False information & scams

Can we trust everything you read online?

• No! Not everything we read is true. Don’t trust everything.
• We often believe information without checking, but we should be very careful about false information during the COVID-19 pandemic.
• FEMA offers a [Rumor Control website](https://www.fema.gov) to help Americans distinguish rumors and facts during the pandemic.

Where can we get trustworthy information about COVID-19?

• [The World Health Organization](https://www.who.int) (WHO)
• [The Center for Disease Control and Prevention](https://www.cdc.gov) (CDC)
• Info from the White House, the CDC, and FEMA: [Coronavirus.gov](https://coronavirus.gov)
• Websites of hospitals and legitimate academic institutions

Never use information online to diagnose yourself or make medical decisions. If you have health concerns, please check with your healthcare provider.

How do I avoid being a victim of scams?

• Verify sender: Some scammers use “From” email addresses that look like those from a real person or company, but they are not. Check the sender’s actual email address.
• Assess the content: scamming emails are often poorly written and contain lots of errors.
• Check the links before clicking on them:
  • On a computer: Move your mouse to hover over a link, but do not click on it yet. The actual link address (URL) will be displayed, so you can see if it is the same as what is shown in the email.
  • On a smartphone or tablet: Touch the link without letting go until the preview shows. The actual link address (URL) will be displayed, so you can see if it is the same as what is shown in the message.
• Malicious emails often ask people to do something urgently. Don't do what they say.
• If the email, text message, or phone call asks you to send money in *gift cards* or *virtual currencies* (e.g. bitcoin), don’t do it.
• Never provide personal information (e.g. usernames and passwords) to other people.