. Plaintiffs Sherri LeShore of Illinois and Laura Lopez of California recently filed the TikTok class action on behalf of their children, claiming that the video social media app violates state laws by gathering data from young users. TikTok started in 2014 under the name Musical.ly. Since then, the app has allegedly failed to protect children. Ring of Fire's Farron Cousins discusses this with Scott Hardy, President of Top Class Actions. The following is a transcript. *This transcript was generated by a third-party transcription software company, so please excuse any typos.

Farron Cousins: The TikTok app has been around in some form or fashion for at least the last five years, but in recent months has once again surged in popularity. And unfortunately as we've seen all too often with these apps, especially those geared towards younger children, it appears that they are taking user's data and not protecting that data, without consent. Joining me now to explain what's happening is Scott Hardy with Top Class Actions. And Scott, again, we've seen this huge resurgence in the last a month or so of TikTok. People love posting these things on other social media networks and kind of like all the other app stories we've had to talk about, they're not protecting consumer data and they may even be selling the data of children. Lay this one out for us.

Scott Hardy: Right. So it's illegal for children under the age of 13 to give their consent to have their likenesses and their pictures broadcast on the internet. That is a huge privacy no-no. But of course you have kids that love to lip-sync to these videos, use all the filters and post these on TikTok and share them with your friends. But the problem is if the kids under 13 even if they say it's make it a private account, TikTok was still allowing these things to be searched and viewed. And, you know, I actually had an issue with one of my daughters who unbeknownst to me had a TikTok account and was posting all of these videos and, you know, having these, it was a private account, but she was still getting likes from people that weren't her friends. And, you know, now all of that has been wiped out. But it really shows a larger issue that TikTok has of underage kids using this app and can get, getting possibly harassed and stalked by people around the world.

Farron Cousins: And that's, you know, it opens the children up, as this lawsuit claims, to predators. You know, if your child has an account here, which, which they can have. But if they've said, I want to be private, I only want, you know, my close friends that I accept into my circle here, only they can look at my things. I am doing this for them. But by not protecting this, by failing to live up to their own standards that TikTok had set for this app, they allow these predators to come in and send messages to, to, to underage people. And that just opens up a whole new can of, you know, terrifying worms here in addition to another lawsuit says they're selling the data. And it's bad enough that we as adults, we understand that look, if I'm going to get on my Amazon app and I'm going to buy something, there goes my data, it's gone. I log into Facebook, my data's gone. They know where I'm at. They've got all my stuff, it sucks and it's horrible, but we've almost become addicted to these apps. These kids on the other hand, they didn't give consent. They don't understand what's happening when they do this. Yet, just like us, their data's being sold as well.

Scott Hardy: It is, I mean, and then we have a second TikTok class action that's not included in the settlement that for a plaintiff over the age of 18 who, who alleges that TikTok accumulates data and transfers that information to servers in China. And that information can be used to identify and track the location of users within the United States among other things. So there are a lot of privacy concerns that have been brought over the TikTok app and how it's based in China and what exactly they're doing with that data.

Farron Cousins: We have to be very careful not just as consumers but especially as parents. You know, as you said, you, you discovered that, that one of your children had this app on there and you didn't even know about it. And while at the same time we've got to respect their privacy. We don't want to be like these corporations and, and swoop in and take their data away from them either. But we've also gotta be a little more vigilant about this. And, and unfortunately it means we probably also have to start having talks with them about data privacy and things like that. Things that kids probably can't even understand. But that's the, that's the position that corporations have put us in. Now, we shouldn't be in this position. Those are things we shouldn't have to do. But unfortunately we do almost like when schools have to go through active shooter drills. It's not something they should have to do. But unfortunately it's something we have to do because of the way the world is now. And so it puts more on us. That's unfair. We shouldn't have to snoop on our kids' phones. We hadn't, shouldn't have to see what kind of apps they're using. We shouldn't have to have a talk about data privacy with them. But it kind of looks like that's, that's what we have to start doing to protect them from these corporations.

Scott Hardy: We are and we had the conversation just last night with our daughter saying, don't take any pictures on your phone that are at all inappropriate. You know, all of these things, don't send pictures to your friends. All of these things will live on the internet forever. And, you know, with these lack of privacy and these privacy breaches, it's just so unsafe for kids right now. It's really scary and now we have to lock down all of their devices and all their access to these devices to make sure that they are, you know, aren't doing anything that they're not even aware could harm them.

