# SCHOOL SECURITY & PREPAREDNESS PACKET:

## EMERGING THREATS AND TRENDS

## FALL 2019

NOVEMBER 2019

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

November 26, 2019

Dear District Educators:

The District of Columbia's Homeland Security and Emergency Management Agency (HSEMA) and the National Capital Region Threat Intelligence Consortium (NTIC) are pleased to continue providing timely and relevant information to our education partners, parents, guardians, and students through the quarterly School Security and Preparedness Packet.

The NTIC is based in HSEMA and is part of the national network of fusion centers that the US Department of Homeland Security (DHS) has designated as strategic partners for sharing information on natural and manmade threats. The NTIC partners with fusion centers in Maryland and Virginia, as well as DHS. Together, we share and assess information on potential regional threats and hazards—including terrorism, crime, and natural hazards. The NTIC is the National Capital Region's (NCR) only all-hazards fusion center and serves a wide customer set, operating 24 hours a day, seven days a week.

The NTIC is comprised of four centers. One of the four, the Public Safety Center (PSC), is the NTIC's interface with our largest customer and partner—the public. The PSC is responsible for leading the research and analysis that HSEMA provides in its School Security and Preparedness Packet each quarter. The PSC values public engagement and is dedicated to writing unclassified intelligence products to inform and prepare NCR residents for all hazards. All public-facing products can be found at www.ncrintel.org.

Below is the second edition of HSEMA's school security packet for the 2019-20 school year. I encourage your participation in this initiative and welcome your feedback and suggestions for product topics for future security packets via nticpsc@dc.gov. We hope these school security packets help facilitate meaningful conversations between educators, school personnel, students, and families.

Respectfully,

Dr. Christopher Rodriguez
Director

WE ARE WASHINGTON DC

# SCHOOL SAFETY & EMERGENCY PREPAREDNESS

## UPCOMING EVENTS

**RESTORATIVE JUSTICE AND IN-SCHOOL SUSPENSION**

This session will take a deeper look into school suspension and how school staff can transform the space, outcomes, and reflection through a restorative lens.

**December 19, 2019**
9:00AM - 5:00PM

Office of the State
Superintendent of Education
1050 First Street Northeast
First Floor, Eleanor Holmes
Norton I, Room 108
Washington, DC 20002

SIGN UP HERE

## MAIN ARTICLES

GOVERNMENT OF THE
DISTRICT OF COLUMBIA
MURIEL BOWSER, MAYOR

NATIONAL CAPITAL REGION
THREAT INTELLIGENCE CONSORTIUM
DC DEPARTMENT OF FORENSIC SCIENCES

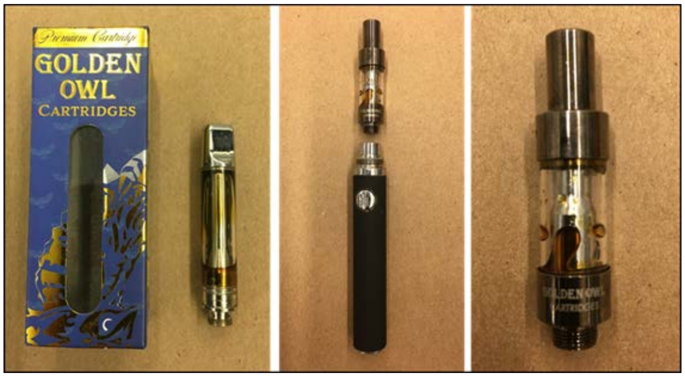
November 26, 2019

Product No. 2019-11-046
NTIC SIN No. 6 | HSEC No. 6

# Vape Cartridges Containing THC Linked to Lung Injury

***Lung injuries and deaths tied to the use of e-cigarettes or vaping products are likely caused by THC vape cartridges with after-market modifications, especially those that contain thickeners and additives.*** The US Centers for Disease Control and Prevention (CDC)—which has dubbed this condition EVALI, e-cigarette, or vaping, product use associated lung injury—estimates that vaping has caused lung injury in over 2,100 US residents, from 49 states and the District of Columbia, and has killed more than 40 people. Most of the afflicted were below the age of 35. Six of these cases have occurred in the District, including one reported death.

- According to the CDC, while no single substance has been linked to every case, 83 percent of evaluated patients for whom data is available have reported using vape cartridges containing THC. There is mounting evidence that vitamin E acetate, an additive present in some THC-containing cartridges, is the likely cause of injury.



