Disinformation Stops With You

Bad actors spread disinformation to undermine democratic institutions and the power of facts. False or misleading information can evoke a strong emotional reaction that leads people to share it without first looking into the facts for themselves, polluting healthy conversations about the issues and increasing societal divisions.

Do your part to stop the spread of disinformation by practicing and sharing these tips.

Share

Recognize the Risk

Understand how bad actors use disinformation to shape the conversation and manipulate behavior.

Question the Source

Check who is really behind the information and think about what they gain by making people believe it.

Investigate the Issue

Search reliable sources to see what they are saying about the issue.

Think Before You Link

Take a moment to let your emotions cool and ask yourself whether your feelings about the content are based on fact.

Talk With Your Circle

Talk with your social circle about the risks of disinformation and how to respond when you see it.

Learn more at **www.cisa.gov/mdm-resource-library**

Who to follow

Trusted Sources Follow

Rely on official websites and verified social media for authoritative information.

Types of false info

Misinformation
is false, but not created or shared with the intention of causing harm.

Disinformation
is deliberately created to mislead, harm, or manipulate a person, social group, organization, or country.

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

Who spreads disinfo?

- Foreign States
- Scammers
- Extremist Groups

The Cybersecurity and Infrastructure Security Agency (CISA) produced this graphic to highlight tactics used by disinformation campaigns that seek to disrupt critical infrastructure in the United States. CISA's publication of information materials about this issue are intended for public awareness, and are not intended to restrict, diminish, or demean any person's right to hold, express, or publish any opinion or belief, including opinions or beliefs that align with those of a foreign government, are expressed by a foreign government-backed campaign, or dissent from the majority.

Disinformation Stops With You

Disinformation Stops with You

Recognize the Risk

Question the Source

Investigate the Issue

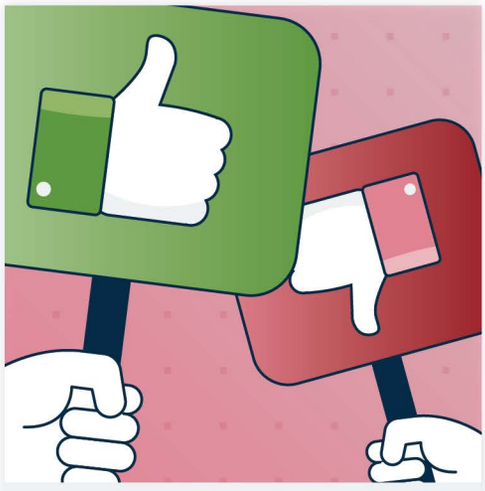
Think Before You Link

Talk With Your Circle

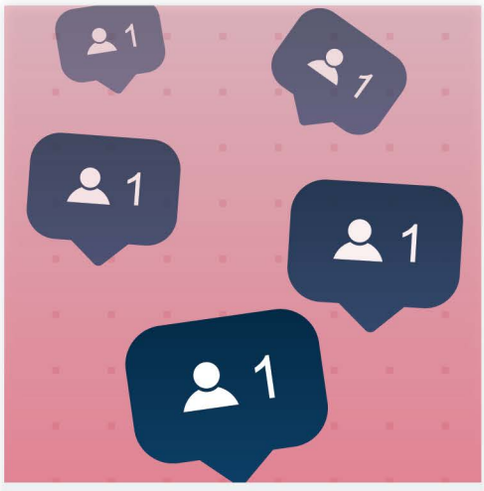
Recognize the Risk

Understand how malicious influencers use disinformation to shape the conversation and manipulate behavior. Once they've built an online presence, they start to post false or misleading content that steers their audience to more extreme positions and spreads to a bigger audience.

