Tips for Spotting and Stopping Misinformation on COVID-19

From rumors to false stats, misinformation about COVID-19 is running rampant online. Cybersecurity companies are reporting an uptick in cyberattacks using the COVID-19 pandemic to trick victims into clicking on links that lead to hacked sites or downloading malicious software designed to spy on them or steal personal information. Watchdogs are seeing a rise in sites pushing unproven medical advice or cures. By following the tips below, you and your family can stay safe and informed, as well as help prevent cybercriminals and purveyors of misinformation from succeeding.

SPOT:

Always be alert and aware of potential scams and health hoaxes

- Always think twice about the information you read online. If you and your family have begun spending more time surfing online, scrolling through social media, and receiving emails about COVID-19, be extra critical of what you're reading, believing, and sharing. Talk to your kids and other loved ones about doing the same.
- Analyze the tone. If a message uses sensationalized language, such as text in ALL CAPS or lots of exclamation points it's probably not credible information.
- Be wary of stories that rely on anecdotal evidence or personal testimonials to promote cures that sound too good to be true.
- Be suspicious of requests for secrecy or pressure to take action quickly.
- Check out NewsGuard's real-time reporting on COVID-19 misinformation to familiarize yourself with the common myths about COVID-19 and the reasons they are untrue at **https://www.newsguardtech.com/covid-19-resources/**

TREND MICRO | cares

NewsGuard

VERIFY:

Always verify the source and question the legitimacy of information online

- Always verify that the information you're reading is coming directly from a reliable source. Try to stick to authoritative sources for the most up-to-date information about COVID-19, such as the World Health Organization, the Centers for Disease Control and Prevention, or your local government officials.
- If you're unsure about the credibility of the source, double-check claims by searching elsewhere to see what other sources say.
- Carefully scrutinize all email requests for the transfers of funds to determine if the requests are out of the ordinary.
- Teach yourself and your kids to ask the tough questions. Here are a few the **National Association for Media Literacy Education suggest:**
  - Why was this piece of content or article created?
  - Who made it?
  - How do I know if it's true?
  - What's missing?
  - Who might benefit from the message behind it?
  - Who might be harmed by the message?

STOP:

Always do your part to prevent online scammers and purveyors of misinformation

- Drown out misinformation by sharing factual updates about COVID-19 from reliable sources like CDC.gov, which offers a social media kit.
- If you see a friend sharing false information, politely set the record straight and refer them to a credible source on the subject.
- Protect yourself from hackers and cybercriminals who are using COVID-19 information as click bait, prompting you to click a link that deceives you into giving up personal information or opening an attachment containing malicious software or spyware. Use reputable, up-to-date security software that will protect you or your family.
- Immediately report and delete unsolicited email (spam) from unknown parties. Do not open spam emails, click on links in such the emails, or open their attachments.
- Encourage your friends and family to install **NewsGuard's browser extension**, which provides thousands of source credibility ratings, to protect themselves against COVID-19 misinformation.
- If you come across a site spreading COVID-19 hoaxes that NewsGuard has not yet rated, send a tip here: **https://www.newsguardtech.com/misinformation-hotline/**.