Farron Cousins: Yeah. We have to basically become the police officers in our own home because of the negligence of these corporations. For more information about this issue, please follow the, in the description of this video, head on over to topclassactions.com and while you're there, make sure you sign up for their weekly newsletter. Scott Hardy, Top Class Actions, always a pleasure talking to you. Thank you.

# Recent School Ransomware Attacks Highlight Need for Ongoing Vigilance

January 3, 2020, Naaz Modan

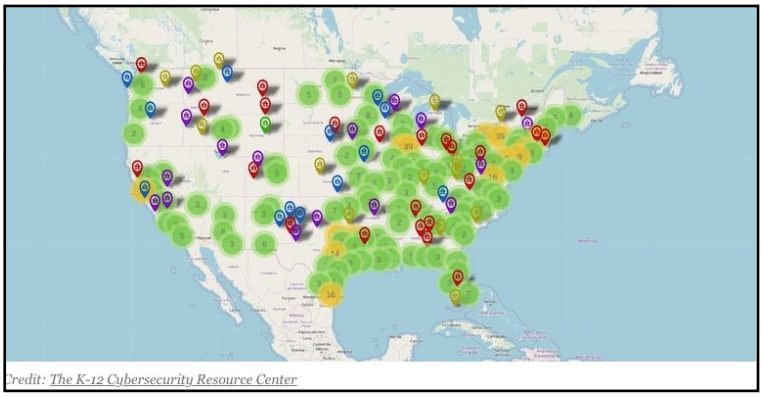
https://www.educationdive.com/news/recent-school-ransomware-attacks-highlight-need-for-ongoing-vigilance/569710/

In a routine cleanup over the holiday break, the IT department in Michigan's Richmond Community Schools "noticed something unusual" with the district's computers. It was a ransomware attack — something districts are becoming all too familiar with.

"Immediately, they shut down the portal where [the virus] had entered the system, shut down other servers that we believe have not yet been infected, and disconnected the internet," Superintendent Brian Walmsley said. "We tried to preserve what was still good and spent the weekend trying to figure out how big the problem was."

While the district confirmed no student or staff information was breached, the ransomware virus impacted several district servers and "affected critical operating systems" including heating, telephones and classroom technology.

The attack mostly infected teachers' saved files, such as curriculum plans and textbook chapters, Walmsley said, and its source demanded $10,000, which the district refused to pay.


Credit: The K-12 Cybersecurity Resource Center

Thanks to a daily backup housed in a separate building that was "disconnected immediately" after discovery of the attack, the district restored phones, operating systems in the classrooms and the internet. Restoring teachers' files "will come at a later date," Walmsley said, noting the district is "trying to make sure that we don't reinfect the systems."

Schools are expected to reopen Monday after an extended closure following the break.

How to protect against cyberattacks

While the district in this incident ensures no student or staff data — stored in a separate county-level building — has been compromised, K-12 cybersecurity expert Doug Levin said in most cases "it can be very difficult to know whether or not there has been a data breach."

According to Levin, Richmond Community Schools' attack is one of 746 publicly disclosed incidents targeting schools since 2016, a number that has climbed significantly from 408 around this time last year and has affected both large urban districts and smaller rural schools. Washington's Issaquah School District 411 also reported a malware attack this week.

As more schools incorporate technology in the classroom, and depend on it for everyday functions like payroll and heating and cooling, potential vulnerability for attacks increases.

"School leaders need to weigh the potential benefits of technology with the potential risks that they introduce, among those are cybersecurity risks," Levin said. "And they need to have a plan in place to manage these risks."

This could include keeping a cybersecurity insurance policy or regularly auditing.

Walmsley said in his district's case, it could've been as simple as regularly changing and strengthening passwords, something Levin agrees can mitigate risk.

Routinely backing up systems and keeping them offline, or "immutable" — meaning the backup cannot be altered by a virus — could also save districts time and money in case of a cyberattack. "If you don't have these backups, you're talking about rebuilding these systems from scratch or negotiating with the actors," Levin explained, pointing to a case last year in Riviera Beach, Florida, where the city paid hackers $600,000 to regain access to their systems.

Schools should also evaluate their tech inventory to determine whether they need as many internet-facing servers and systems — not doing so means a school could increase the odds of exposing data.

Regularly keeping up with security updates and patches from software vendors takes time and energy, but is another straightforward process that can go a long way to secure systems.