THC vape cartridge with packaging (Left). Positioning of how cartridge assembles to base (Middle). Close view of cartridge containing residue THC oil (Right). (Source: DC Department of Forensic Sciences)

- Testing at the DC Department of Forensic Sciences Public Health Lab confirms the presence of THC in cartridges tied to five out of six cases in the District; at least one cartridge from each case also contained vitamin E acetate.

***Cartridges obtained from informal sources such as friends or dealers (in person or online) are more likely to contain hazardous chemicals than retailer sold cartridges.*** Users are cautioned not to use non-manufactured or modified cartridges, especially those that contain THC.

## Symptoms of E-Cigarette or Vaping Product Use Associated Lung Injury (EVALI)

***According to the CDC, EVALI can cause symptoms that resemble pneumonia or the flu, such as:***

- Coughing, chest pain, shortness of breath;
- Abdominal pain; nausea, vomiting, diarrhea;
- Fever, chills, fatigue; and
- Unexpected weight loss.

Some patients have reported symptoms manifesting over a few days, while others have reported symptoms taking weeks to develop. ***Anyone experiencing these symptoms who has used a vaping product in the past three months should seek immediate medical attention.***

NATIONAL CAPITAL REGION
THREAT INTELLIGENCE CONSORTIUM
Situation Awareness Bulletin

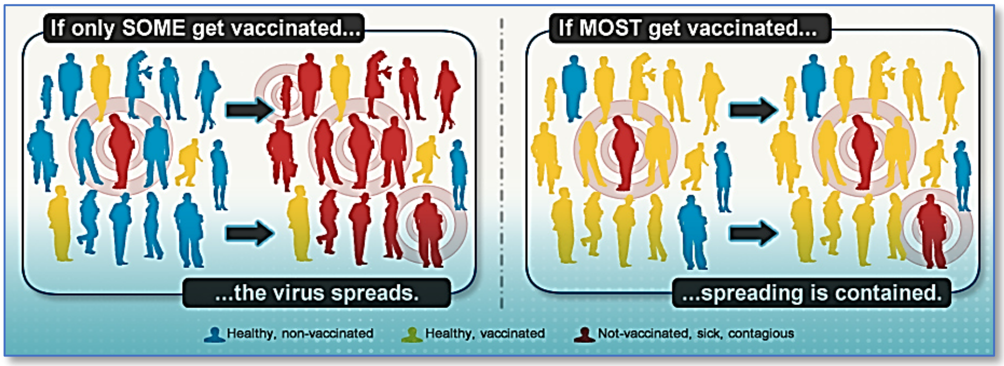
November 26, 2019

Product No. 2019-11-033
NTIC SIN No. 6 | HSEC No. 6, 6.2

## Building Community Resiliency Against Vaccine-Preventable Diseases

***Communities looking to build resilience against common infectious diseases can increase herd immunity by encouraging vaccinations for preventable diseases and addressing vaccine hesitancy spread through mis- and disinformation.*** Herd immunity occurs when a large percentage of individuals in a community—such as schools and offices—are immunized against vaccine-preventable contagious diseases.

***Vaccinations can be effective in preventing outbreaks of infectious diseases such as measles, whooping cough (pertussis), and seasonal influenza***[1]. In 2019, the United States experienced the largest number of reported measles cases since 1992, with the majority of cases among people who were not vaccinated. The United States also endured a severe 2017-2018 influenza season with higher rates of outpatient visits and hospitalizations compared with recent seasons. The 2017-2018 influenza vaccine is estimated to have reduced overall risk of having to seek medical care by 40 percent, according to the Centers for Disease Control and Prevention.


If only SOME get vaccinated...
...the virus spreads.
If MOST get vaccinated...
...spreading is contained.
Healthy, non-vaccinated
Healthy, vaccinated
Not-vaccinated, sick, contagious

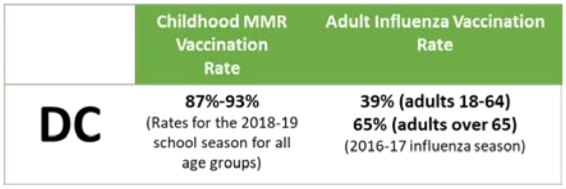
*Source: Centers for Disease Control and Prevention*

- Herd immunity becomes most protective when vaccination rates in a population are high—that is a 93 to 95 percent vaccination rate for childhood vaccine-preventable diseases such as measles and a 95 percent rate for whooping cough. Seasonal influenza prevention in adults requires at least a 70 percent vaccination rate.[2]
- Herd immunity also better protects vulnerable people from vaccine-preventable diseases, creating resiliency in communities. Vulnerable people include infants too young to be vaccinated, the elderly, people with some serious allergies, and those with weakened or failing immune systems due to cancer, HIV/AIDS, type 1 diabetes, or other health conditions.

