SCHOOL SECURITY PACKET:
EMERGING THREATS AND TRENDS

NOVEMBER 2018

READY DC

HSEMA

GOVERNMENT OF THE DISTRICT OF COLUMBIA
MURIEL BOWSER, MAYOR

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security and Emergency Management Agency

Muriel Bowser
Mayor

Dr. Christopher Rodriguez
Director

August 15, 2018

Dear District Educators:

Earlier this year, Mayor Bowser asked the DC Homeland Security and Emergency Management Agency (HSEMA) to work with District of Columbia Public Schools, DC Public Charter Schools, and the Metropolitan Police Department (MPD) to evaluate the overall preparedness posture of our District's schools.

School administrators and teachers are focused the education and safety of our students. Over the years, DCPS has used the Emergency and Safety Alliance (ESA) to bolster preparedness for schools, staff, and students.

As a member of ESA, HSEMA is launching a new tool to help secure our schools—a resource packet highlighting threats to students and school employees. During the upcoming school year and in coordination with our partners, HSEMA's intelligence bureau—the Washington Regional Threat Analysis Center (WRTAC)—will disseminate the school resource packets highlighting threat issues for students and personnel. These packets will raise awareness of emerging issues, safety trends, and available resources. The WRTAC, in coordination with many partners, reviews emerging terror, crime, and health threats in the District, National Capital Region, and throughout the United States to provide situational awareness.

You are encouraged to actively participate in topics provided in this school resource packet initiative by providing feedback and emailing requests for product topics to WRTAC.AnalysisCenter@dc.gov.

I'm a father of three school-aged children, so for me, this is personal. The safety and security of our children and school staff is of the utmost importance to us. My team pledges to empower you with timely and relevant information.

We look forward to your partnership during the upcoming year.

Respectfully,

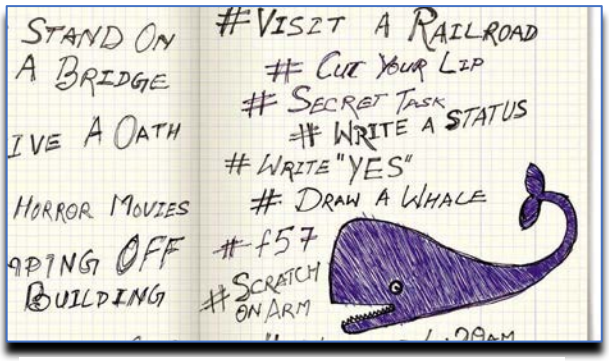
Dr. Christopher Rodriguez
Director

Young People Put at Risk in Social Media Challenge Games

Online social media "challenges"—games that require or dare a user to complete certain tasks—promote risky and dangerous behavior, sometimes resulting in injuries and death. Young teens and adolescents are more likely exposed and susceptible to participating in these types of online engagements due to their prevalent use of social media platforms and applications. Teenagers' lack of impulse control also means they are more prone to engage in risk-taking behavior.

Dangerous social media challenges can be broken down into categories based on the behavior they promote, including, self-harm, extreme physical stunts, and ingestion challenges.

- **Self-harm challenges** promote individuals to self-inflict burning and cutting and some even promote suicide. One of the most well-known challenges—the Blue Whale Challenge—has been connected to over 130 deaths worldwide, including a 16-year-old Georgia girl and a 15-year-old boy from Texas, according to media. The challenge is conducted over a 50-day period with participants assigned tasks to complete via an administrator. Tasks include cutting an image of a whale into one's forearm and ultimately committing suicide on the last day of the challenge.



Journal depicting some of the tasks in the Blue Whale Challenge.
(Source: Hindustan Times)

- **Extreme physical stunts** are not technical or organized social media challenges, rather individuals engage in these stunts usually to promote personal social media profiles and appeal to online followers. Extreme physical stunts include jumping out of moving cars, standing in front of trains, and climbing tall buildings and natural structures to take videos, photos and "selfies." Over 250 people have died in the last six years worldwide from attempts to take selfies in dangerous or extreme places–with more than 85 percent of the victims between the ages of 10 and 30— according to the Journal of Family Medicine and Primary Care study.