While there's no one way to mitigate risk entirely, "School districts that have plans in place may discover them quicker, may recover quicker, and they communicate about them better to the school community," Levin said. "It helps them maintain trust."

## Texas School District Loses $2.3 Million from Phishing Scam

January 11, 2020, Alexis Page

https://www.ksat.com/news/texas/2020/01/11/texas-school-district-loses-23-million-from-phishing-scan/

Manor Independent School District, just east of Austin, is out of $2.3 million from a phishing scam.

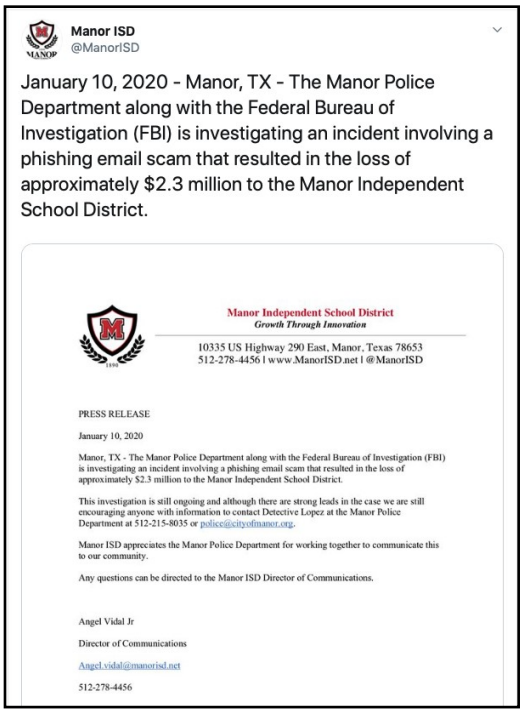
Investigators say the phishing email was sent to multiple people at the school district and it was a single person that responded.

The money was sent through three separate transactions.

Investigators said whoever paid didn't realize the bank account information was changed and it was being sent to a fake bank.

School officials say they have a "strong lead" in the case but no arrests have been made.

The district and the FBI are still investigating the scam.



Manor ISD
@ManorISD

January 10, 2020 - Manor, TX - The Manor Police Department along with the Federal Bureau of Investigation (FBI) is investigating an incident involving a phishing email scam that resulted in the loss of approximately $2.3 million to the Manor Independent School District.

**Manor Independent School District**
*Growth Through Innovation*

10335 US Highway 290 East, Manor, Texas 78653
512-278-4456 | www.ManorISD.net | @ManorISD

PRESS RELEASE

January 10, 2020

Manor, TX - The Manor Police Department along with the Federal Bureau of Investigation (FBI) is investigating an incident involving a phishing email scam that resulted in the loss of approximately $2.3 million to the Manor Independent School District.

This investigation is still ongoing and although there are strong leads in the case we are still encouraging anyone with information to contact Detective Lopez at the Manor Police Department at 512-215-8035 or police@cityofmanor.org.

Manor ISD appreciates the Manor Police Department for working together to communicate this to our community.

Any questions can be directed to the Manor ISD Director of Communications.

Angel Vidal Jr

Director of Communications

Angel.vidal@manorisd.net

512-278-4456

## An 11-year-old in Mexico Told Some of His Classmates 'Today is the day.' Then He Opened Fire

January 10, 2020, CNN

https://www.cnn.com/2020/01/10/americas/mexico-coahuila-school-shooting/index.html

A teacher was killed and six other people injured when an 11-year-old student opened fire January 10, 2020, at a private school in the northern Mexican state of Coahuila, officials said.

The shooter, a sixth-grader armed with two guns, also died, said Adelaido Flores, the regional coordinator for public safety in Coahuila, near the Texas border.

Coahuila Gov. Miguel Angel Riquelme told reporters that classmates said the boy was generally well behaved but voiced a strange warning before his rampage on Friday. "He told some classmates, 'Today is the day,' " Riquelme said.

Shortly after 8 a.m., the student asked to use the restroom. After about 15 minutes, the teacher went to look for him and found him leaving the restroom with weapons in hand, the governor said.

Riquelme said authorities believe the boy was influenced by the video game Natural Selection, a first-person shooting game. He said the boy was wearing a undershirt emblazoned with the game's name. "He had mentioned the video game, which I believe he tried to recreate today," the governor said.

The website for Natural Selection 2 bills it as "an immersive, multiplayer shooter that pits aliens against humans in a strategic and action-packed struggle for survival." Unknown Worlds Entertainment, which manufactures the game, did not immediately respond to an email seeking comment.