[1] Not all vaccine-preventable diseases are reviewed in this bulletin. Vaccinations for measles are commonly referred to as the Measles, Mumps and Rubella (MMR) vaccination. Only references to measles are presented in this bulletin.

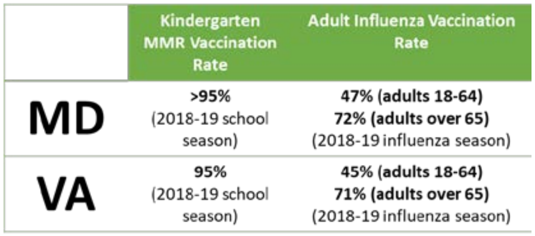
[2] Immunization rates for vaccination-preventable diseases in all age groups can be found through the Office of Disease Prevention and Health Promotion.

***The District of Columbia, Maryland, and Virginia's vaccination rates for childhood vaccine-preventable diseases—such as measles and whooping cough—are higher than the level of vaccination rates for influenza in adults***. For example, in DC vaccination rates for adults aged 18 to 64 years was less than 40 percent during the 2016-2017 influenza season. This indicates there was a lower herd immunity for influenza. Adults can contribute to the resiliency of their communities by getting an influenza vaccine anytime during the influenza season, which generally runs from October to May.



| | Childhood MMR Vaccination Rate | Adult Influenza Vaccination Rate |
|---|---|---|
| DC | 87%-93%<br>(Rates for the 2018-19 school season for all age groups) | 39% (adults 18-64)<br>65% (adults over 65)<br>(2016-17 influenza season) |

*Source: Washington Post (Childhood MMR), and Centers for Disease Control and Prevention (Adult Influenza)*



| | Kindergarten MMR Vaccination Rate | Adult Influenza Vaccination Rate |
|---|---|---|
| MD | >95%<br>(2018-19 school season) | 47% (adults 18-64)<br>72% (adults over 65)<br>(2018-19 influenza season) |
| VA | 95%<br>(2018-19 school season) | 45% (adults 18-64)<br>71% (adults over 65)<br>(2018-19 influenza season) |

*Source: Centers for Disease Control and Prevention*

***Low vaccination rates indicate vaccine hesitancy—the reluctance or refusal to vaccinate despite the availability of vaccine— negatively impacting the community's herd immunity.*** A worldwide increase in vaccine hesitancy threatens to reverse progress made in tackling vaccine-preventable diseases. One factor contributing to vaccine hesitancy is the spread of mis- and disinformation. A research study of anti-vaccination tweets between July 2014 and September 2017 revealed that, in addition to real Twitter users posting pro- and anti-vaccination messaging, bots, Russian trolls, and content polluters (accounts that disseminate malware) were spreading mis- and disinformation[3], about vaccines.

- Twitter bots are accounts that automate content promotion or production. Vaccine proponents and opponents may disseminate messages using bot networks.
- Russian trolls are disinformation campaigns that are designed to amplify discord around divisive issues; the study indicated these campaigns in the United States gave equal attention to pro and anti-vaccination messaging.
- Content polluters use "clickbait" or divisive content to lure people to click on their tweets. These posts can contain links to malicious websites or files that, when accessed, download malware onto victims' computers.

Earlier this year, Twitter and Facebook tried to disrupt disinformation about vaccines. Twitter now displays a post entitled "know the facts" from the United States Department of Health and Human Services (HHS); when users search words related to 'vaccine' the HHS link pops up and directs them to reliable health information about vaccines.

***Visit your local health care provider for specific vaccination information and guidance.***

**Additional Resources:**

- Why Vaccinate?
- Influenza Vaccination Coverage Information (FluVaxView)
- School Year Vaccination Coverage Information (SchoolVaxView)

[3] NTIC's "How to Detect Disinformation Campaigns"

NATIONAL CAPITAL REGION
THREAT INTELLIGENCE CONSORTIUM
Intelligence Bulletin

November 26, 2019

Product No. 2019-11-042
NTIC SIN No. 2.5, 6 | HSEC No. 6

## Child Predators Leverage Popular Online Communication Platforms

***Child predators are using popular social media applications to scout and initiate contact with potential victims, especially those communication platforms that are popular among a younger demographic—under the age of 18***. A number of these applications advertise privacy-centric features such as end-to-end encrypted messaging, direct messing capabilities, and the ability for users to share photos, videos, and their physical location.