- **Ingestion challenges** encourage participants to consume toxic chemicals, alcohol, spices, or large amounts of food such as marshmallows and crackers. Obvious risks include potential choking hazards and complications from blocked airways and inhalation of the substances. Severe allergic reactions are also possible. Harsh chemicals, spices and food risk damaging a victim's esophagus or lungs. According to Poison Control Centers, in 2017 there were 10,000 cases reported involving the ingestion of laundry soap detergent.

Young People Put at Risk in Social Media Challenge Games

Self-Harm Challenges	
Salt and Ice	Participants place salt and ice on their skin and attempt to withstand the pain.
Fire/Fire Spray Challenge	Participants apply flammable liquids to one's body and then set the liquids aflame or use aerosols and lighters to create a makeshift blow torch.
Blue Whale Challenge	A series of tasks are assigned to a player over a 50-day period, beginning with harmless tasks before introducing elements of self-harm and ultimately requiring the player to commit suicide.
Hot Water Challenge	Participants pour boiling or hot water on an unaware individual.
Eraser Challenge	Participants rub a synthetic rubber eraser across their skin while having to say or do something.
Deodorant Challenge	Participants hold a can of aerosol deodorant to the skin while spraying for a prolonged period, the can cools sharply and causes frostbite.
#CutforBieber Challenge	An online hoax and Twitter hashtag campaign created by members of 4chan trying to spread a rumor that fans of Justin Bieber are cutting themselves in response to photographs of the singer allegedly smoking marijuana.
Extreme Physical Stunts	
"In My Feelings"/Kiki Challenge	Participants exit the passenger side of a car and proceed to dance alongside the vehicle while playing the song "In My Feelings."
Chokehold/Pass Out Challenge	A game where a person is choked or chokes themselves until they lose consciousness due to the lack of blood and oxygen supply to the brain.
Kylie Jenner Lip Challenge	Participants insert their lips into a glass container and suck out the air, creating a vacuum that causes their lips to swell.
Car Surfing Challenge	Participants ride on the outside of a moving vehicle on the hood, roof, or trunk while another person drives.
Sunburn Art Challenge	Participants "paint" a design on one's skin with sunscreen and leave the rest uncovered and untreated.
The Game of 72 Challenge	Participants dare one another to disappear for 72 hours without telling relatives.
Rubber Band Face Challenge	Participants challenge one another to see how many rubber bands they can place on their face.
Ingestion Challenges	
Tide Pod Challenge	Participants record themselves eating Tide laundry pods and then post videos of them gagging on the product on YouTube.
Cinnamon Challenge	Participants film themselves eating a spoonful of ground cinnamon in under 60 seconds without drinking anything.
Ghost/Hot Pepper Challenge	Participants film themselves while eating and swallowing a chili pepper that is spicy.
Saltine Challenge	Participants have sixty seconds to eat six saltine crackers without drinking anything.
Banana Sprite Challenge	Participants quickly consume two bananas and one liter of Sprite without vomiting.
Snorting Condom Challenge	Participants must unroll a condom, stuff it up the side of one's nose, then plug the other nostril and inhale until the piece of latex slides into your throat. Then participants reach back and pull it from their mouth.
The Real Food Challenge	Two participants flip a coin to decide who will eat a plate of food, one real and one made of gummy candy.

Social Media Campaign Highlights Consequences of Online Hoaxes

In May, the FBI released its "#ThinkBeforeYouPost" campaign to warn the public that anyone posting school threats and hoaxes online could face federal felony charges with a maximum of five years in prison. FBI Deputy Director said hoax threats disrupt schools, waste law enforcement resources and put first responders in danger. He also cautioned that young people risk going into adulthood with a felony record over an impulsive social media post.

- Federal and state agencies are using the "#ThinkBeforeYouPost" social media campaign to highlight that hoaxes squander public safety resources and risk diverting resources away from real threats. According to the FBI, incidents of hoax type threats to schools are rising, with 300 cases so far in 2018, a jump from 124 cases in 2017.

- In the aftermath of the school shooting in Parkland, Florida, officials and educators are taking online threats more seriously, ramping up school safety protocols, and imposing more severe penalties on perpetrators of online threats.

- In September, two people in Kentucky were sentenced to 21 months and 27 months in prison for creating a fake social media account to make threats against a public school.

- In April 2017, a South Carolina man was sentenced to a year in federal prison after texting a bomb threat to a Veterans Affairs Medical Center.