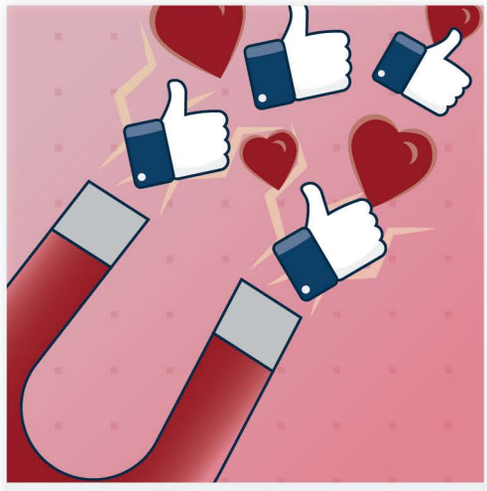
Learn more at www.cisa.gov/mdm-resource-library



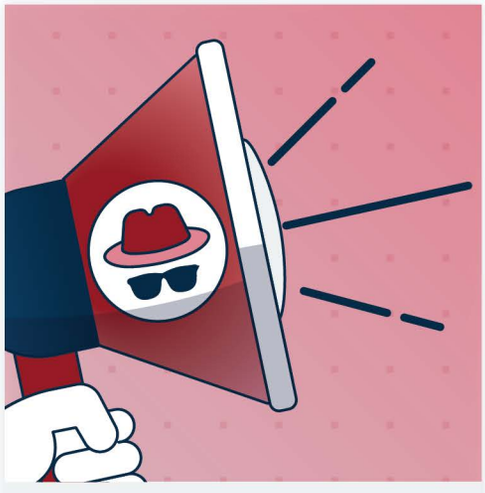
Divide Us Bad actors use divisive societal issues to polarize Americans and push us into echo chambers that further amplify disinformation and obstruct healthy conversations about the issues.



Build a Following They may start to attract followers by posting entertaining, non-controversial content that appeals to their audience and builds trust before sharing disinformation.

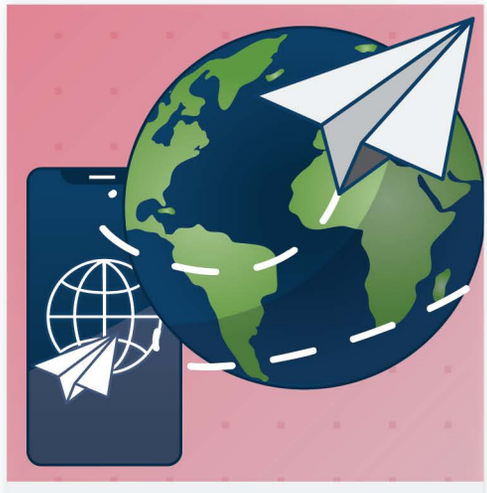


Go Viral They'll often post disinformation as fun memes that are easy to share and get high engagement on social media, like captioned photos and GIFs. It may appear next to other entertaining content.



Amplify Coordinated campaigns spread disinformation across social media platforms, state-funded communication channels, and sometimes even official accounts, reaching far beyond the bad actor's immediate followers.

Make It Mainstream Even disinformation originally shared to a small audience can do huge damage when it is amplified, sometimes gaining mainstream media coverage that may lend it further credibility and a bigger audience.



Real World Effects Bad actors use online disinformation to affect our real-world behavior, like trying to influence how we vote, inciting physical confrontations, and disrupting healthy democratic discussions and participation.

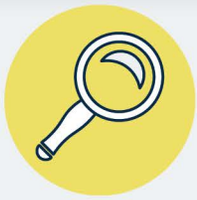
The Cybersecurity and Infrastructure Security Agency (CISA) produced this graphic to highlight tactics used by disinformation campaigns that seek to disrupt critical infrastructure in the United States. CISA's publication of information materials about this issue are intended for public awareness, and are not intended to restrict, diminish, or demean any person's right to hold, express, or publish any opinion or belief, including opinions or beliefs that align with those of a foreign government, are expressed by a foreign government-backed campaign, or dissent from the majority.