- Child predators, after initially contacting and developing a rapport with victims on one platform, may convince them to move their communications to a different platform to isolate them from other users and make it more difficult for law enforcement to monitor and track predator activity.

**What is Encryption?**

Encryption is the process of encoding information so that is only accessible to authorized parties.

- Although the popularity, features, and usage of communication applications may change rapidly due to acquisitions and rebranding, the following is a list of applications that are known to have been used by predators to target minors.

| Application | Description |
|---|---|
| Discord | Discord is a messaging platform for the gaming community. In 2019, suspects leveraged Discord to contact minors for the purposes of human trafficking. |
| Facebook | Facebook is a social media and social networking platform. In 2017, a popular online musician featured on Facebook and YouTube leveraged Facebook to convince minors to send him sexual videos of themselves. |
| Kik | Kik is a messaging platform. In 2018, a suspect leveraged Kik to send a minor threats after following her from the Live.me application and later coerced the victim into sending pictures. |
| LiveMe | Live.me is a social broadcasting platform. In 2018, a suspect leveraged Live.me to threaten a minor and demand nude pictures and videos. |
| MocoSpace | MocoSpace is social media platform. In 2017, an individual leveraged MocoSpace and Facebook to have sex with a minor. |

Please note, while dating mobile applications and communication platforms can be exploited for predatory intentions this list excludes dating apps.

| | |
|---|---|
| **Omegle** | Omegle is a video chat platform that pairs random users for a one-on-one chat session. In 2019, a suspect leveraged Omegle to engage in sexual acts with a minor at multiple locations. |
| **ooVoo** | ooVoo is video chat and messaging platform. In 2015, an individual leveraged ooVoo to expose himself to two minors. |
| **Smule** | Smule is a video karaoke platform. In 2019, an individual leveraged Smule to sing while almost naked for a video in an alleged "Disney" song group. |
| **Snapchat** | Snapchat is a social media platform. In 2019, an individual leveraged Snapchat to meet with a minor; the individual was later charged with Aggravated Kidnapping and Aggravated Sexual Assault of a child. |
| **TikTok** | TikTok is a short video social media platform. In 2019, an individual leveraged TikTok to initiate sexual conversations with minors. In one case, the individual came to the victim's residence posed as a delivery driver. |
| **Whisper** | Whisper is an anonymous social media platform. In 2018, a suspect—who was a social studies teacher, coach, and city council member—leveraged Whisper to communicate with a minor. |

Parents and guardians are encouraged to check application review sites before downloading such as Common Sense Media, Protect Young Eyes and Smart Social.

