

Identifying Signs of Fraudulent Communication

Being mindfully aware of suspicious or unusual interactions will help limit the risk of fraudulent activity. Outreach from individuals or groups pretending to work for Gartner who try to get you to provide personal information, money, payment information or accept payment deposits are not legitimate, even if they appear to include Gartner branding.

Do not reply, transfer funds, deposit checks, open attachments, or use contact details provided in the suspicious communication.

To help you identify these fraudulent communications, please note:

- Legitimate Gartner emails are sent from individuals with firstname.lastname@gartner.com emails, or other gartner.com email addresses.
- We will NEVER ask you to wire money anywhere, send us cash, purchase gift cards on our behalf, or provide us with your bank account information.
- We will NEVER send you payment in advance for activities related to employment with Gartner.
- We will NEVER ask for personal information or payment for Gartner services via LinkedIn, or any other social media platform.
- We will NEVER ask you to be a mystery or secret shopper – we don't conduct that kind of research!
- We will NEVER sell tickets to Gartner conferences outside of Gartner's authorized websites, representatives, and registration platform.
- We will NEVER send you a physical third-party check for any amount of funds.

Resources

- Learn more about spotting and reporting [recruitment fraud](#).
- Learn more about known [fraudulent Conferences ticket providers](#) and how to report suspicious activity.
- For additional information about recent scams and how to recognize the warning signs, visit the [Federal Trade Commission's website](#).
- Emails may be sent from email addresses that include the Gartner name. Always be cautious before opening emails, attachments, or responding. If you are concerned about other emails claiming to be from Gartner and want to check if it's legitimate, please contact privacy@gartner.com.