Disinformation Stops With You

Disinformation
Stops with You

Recognize
the Risk

Question
the Source



Investigate
the Issue

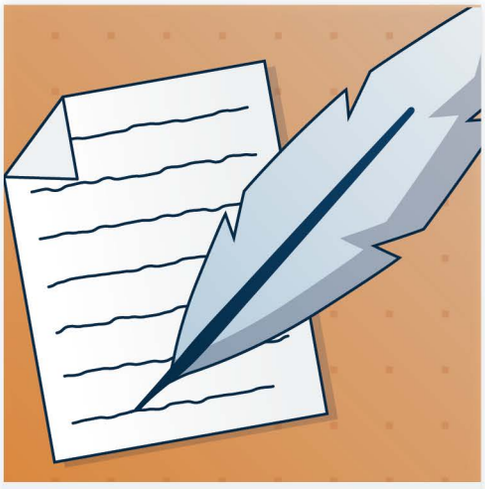
Think
Before You Link

Talk
With Your Circle

Question the Source

Check who is really behind the information and think about what they gain by making people believe it. Disinformation is often designed to look authentic. Critically evaluate content to discern whether it's trustworthy.

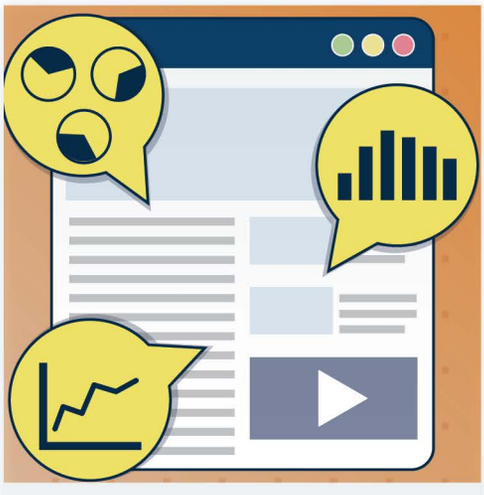
Learn more at www.cisa.gov/mdm-resource-library



Check the Author Research the author's credentials. What else have they published? Are they qualified to cover the topic? If the content doesn't include an author's name, it might be disinformation.

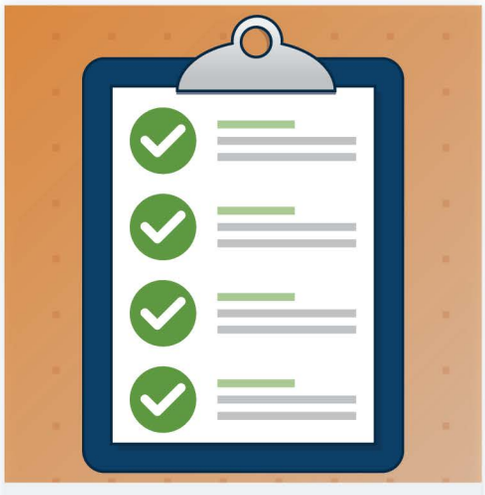
Check the Date When was it published? Outdated content can lack important context, making it irrelevant to current events and misleading to someone reading it in the present.

Check the Message What is the content really saying? Disinformation often pushes a single viewpoint, takes an emotional tone, and uses attention-grabbing headlines that may not match the actual content.



Check for Facts Consider how the author supports their arguments and whether they address counterarguments. Opinions without evidence may not be accurate. Trustworthy fact-checking sites can help evaluate claims.

Check the Sources Credible content will cite supporting sources and provide additional resources for more information. Click on source links to make sure they work and support the content.



Check the Quality Disinformation is often hosted on low-quality websites. Look for signs, such as many ads; questionable sponsors; poor spelling, grammar, and punctuation; and suspicious URLs that mimic legitimate news sites.

The Cybersecurity and Infrastructure Security Agency (CISA) produced this graphic to highlight tactics used by disinformation campaigns that seek to disrupt critical infrastructure in the United States. CISA's publication of information materials about this issue are intended for public awareness, and are not intended to restrict, diminish, or demean any person's right to hold, express, or publish any opinion or belief, including opinions or beliefs that align with those of a foreign government, are expressed by a foreign government-backed campaign, or dissent from the majority.

Disinformation Stops With You

Disinformation Stops with You

Recognize the Risk

Question the Source

Investigate the Issue

Think Before You Link

Talk With Your Circle

Investigate the Issue

Search other reliable sources to see what they are saying about the issue. A thorough search will help make sure you that you are sharing accurate information. Don't share content if it isn't from a credible source or you can't find another credible source to confirm it.