NATIONAL CAPITAL REGION
THREAT INTELLIGENCE CONSORTIUM
Intelligence Bulletin

November 26, 2019

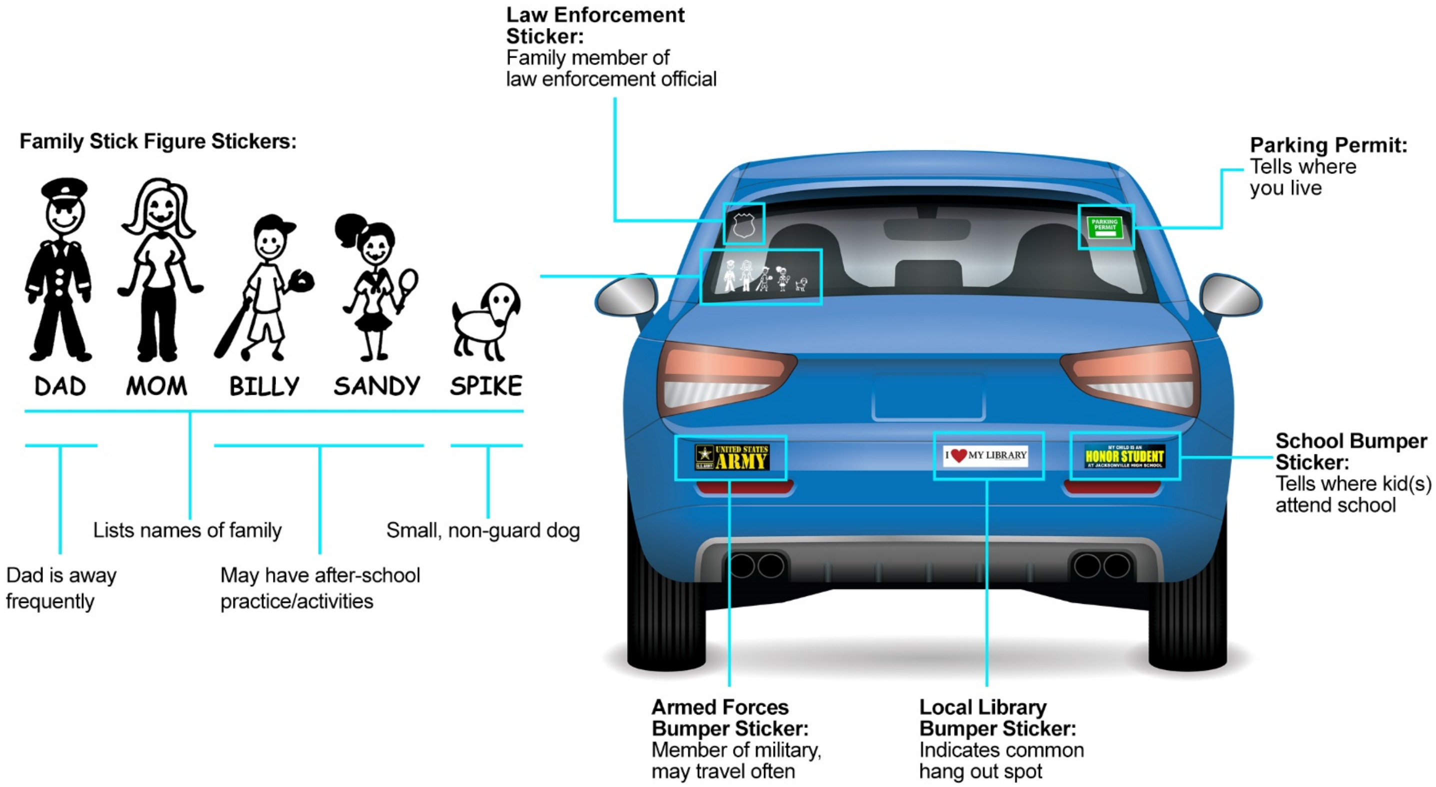
Product No. 2019-10-034
NTIC SIN No. 2.7

# Bumper Sticker Safety Risks: Securing Personal Information

***Malicious actors seeking to target children and families—including child predators and criminals plotting home invasions—could exploit personal information on vehicle bumper stickers.*** Stickers and decals can unintentionally convey information about a driver or a family's geographic location, affiliation with the military or law enforcement, schools children attend, and local sports team memberships. Stickers can also reveal personal information such as the number of family members, their names, and residential information.

- In April, an Alabama sheriff's office informed the public about the risks associated with bumper stickers, offering tips to protect themselves and their families. An Alabama police officer noted that several vehicle break-ins were perpetrated by individuals who admitted to targeting vehicles with specific gun labels.

***Drivers are encouraged to keep their bumper stickers generic.*** The below graphic highlights the personal information unintentionally provided in stickers.


Law Enforcement Sticker:
Family member of law enforcement official
Family Stick Figure Stickers:
DAD
MOM
BILLY
SANDY
SPIKE
Lists names of family
Small, non-guard dog
Dad is away frequently
May have after-school practice/activities
Parking Permit:
Tells where you live
PARKING PERMIT
UNITED STATES ARMY
I ♥ MY LIBRARY
HONOR STUDENT
School Bumper Sticker:
Tells where kid(s) attend school
Armed Forces Bumper Sticker:
Member of military, may travel often
Local Library Bumper Sticker:
Indicates common hang out spot

**Report Suspicious Activity**

For immediate threats or emergencies call 911. Report suspicious activity to the iWatchDC platform.

NATIONAL CAPITAL REGION
THREAT INTELLIGENCE CONSORTIUM

Intelligence Bulletin

November 26, 2019

Product No. 2019-08-009
NTIC SIN No. 4.2 | HSEC No. 8.8, 8.10

## Incel Extremist Rhetoric

***Involuntary celibates (incels) are men who believe society and women are to blame for their failure to develop romantic or sexual relationships. In recent years, incels have conducted acts of violence against women and men who they view as successful at dating.*** Incels often use specific rhetoric in online posts and chatrooms to express their misogynist sentiments, incite violence, or express self-hate. The use of inconspicuous language builds camaraderie among like-minded men and is repeated by men who conducted incel-related attacks. Below is a reference list of commonly-used terms and case studies of perpetrators using the rhetoric. School personnel are encouraged to follow internal protocols regarding cases of hate speech in schools and reference the NTIC's product regarding resources for combating hate speech, bias incidents, and extremism.

