

Be Aware of Fraudulent Communications

You may be contacted by unscrupulous people who pretend they work for Gartner to try to get you to provide personal information, money, or payment information. These communications may include Gartner branding, but they are not legitimate.

To help you identify these fraudulent communications, please note:

- We will NEVER ask you to wire money anywhere, send us cash, 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 you to be a mystery or secret shopper – we don't conduct that kind of research!
- We will NEVER ask for personal information or payment for Gartner services via LinkedIn, or any other social media platform.

Legitimate emails only come from firstname.lastname@gartner.com email addresses. We have provided an example below of a scam email using a fraudulent Gartner email account, with other red flags of a potentially fraudulent communication.

If you've received an email similar to the one below, it is **NOT** valid. If you are concerned about an email claiming to be from Gartner and want to check if it's legitimate, please contact us at privacy@gartner.com.

Please don't reply or otherwise respond to the suspicious email – by doing so, you would confirm your email account is active and you might receive even more spam.

For additional information about recent scams and how to recognize the warning signs, visit the [Federal Trade Commission's website](#).

The image shows a screenshot of an email with several red flags highlighted by callout boxes:

- From:** Gartner R <gartner1199@gmail.com> → Legitimate emails will be sent from a gartner.com email address.
- Subject:** APPLE STORE BRAND-ASSESSOR SURVEY ASSIGNMENT → Scam emails often overuse punctuation or capital letters in the subject line to get your attention.
- Body text:** This envelope contains a check of \$5,900.25 You are required to deposit the check at your bank and wait for funds to be available before you begin your task. → Receiving money unprompted, before completed a requested task, is most likely a scam.

Other visible text in the email includes:

- To: [Redacted]
- Attn: Prospective Brand-Assessor,
- You will be evaluating any APPLE STORE in your Area. The technology market is affected by rapid innovation, regulatory intervention, and overwhelming choice. Therefore differentiation and loyalty are major challenges for brands. We help hardware and software manufacturers by providing a clear understanding of consumer and business, needs, behaviors, and perceptions, enabling them to develop and deliver the most relevant positioning, communications, customer management initiatives, products, and services.
- ASSIGNMENT INSTRUCTION
- You will be evaluating a local APPLE STORE in your city. Our check is for \$5,900.25. You are required to deposit the check at your bank and wait for funds to be available before you begin your task.
- SPECIFICATIONS TO PURCHASE

ITEM 1: Apple store gift card - \$1500
ITEM 2: Apple store gift card - \$1500
ITEM 3: Apple store gift card - \$1000
ITEM 4: Apple store gift card - \$1000

BELOW IS THE EXPENDITURE BREAKDOWN

AMOUNT RECEIVED : \$5,900.25
GIFT CARD (4 PIECES) : \$5,000.00
SALARY : \$900.25

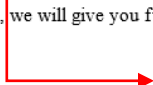
Whilst conducting an assignment always remember that you are incognito so you cannot use notepads in, or within sight of the location.

Please send both email and text message immediately you make the purchase with the picture of the purchased Apple store gift card for our records, peel off the silver strip at the back of the card neatly before taking the picture. The picture of each Apple store gift cards must be clearly and separately.

Please keep the Apple store gift cards safe, we will give you further instructions on how to complete your second task with the Apple store gift cards before end of the week.

Regards,


Gartner Market Research Group
www.Gartner.com



Grammatical errors, or an omission of key words, can help identify a scam email.