FBI's Social Media Best Practices

- **NEVER** post or send any hoax threats online.
- Notify local law enforcement immediately – and parents and teachers – if you are a victim of an online threat.
- If you see a threat of violence posted on social media, immediately contact local law enforcement or your local FBI office. The public can also submit a tip to the FBI at tips.fbi.gov.
- **NEVER** share or forward an online threat until law enforcement has had a chance to investigate—doing so can spread misinformation and cause unwanted panic.
- ***Teachers, parents and guardians:*** be aware that posting threats and hoaxes online may be a cry for attention or an effort to get revenge or exert control. Talk to your student or child about the proper outlet for stress or emotional distress. Explain the importance of responsible social media use and the consequences of posting hoax threats.

Additional Resources:

- FBI: Think Before You Post
- Think Before You Post PSA (FBI Chicago)

FDA Cracks Down on Sale and Marketing of E-Cigarettes to Teens

In September, the US Food and Drug Administration (FDA) announced a campaign against the illegal sale and marketing of e-cigarettes to teens that targets 1,300 retailers and 5 major manufactures. E-cigarettes, a $1 billion industry in the United States, are popular among teenagers due to their easy availability and concealment. According to the Center for Disease Control and Prevention (CDC), 2.1 million middle and high-school students used e-cigarette devices in 2017.

- "Vaping" products are sold at local gas stations, bodegas, and "head shops"—stores that sell drug-related paraphernalia. Teens can also purchase e-cigarettes online and from second hand sellers on the street—including at metro stops and schools—without showing proof of age.

- E-cigarette devices, which can also be used to smoke illicit substances, are easily concealed and often resemble pens or USB drives. They emit minimal vapor fumes and smell like fruit or other flavorings, allowing users to smoke indoors undetected.

JUUL e-cigarette "vaping" device with replacement pods

Since September, the FDA has conducted 978,290 retail inspections, issued 77,180 warning letters and approximately 18,560 money penalties to violating retailers—including 29 retailers in the National Capital Region.

- Five major e-cigarette manufacturers—Vuse, Blu, JUUL, MarkTen XL, and Logic—are required to submit plans to address and mitigate the prevalent access of their products to minors no later than November 11. The FDA expanded the award-winning "The Real Cost" public education campaign to further address the issue of accessibility and prevention of e-cigarette use in minors.

- Additional warning letters were sent to online retailers "selling misleadingly labeled and/or advertised e-liquids resembling kid-friendly food products such as candy and cookies."

Additional Resources:

- FDA Press Release Statement
- FDA: The Real Cost Campaign
- FDA Cracks Down on E-Cigarettes to Curb Teen-Vaping 'Epidemic'

Cyber: Make Your Classroom a Haven for Online Safety

In honor of DC Homeland Security and Emergency Management Agency (HSEMA)'s National Cybersecurity Awareness campaign, the WRTAC is sharing the following tips to help school professionals within the District learn more about cybersecurity and how to better protect themselves and their students from cyber threats.

You lock the doors of your home to counter the physical threat of an intruder stealing your belongings or harming your loved ones, but have you thought about protecting your classroom from cyber threats? Have you taken steps to protect your school network and keep your internet-connected devices from being hacked? Do you teach your students how to stay safe online?

If you answered "no" to any of these questions, please read the following tips to help protect yourself and your students from some of the more common cyber threats.

- Change default usernames and passwords on devices such as routers, DVRs, and other internet-connected devices. Hackers can use default login credentials to gain unauthorized access to devices and infect them with malware, steal data, and spy on users.

- Monitor and limit student's internet usage by modifying the settings on your router. If possible, block access to known malicious or inappropriate websites.

- Talk to your students about the dangers of sharing too much personal information online. Tell them not to share their phone numbers, home addresses, or school locations on social media, public forums, or with people they do not personally know.

- Be careful letting your students play online multiplayer games as they can be used as vehicles for cyberbullying. Additionally, sexual predators can use these games to contact children and gain their trust. Advise your students to tell you immediately if they are victims of cyberbullying or if they have received unwanted contact through an online game.

For more cybersecurity tips, visit the District of Columbia's Office of the Chief Technology Officer (OCTO) at octo.dc.gov/cybersecurity and the National Cyber Security Alliance at StaySafeOnline.org.