## TERMS AND DESCRIPTIONS

### GENERAL TERMS

| | |
|---|---|
| **AMOG** | "Alpha Male of Group"- the man in a group who commands the most attention. "Mog" is the verb form and means to feel intimidated by a supposedly better man |
| **Becky** | A derogatory term referring to an "ugly" woman |
| **Blackpill** | Sexual fatalism; to accept that you have no sexual value and will never have a romantic partner |
| **Bluepill** | To believe that kindness toward women will increase chances of a relationship. Term is not exclusive to incels, but others use the term to mean ignoring reality |
| **Chad** | The opposite of an incel; a "perfect" man who can supposedly get any woman even though he does not treat women well |
| **Femoid/Foid** | Demeaning term referring to women as less than human |
| **-Maxx** | Used as a suffix to mean maximizing or focusing on an attribute, usually a physical one (i.e. looksmaxx, killmaxx) |
| **Normies** | Individuals not part of the incel subculture |
| **PSL** | Stands for "Pickup artists/Sluthate/Lookism"— Incel-related ideas |
| **Redpill** | To believe women are only attracted to a small subset of men with certain physical features. Not exclusive to incels, but others use the term to mean "waking up to a truth" |
| **Stacey** | The "perfect" woman who incels believe spends her days lusting after Chads |

### SELF-IDENTIFIERS

| | |
|---|---|
| **-Cel** | Subset of incel based on physical features, interests, race, or defining traits |
| **Clowncel** | Referring to an incel who identifies with and admires the Joker character from the DC Comics series |

### VIOLENT INTENT

| | |
|---|---|
| **Day of Retribution** | Idealized day in which incels will strike back against Chads and women; also referred to as "Beta Uprising" or "Incel Rebellion" |
| **Go ER/ER/Go Rodger** | To follow the example of Elliot Rodger and go on a killing spree. The letters E and R are sometimes capitalized in unrelated words to imply the same (i.e. sEcuRity) |
| **My Twisted World** | Name of Rodger's manifesto- seen as a basis of incel ideology |
| **RGIF** | "Raping Girls is Fun"— an online extremist community of incels who believe they should harass and assault women as payback |
| **Saint Alek** | Referring to Alek Minassian |
| **Saint Elliot** | Referring to Elliot Rodger |
| **Saint Yogacel** | Referring to Scott Beierle |
| **Supreme Gentleman** | How Elliot Rodger referred to himself. Women go after Chads even though incels are "Supreme Gentlemen" |

### SELF-HARM LANGUAGE

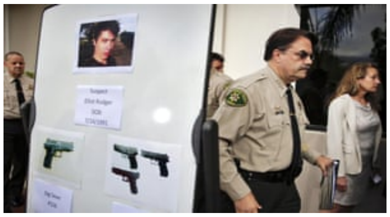
| | |
|---|---|
| **Cope** | A means or an act, thought process, item, or person – of mitigating self-hate |
| **LDAR** | "Lie Down and Rot"— To give up on participating in society |
| **NEET** | "Not in education, employment, or training" |
| **Rope/Roping** | Intent to commit suicide |
| **Suicide-fuel** | Something that makes the individual dive deeper into self-hate; i.e. seeing happy relationships or men who are with multiple women |

## EXAMPLES OF ORIGINS AND USE

*ISLA VISTA ATTACK*

In 2014, 22-year-old Elliot Rodger killed six people and injured 14 others in a stabbing, shooting, and vehicle ramming attack at the University of California, Santa Barbara. Before Rodger committed suicide, he posted a 137-page manifesto and a YouTube video detailing his hatred toward society and women. His manifesto and video became a source of ideology and language for incels. Rodger's words were cited in subsequent incel-related attacks.

*"I don't know why you girls aren't attracted to me, but I will punish you all for it…I'm the perfect guy and yet you throw yourselves at these obnoxious men instead of me, the supreme gentleman."*

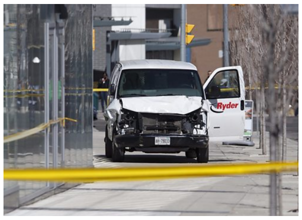


*Police board of Rodger attack* (Source: The Guardian)

*TORONTO VAN ATTACK*

In 2018, 25-year-old Alek Minassian killed 10 people and injured 16 others in a vehicle ramming attack in Toronto, Canada. Minassian told police that he considered Rodger a "founding father" of the incel movement who inspired his own attack. Minassian said he hoped to inspire a "beta uprising."

