## We're in This Together. Disinformation Stops With You.



#### Disinformation and COVID-19: How State and Local Officials Can Respond

State and local officials play a critical role in countering the abundance of false COVID-19 information that is spreading through public information channels. This toolkit is intended to be used by state, local, tribal and territorial officials. COVID-19 is and will continue to be a threat to public health. Throughout the COVID-19 pandemic disinformation, much of it produced and amplified by foreign actors, has consisted of false treatment and prevention measures, unsubstantiated rumors regarding the origin of the virus, and more. As such, it is imperative that State and local officials continually convey timely, trusted, and verified COVID-19 details and developments to their constituents to avert a vacuum of credible information, which can be exploited for misuse as disinformation by bad actors.

What are the different kinds of false information?

- Misinformation is false, but not created or shared with the intention of causing harm.
- Malinformation is based on fact, but used out of context to mislead, harm, or manipulate.
- **Disinformation is deliberately** created to mislead, harm, or manipulate a person, social group, organization, or country.

All three are harmful, but disinformation is a particular source of concern.

In a February report by the World Health Organization (WHO) report, officials included the term "infodemic" to describe the "overabundance" of information and false information that has arisen in conjunction with the COVID-19 pandemic. State and local government officials should combat ongoing campaigns aimed at undermining the ability of governments to respond to the COVID-19 pandemic. State-level officials should also remind citizens to remain vigilant in their online activities, especially during this time of unprecedented teleworking, virtual education classes, and online personal information gathering regarding the COVID-19 pandemic.

#### **Core Messaging**

See below for messaging that can be used in all public communications, including social media. Provide direct links to your state's health department and underscore that the state pledges to be transparent and will share all public information at that site. Feel free to edit, reuse, and rebrand this document and its content to suit the needs of your constituents.

**Rely on trusted sources.** For situational updates on COVID-19 and stay-at-home guidelines, rely on information provided by state and local health officials, as well as the Centers for Disease Control and Prevention (CDC) at coronavirus.gov and the Cybersecurity and Infrastructure Security Agency (CISA) atcisa.gov/coronavirus.

**Think before you link.** Slow down. Don't immediately click to share posts, memes, videos, or other content you see online. Some of the most damaging disinformation spreads rapidly via shared posts. Check your sources before sharing.

**Be careful what you post.** The information you share online can be misunderstood or repurposed via manipulation. Do a privacy check on your social media accounts and make sure you are not sharing content broadly that you mean only for close family and friends. Be aware that agents of disinformation often steal identities of real people, profile photos, and other information.

Be wary of manipulative content. Agents of disinformation are known to create or repurpose emotional videos and photos, and to use sensational terms to divide us. Be especially careful of content that attempts to make people angry or sad or create division.

**Don't become a victim of COVID-19-related scams.** Be wary of dishonest solicitations designed to take your money and gather your personal information. For more information about scams visit www.consumer.ftc.gov/blog/2020/02/coronavirus-scammers-follow-headlines.

### **TALKING POINTS:**Disinformation Stops With You.



- For COVID-19 facts and stay-at-home guidance, rely on state and local health official websites, as well as the CDC (www.cdc.gov) and FEMA's rumor control webpage at fema.gov/coronavirus/rumor-control.
- Misinformation is false, but not created or shared with the intention of causing harm. Malinformation is based on fact, but used out of context to mislead, harm, or manipulate. Disinformation is deliberately created to mislead, harm, or manipulate a person, social group, organization, or country. All three are harmful, especially now.
- Think before sharing content on social media or emails—be sure to check your sources first.
- Be mindful of what you are sharing or posting online—check your privacy settings.
- Watch out for emotionally manipulative content designed to make us angry or sad.
- Take care when viewing or sharing content that uses sensational terms to divide us in a time of crisis.
- Report scams to trusted agencies, such as the Federal Trade Commission or state consumer protection agencies.

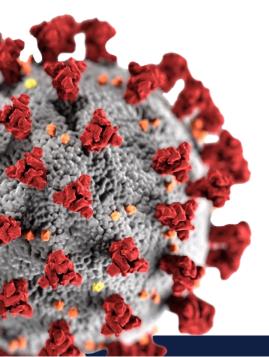
## FAQs:

#### Stopping COVID-19 **Disinformation**

What are the best sources for accurate and reliable COVID-19 information? Your home state health department; your county-level department of public health; U.S. Centers for Disease Control and Prevention (CDC) www.cdc.gov; FEMA's rumor control page at www.fema.gov/rumor-control; and the U.N. World Health Organization (WHO) www.who.int/emergencies/diseases/novel-coronavirus-2019.

What are the different kinds of false information? Misinformation is false, but not created or shared with the intention of causing harm.

Malinformation is based on fact, but used out of context to mislead, harm or manipulate others. Disinformation is deliberately created to mislead, harm or manipulate others.



# We're in This Together. Disinformation Stops With You.

What can our state and local officials do in countering disinformation?

State and local officials have emerged as some of the most visible government officials during the COVID-19 pandemic. In addition to being empathetic, state officials need to quickly and clearly communicate factual information and appropriate actions.

#### Who are the primary malign actors associated with the spreading of COVID-related disinformation?

Russian, Chinese and Iranian statesponsored elements, as well as domestic extremist groups.

What are these malign actors trying to accomplish by spreading disinformation? Their goal is creating chaos, confusion and division. They also want to degrade confidence in U.S. institutions, which in turn undermines our ability to respond effectively to the pandemic.

Who else is spreading disinformation? Scammers, cyber criminals and con artists are also taking advantage of fears surrounding COVID-19. They promote questionable awareness and prevention tips, as well as fake information about cases in your neighborhood. They may ask for donations, offer advice on unproven treatments or spread malicious email attachments.

#### How is false information spread?

All kinds of false information are spread through a variety of mediums, including mainstream media, social media, word of mouth, online forums, texts and emails. When people share disinformation, they may be unaware of the true source of a link or email.

What can our state and local officials tell their constituents about stopping disinformation? Core messaging should emphasize that "we're all in this together" and that "disinformation stops with you." Basic tips to include are:

- Rely on trusted sources such as the CDC and your health department. For situational updates on COVID-19 and stay-at-home guidelines, rely on state and local health officials.
- Think twice before sharing content online.
- Be careful about posting personal information.
- Be on the lookout for content that seems manipulative or overly emotional.
- Report scams to appropriate federal agencies, such as the Federal Trade Commission or state consumer protection agencies.



This poster was created by the Cybersecurity and Infrastructure Security Agency (CISA), an agency within the Department of Homeland Security (DHS), for the purpose of sharing information related to election security and should not be considered an endorsement of any other entity. See CISA.gov/protect2020 for more information.