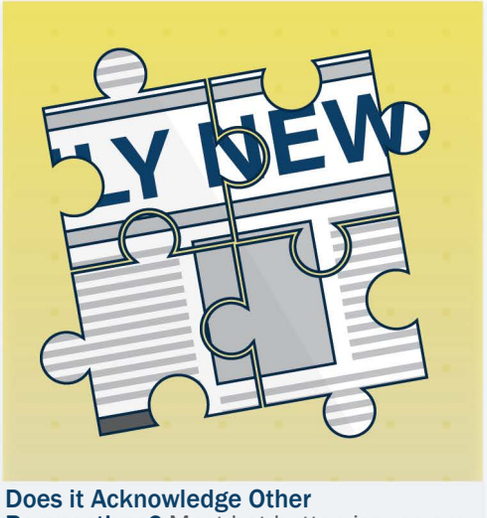
Learn more at www.cisa.gov/mdm-resource-library

Is the Source Credible? Look at the site's "About" page to see whether it includes detailed information, such as its values, ownership, location, funding, and contact information.

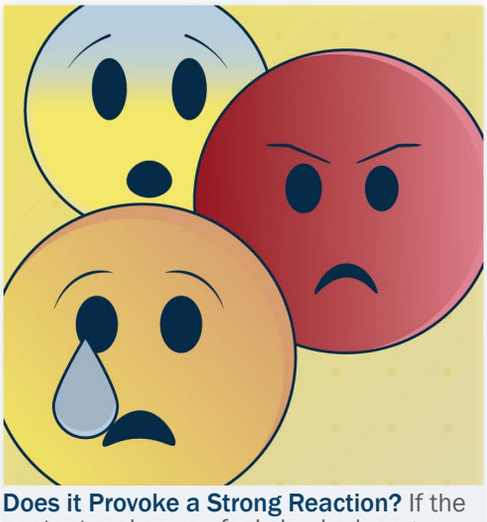
What are Credible Sources Saying? Search the issue on trustworthy sites. If the facts reported by credible sources don't align with the content you're reviewing, don't share it.

What are Fact Checkers Saying? It's easy to believe things that confirm our views. If a claim seems too good to be true, see whether a trustworthy fact-checking organization has evaluated it and provided additional context.

Is Your Investigation Neutral? Make sure you are using unbiased search language and remain open-minded to evidence that might contradict your beliefs.



Does it Acknowledge Other Perspectives? Most hot-button issues are complicated. Although all authors have their own viewpoint, credible sources will recognize other perspectives and provide factual context around the issue.



Does it Provoke a Strong Reaction? If the content makes you feel shocked, angry, or sad, consider that its purpose may be to get you to respond emotionally and share it without confirming its accuracy.

The Cybersecurity and Infrastructure Security Agency (CISA) produced this graphic to highlight tactics used by disinformation campaigns that seek to disrupt critical infrastructure in the United States. CISA's publication of information materials about this issue are intended for public awareness, and are not intended to restrict, diminish, or demean any person's right to hold, express, or publish any opinion or belief, including opinions or beliefs that align with those of a foreign government, are expressed by a foreign government-backed campaign, or dissent from the majority.

Disinformation Stops With You

Disinformation Stops with You

Recognize the Risk

Question the Source

Investigate the Issue

Think Before You Link

Talk With Your Circle

Think Before You Link

Take a moment to let your emotions cool and ask yourself whether your feelings about the content are based on fact. Disinformation is designed to evoke a strong emotional reaction that bypasses your critical thinking. You can interrupt the cycle of disinformation by taking time to research the content and reflect on whether sharing it would benefit the conversation.

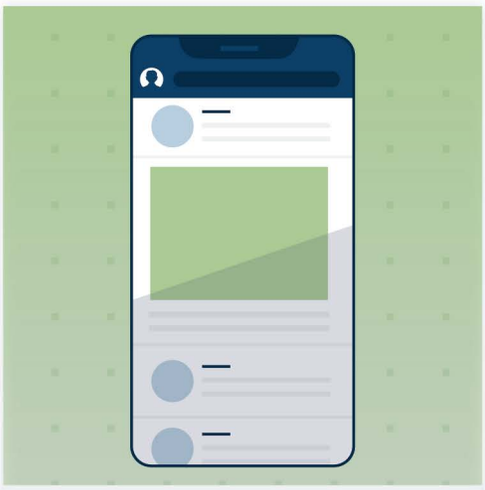
Learn more at www.cisa.gov/mdm-resource-library

Know the Risk Sharing something you see online can seem harmless in the moment, but spreading disinformation can damage our ability to have meaningful conversations.