*"The Incel Rebellion has already begun! We will overthrow all the Chads and Stacys! All hail the Supreme Gentleman Elliot Rodger!"*



*Van used in Toronto attack* (Source: BBC)

NATIONAL CAPITAL REGION
THREAT INTELLIGENCE CONSORTIUM
Intelligence Bulletin

November 26, 2019

Product No. 2019-11-045

# National Capital Region: Outlook for 2019-2020 Winter Season

***During the 2019-2020 winter season, the National Oceanic and Atmospheric Administration (NOAA) expects warmer than average temperatures, more rain, and unpredictable weather patterns in the National Capital Region (NCR).***

- NOAA has indicated that it will be harder to predict weather patterns weeks in advance because at this time, there will be no predictable El Niño or La Niña climate patterns this winter.
- For the NCR, this could mean that there are large swings in temperature and precipitation. Last snow season, the NCR accumulated a total 16.9 inches of snow with maximum snowfall in January.
- DC Homeland Security and Emergency Management (HSEMA) continues to practice preparedness by updating winter weather plans to assist with rapid response, coordinating across agencies to anticipate resource needs, and preparing residents for winter conditions through media outreach and public messaging.

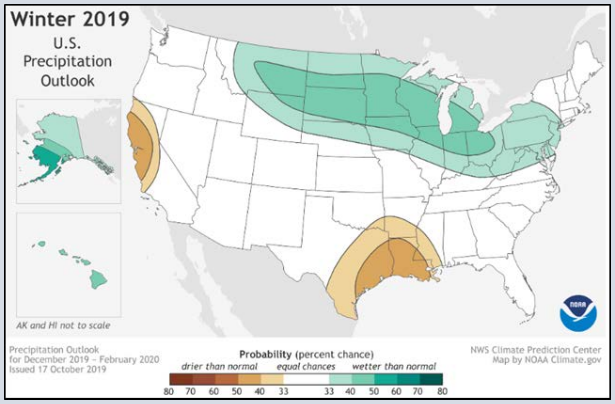
## Student Preparedness Tips

***Many community members spend time outdoors in the winter waiting for the bus, walking to school, or enjoying winter sports. Outdoor activities in the winter can expose you to several safety hazards, but you can take these steps to prepare for them:***

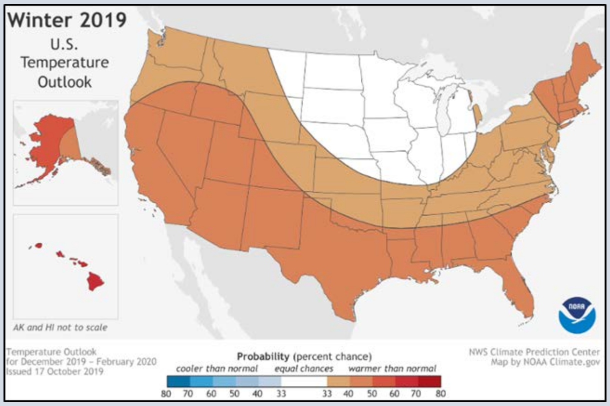
- Pay attention to weather reports and warnings of freezing weather and winter storms. Sign up AlertDC to informed. The Emergency Alert System and NOAA's Weather Radio also provide emergency alerts.
- Wear appropriate outdoor clothing: wear a tightly woven, preferably wind-resistant coat or jacket; inner layers of light, warm clothing; mittens; hats; scarves; and waterproof boots.
- If you drive, create an emergency supply kit for your car.
- If you take public transit, dress in layers and keep additional emergency supplies in a backpack or purse.
- Learn safety precautions to follow when outdoors.
  - Work slowly when doing outside chores.
  - Take a buddy and an emergency kit when you are participating in outdoor recreation.
  - Carry a cell phone.
  - Watch the forecast.

***Visit the following websites for more information on how to stay prepared and notified during the winter months:***

- Sign up for the District's emergency alerts here!
- Learn how to build your personal emergency kit.
- Be aware of school closures and delays.
- Click here for general preparedness tips and considerations.



