Published by: Educause Review
URL: https://er.educause.edu/blogs/2020/10/october-2020-misinformation-disinformation-hoaxes-and-scams

Misinformation, Disinformation, Hoaxes, and Scams

Author: by Jay Gallman
Published: Thursday, October 8, 2020

People have been dealing with dubious information, hoaxes, and online scams since the World Wide Web became publicly available over twenty-five years ago. Statista estimates the current online population at 4.57 billion. Of that total, 2.7 billion people are active Facebook users—up from 2.4 billion people just one year ago.[1] That growth shows no sign of slowing. In the United States alone, there are over 223 million Facebook users. As the events of 2020 unfold and the screen time for users of all ages rises, those seeking to benefit from deceit have been quick to take advantage. The level of sophistication in efforts to mislead and misinform users is ever-increasing, and technology can only do so much to protect us. User awareness and critical thinking skills are essential.

With the 2020 US election season and the current worldwide coronavirus pandemic as a backdrop, there are four major concerns that underscore the need for greater user awareness about the online content posted to social media platforms.

- **Misinformation** is false content that is spread by users in good faith. "Fake news" is not a phenomenon that arose during the forty-fifth presidency. As newspaper readership shifted online, new websites sprung up with legitimate-sounding names like the Denver Guardian and The Boston Tribune. These sites serve up ready-to-share stories and often include links to facilitate sharing on Facebook, Instagram, and Twitter. The reader has no real means of identifying who created the content published on the site and is generally not inclined to fact-check the content before sharing it.
- **Disinformation,** unlike misinformation, is content known to be false by those who spread it. Increasingly, social media platforms like Facebook and Twitter have found themselves fighting wars against fake users and fake news sites. Mark Zuckerberg stated in 2018 that Russian disinformation campaigns on social media platforms during the 2016 presidential campaign were not well understood. Today, the FBI monitors the efforts of foreign actors like the Russian troll group known as the Internet Research Agency (IRA) and sends tips to the social media platforms in an ongoing battle to limit the ability of foreign actors to meddle in domestic affairs. In September 2020, Facebook—acting on a tip from the FBI—announced that it had removed more than a dozen fake accounts and pages linked to the IRA.[2]

These efforts go beyond influencing elections, and America is not the sole target. A 2018 study published in the *American Journal of Public Health* uncovered a link between Russian efforts via Twitter and the anti-vaccination movement in the United States.[3] The goal of this campaign was to promote discord.

- **Hoaxes** are often created to take advantage of a major political, climatological, or human-condition event to persuade people that things that are unsupported by facts are true. Mixing misinformation and disinformation, perpetrators use a situation like the coronavirus pandemic, where people have heightened fears, to convince large numbers of people not only to believe things that aren't real but also to view as hoaxes things that are supported with facts. Disinformation campaigns in the United States have claimed the coronavirus itself is a political hoax. In the United Kingdom, a study of 2,500 English adults found that over 20 percent of them believed the coronavirus outbreak is a hoax.[4]
- **Scams** are ongoing efforts by those simply looking to make money at the expense of the concern of the day. In March, after fraudsters flooded social media platforms with marketing messages offering bogus cures and unapproved COVID-19 treatments to a scared public, the US Food and Drug Administration (FDA) sent warning letters to seven companies for selling unapproved coronavirus drugs and treatment products. Notable among them was *The Jim Bakker Show,* a daily broadcast featuring convicted felon and televangelist Jim Bakker, who changed with the times and moved from cable television to the web as his platform for perpetrating fraud. The effort to identify these operations is ongoing, and new scams offering untested treatments and unapproved testing kits continue to appear in people's social media feeds. Often, these efforts are outright financial scams that take money people pay for goods and services related to COVID-19 and deliver nothing.

Turning the Tide

It is unrealistic to expect that social media platforms will be able to implement changes to eliminate these undesirable practices in the near term. Nor is it likely that those who share content via social media despite the platform labeling the content as false or of dubious origin will be swayed. We can, however, resist the urge to repost and retweet content without fully reading it first and, where possible, doing our own fact-checking.

If the original source of a story is one you are not familiar with, search the web to see if any outlet that would be considered mainstream is also covering the story. Media bias is real, and an excellent resource for evaluating news sources for both political bias and factual veracity is Ad Fontes Media's Media Bias Chart, which focuses on analyzing the news content of articles and news-focused television shows. One of the most respected sources from that chart, Reuters, maintains its own fact-check web page that tracks current popular claims.

In a recently published study, researchers at the University of California (UC) San Diego School of Medicine found thousands of social media posts on two popular platforms—Twitter and

Instagram—tied to financial scams and possible counterfeit goods specific to COVID-19 products and unapproved treatments. Timothy Mackey, associate adjunct professor at UC San Diego School of Medicine and lead author of the study, provided the following three sound pieces of advice to help people identify a fraudulent post or scam:

1. If it sounds too good to be true, it probably is. Look out for mentions of bulk or rapid sales, cheap pricing, and questionable claims such as FDA approval or specific certifications.
2. Be wary of products imported from another country. If you're a United States consumer, it is likely illegal to import products such as COVID-19 tests from another country. Such purchases should be considered risky.
3. Watch out for illegitimate contact methods. If the seller is conducting business or a transaction through social media direct messages or another non-traditional communications application, including Skype or WhatsApp, it probably isn't legitimate.[5]

Finally, encourage others to engage in critical thinking around what they read and share online. When possible, avoid getting caught up in discussions that may only serve to give these stories more attention than they warrant. Use the tools in each platform to report posts and sites you believe may contain false or intentionally misleading information.

Notes

1. J. Clement, "Global Digital Population as of July 2020," Statistica (website), July 24, 2020. ⮌
2. *August 2020 Coordinated Inauthentic Behavior Report,* (Menlo Park, CA: Facebook, August 2019). ⮌
3. David A. Broniatowski et al., "Weaponizing Health Communication: Twitter Bots and Russian Troll Amplify the Vaccine Debate," *American Journal of Public Health,* September 12, 2018. ⮌
4. Daniel Freeman et al., "Coronavirus Conspiracy Beliefs, Mistrust, and Compliance with Government Guidelines in England," *Psychological Medicine,* May 21, 2020. ⮌
5. Tim Ken Mackey et al., "Big Data, Natural Language Processing, and Deep Learning to Detect and Characterize Illicit COVID-19 Product Sales: Infoveillance Study on Twitter and Instagram," *Journal of Medical Internet Research Public Health and Surveillance* 6 no. 3, (July–September 2020); Jeanna Vazquez, "Researchers See an Increase in Fraudulent COVID-19 Posts on Social Media," (news release), UC San Diego Health, August 25, 2020. ⮌

Jay Gallman is a Security Analyst at Duke University.