Know the Content Headlines and captions are often exaggerated to get an emotional response. Take time to read the entire post and determine whether they accurately reflect the content.

Know the Facts Investigate the issue being discussed. Check with trustworthy sources and fact checkers to verify the claims and make sure that they have not been taken out of context.

Know the Source Question who is really behind the content. Critically evaluate the credibility of the author and the legitimacy of the outlet by checking for facts, sources supporting the claims, and quality of the site.



Know Why You're Seeing It Social media algorithms promote content they think you will engage with, sometimes through specific targeting. If it was shared by a friend, make sure you trust the original source as much as the friend.

Know Yourself Ask yourself why you are sharing the content. People often share content that confirms their beliefs, even if it is untrue. If you wouldn't share it in person, don't share it online.

The Cybersecurity and Infrastructure Security Agency (CISA) produced this graphic to highlight tactics used by disinformation campaigns that seek to disrupt critical infrastructure in the United States. CISA's publication of information materials about this issue are intended for public awareness, and are not intended to restrict, diminish, or demean any person's right to hold, express, or publish any opinion or belief, including opinions or beliefs that align with those of a foreign government, are expressed by a foreign government-backed campaign, or dissent from the majority.

Disinformation Stops With You

Disinformation Stops with You

Recognize the Risk

Question the Source

Investigate the Issue

Think Before You Link

Talk With Your Circle

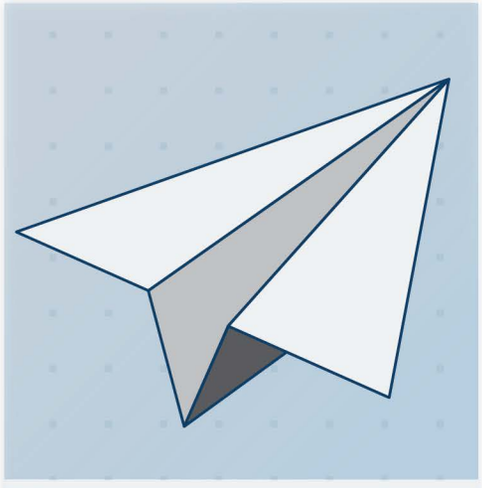
Talk With Your Circle

Talk with your social circle about the risks of disinformation and how to respond when you see it. It's probably not worth engaging with every piece of disinformation, but speaking up can help stop the spread. Do your research and share what you know with friends and family.

Learn more at www.cisa.gov/mdm-resource-library

Come Prepared Make sure you've done your homework and know the facts before starting a conversation. Even if you're sure it's disinformation, brush up on the latest evidence to be safe.

Decide If It's Worth It Once you have the facts, evaluate whether it's worth weighing in. Will your response help the conversation or cause conflict?



Respond Privately If you decide to respond, try doing so via direct message or even an offline conversation. Public comments can give disinformation more visibility and make discussions more confrontational.

Focus on the Facts If you do respond publicly, lead with the truth and don't repeat the false claim. Provide links to neutral, credible sources with more information about the issue.

Be Respectful Try to understand the beliefs of the person you're speaking with so you will be heard in return. It can be hard to change attitudes, but stay calm, positive, and empathetic to get your message across.

Be a Resource Stopping disinformation when you see it is important, but you can help friends and family build resilience to disinformation by proactively sharing resources and tips for doing their own fact-checking.

The Cybersecurity and Infrastructure Security Agency (CISA) produced this graphic to highlight tactics used by disinformation campaigns that seek to disrupt critical infrastructure in the United States. CISA's publication of information materials about this issue are intended for public awareness, and are not intended to restrict, diminish, or demean any person's right to hold, express, or publish any opinion or belief, including opinions or beliefs that align with those of a foreign government, are expressed by a foreign government-backed campaign, or dissent from the majority.