Anxious relatives arrived at the school to pick up students after the incident, news footage from affiliate TV Azteca showed. The shooting occurred at the Cervantes de Torreón School in the industrial city of Torreón, the city's mayor, Jorge Zermeño Infante, told reporters.

Preliminary reports were that the student entered the school and fired at a teacher before apparently shooting himself, the mayor said. Four of the wounded were taken to a nearby hospital, he said. Their condition was unknown. The school, in a Facebook post, said a teacher and a student died in the shooting. Additionally, five students and a teacher were wounded, the post said.

"We never would have imagined that a situation like this could occur in our society," the post said, adding that school officials were cooperating with the authorities.

The private school serves students from kindergarten through high school, according to its website. Enrollment was more than 1,900 students in 2016, the site states.

## How to Talk to Your Kids About Weed, Now That It's Legal in Illinois

December 31, 2019, Nara Schoenberg

https://www.chicagotribune.com/lifestyles/ct-life-legal-weed-parenting-12302109-20191231-qfdzaxuopfcu3lq6poz6qg6mbe-story.html

"Legal does not equal safe," said Jim Scarpace, executive director of the Gateway Foundation drug treatment programs in Aurora and Joliet. Alcohol, he pointed out, has been legal since the 1930s, but there are still medical risks and psychological consequences.

In the case of weed, 10% to 20% of those who try it will develop a substance use disorder, Scarpace said. Excessive use in adolescents has been linked to problems with learning, memory and mental health, Scarpace said. And experts are particularly concerned about the effects on young people, whose brains won't fully develop until their mid-20s.

With legalization of limited amounts of marijuana for recreational use, Scarpace cautioned parents against using outdated scare tactics, which are now believed to backfire, triggering a "This isn't going to happen to me" response — and actually increasing interest in drug use. Instead, he urged parents to arm themselves with the facts, among them, that if you're under 21, recreational marijuana use is still illegal in Illinois.

Among the other key points you can discuss with your kids:

**The risk of addiction is real.** Approximately 1 in 10 marijuana users will become addicted, according to the U.S. Substance Abuse and Mental Health Services Administration (SAMHSA) website. For those who start using marijuana before age 18, the rate is higher: About 1 in 6 will experience addiction.

**Your IQ may be affected.** Results are mixed, but one study found that heavy marijuana use starting at a young age can cause an IQ loss of as much as 8 points.

**Marijuana has been linked to mental illness.** It's unclear whether weed actually causes mental illness, or if people with mental health issues are prone to self-medicate with weed. Still, the link in a recent study in Lancet Psychiatry was striking. The chance of developing psychosis — a very serious condition in which a person loses touch with reality — was nearly five times greater for those who used high-potency weed daily, as opposed to those who never used.

## United States Army Warns of Fake Text Messages About Military Draft

January 8, 2020, Stephanie Susskind

https://www.wptv.com/news/region-c-palm-beach-county/u-s-army-warns-of-fake-text-messages-about-military-draft

PALM BEACH COUNTY, Fla. — The U.S. Army wants people to be aware of fake text messages circulating that tell people they have been selected for a military draft.

These messages are popping up amid the tensions with Iran. The U.S. Army Recruiting Command says it has received multiple calls and emails about the fake messages, and "wants to ensure Americans understand these texts are false and were not initiated by this command or the U.S. Army," according to a news release. The Army also reiterates that the decision to enact a draft is not made by U.S. Army Recruiting Command. The Selective Service System manages registration for the Selective Service. It also says its website saw very high traffic as misinformation spread among the public.

"The Selective Service System is conducting business as usual," according to its official Facebook page. "In the event that a national emergency necessitates a draft, Congress and the President would need to pass official legislation to authorize a draft." The draft has not been in place since the Vietnam War and was abolished in 1973. In order for the draft to be reinstated, the U.S. House of Representatives and the Senate would need to approve a new bill, and the president would need to sign it into law. It is also important to note that registering for the Selective Service, which is still required for men 18-25, does not enlist a person into the military. Army recruiting operations are proceeding as normal.

**School Safety Newsletter**

Statewide Terrorism &
Intelligence Center
2200 S. Dirksen Parkway
Springfield, IL 62703
Phone: 217-558-2661
E-Mail:
Isp.schoolsafety@illinois.gov

**Mia A. Ray**
School Intelligence
Officer