This 2019-20 Winter Outlook map for temperature shows warmer-than-average temperatures are likely for much of the U.S. this winter. (Source: Weather.gov)



This 2019-20 Winter Outlook map for precipitation shows wetter-than-average weather is expected across the Northern Tier of the U.S. (Source: Weather.gov)

NATIONAL CAPITAL REGION
THREAT INTELLIGENCE CONSORTIUM

Cyber Center

Cyber Advisory

25 November 2019 | Product No. 2019-11-32
NTIC SIN No. 2.5 | HSEC SIN No.1

# Staying Cyber Safe This Holiday Season

As the holiday season rapidly approaches, millions of Americans are preparing for the busiest shopping time of the year. Unfortunately, cyber criminals are also preparing for the holidays along with the lucrative opportunities they bring to steal passwords, financial details, and personal information from busy, unsuspecting shoppers. To help protect yourself and your information, be sure to read the following tips to stay cyber safe while shopping this holiday season:

- **Beware of phishing websites designed to steal your usernames, passwords, and payment card information.** Cyber criminals commonly build webpages that look like popular Internet shopping and banking websites, even using valid digital certificates to make the websites appear legitimate. Although it's important to check that the address of the website you are visiting starts with HTTPS (the "S" stands for "Secure"), double-check the URL to make sure that you are visiting the real site and not a fake one.

- **Remember: if it sounds too good to be true, it probably is.** Companies have already begun advertising their holiday deals on goods and services through marketing emails, online advertisements, and social media platforms to drive business and increase profits. However, be wary of anything that's advertised at extremely low prices. Scammers may use these tactics to trick shoppers into visiting malicious or fraudulent websites. Even legitimate retailers may use the lure of deeply discounted products to try and trick shoppers into signing up for unwanted recurring subscription charges or additional items. This tactic is called "dark pattern manipulation" and it's important for online shoppers to recognize the signs before making any online purchase. Read the NTIC Cyber Center's blog post titled *Securing Our Communities: Dark Patterns* to learn more.

- **Don't click on links or open attachments in emails from unexpected or unknown sources**. 'Tis the season for phishing emails disguised as legitimate communications such as package tracking notifications, e-cards, charity donation requests, or purchase confirmations. Remember, just one click can result in the compromise of your computer, information, and identity.

- **Watch out for malicious mobile apps**. Cyber criminals are increasingly targeting mobile device users by developing and distributing malicious apps designed to steal data, monitor phone usage, or deliver unwanted advertisements. Only download apps from official app stores and make sure to read user reviews prior to installation to help you determine if an app is legitimate. If an app requests certain permissions on your mobile device, make sure that they match its advertised functionality. For example, a simple flashlight app should never need access to your camera or contacts to work properly.

- **Be on the lookout for indications that a website may be compromised with a payment card skimmer**. Profit-motivated cyber crime groups, known collectively as Magecart, inject malicious code into ecommerce websites to steal payment card information from online shoppers. Signs that a legitimate site may be compromised by Magecart include being asked twice to enter payment or login information or being prompted to enter payment card details before being forwarded to a secure payment service provider. No matter where you shop, though, it's always a good idea to monitor bank account statements closely for unauthorized charges and suspicious activity.

- **Gift Cards: Don't get stuck holding a dud.** Criminals often try to steal serial numbers and PINs from gift cards before they are purchased so they can quickly drain any amounts that unsuspecting buyers load onto them upon activation. To avoid raising suspicion, they replace the protective coating that covers these numbers with tape purchased cheaply online. Carefully check gift cards before purchasing and look for any evidence of physical tampering and, if you receive a gift card, use it as quickly as possible to avoid loss or theft.

- **Avoid connecting to unsecured public Wi-Fi networks**. Attackers can easily intercept communications transmitted between mobile devices and Wi-Fi networks in hotels, airports, coffee shops, or other public places to steal passwords, payment details, or other sensitive information without your knowledge. Disable your devices' Wi-Fi connections when not in use and set them to "ask" before joining new or unknown Wi-Fi networks to avoid connecting to unsecured or dangerous hotspots.

- **When possible, use credit cards rather than debit cards online and at physical retailers**. If your payment card numbers are stolen or compromised, using credit cards can limit your liability for fraudulent charges. Debit cards often do not afford these same protections, so any charges incurred will be withdrawn directly from your bank account and can take up to 60 days to reverse.

- **Recycle your unwanted gifts, but never recycle your passwords!** The sale of stolen username and password combinations is big business for criminals on underground marketplaces and recent large-scale data breaches have made it easier than ever for hackers to get their hands on your login information. The best way to protect your online accounts from unauthorized access is to use a lengthy, complex, and unique password for each account. To help you generate secure passwords and easily manage all of your login credentials, consider using a reputable password manager. Also, always enable two-factor authentication (2FA) on any account that offers it for an additional layer of security.