

Evite – Is it Real or a Phishing Scam? More Detailed

If you have looked at the document Evite – Is it Real or a Phishing Scam? and want a more detailed explanation, then read on with this document.

1-Check the sender's email address. Real Evite emails ONLY ever come from the domain evite.com and verified subdomains of evite.com. All of these domains are authenticated with SPF, DKIM and DMARC. Phishing emails will sometimes use what looks like personal email or GMAIL addresses to send. **This is a clear red flag**. Evite will never send from a gmail.com, yahoo.com hotmail.com or any personal email.

example - To: your email@website.com

From: Eric Scammer cooleviteguy@evite.com. Here a personal email is being used to send what looks like a real evite.

Subject: Best planning guide you need for birthday parties

Be aware that if the sender appears to be someone you know personally, their account may have been hacked to send the phishing emails.

2-Hover over links before clicking by looking at "View and RSVP" button or any link in the mail and look at the URL that appears at the bottom of your screen. Real evite links go to <https://evite.com> or <https://evite.me>. Scams links go somewhere else entirely. IF the hovered URL does not contain evite.com as the main domain, treat the email as a phishing attempt regardless of how legitimate it looks.

3-Verify email authentication headers (advanced). In Gmail, you do the following:

- a. Open the email in Gmail.
- b. Click the three vertical dot menu in the top right corner of the email.
- c. Select "Show original."
- d. Look for SPF, DKIM and DMARC – all three should say "PASS" for legitimate Evite emails.

Scammers who try to spoof Evite's domains will generally fail these checks and be filtered to spam automatically. If a phishing email does reach your inbox and you check the headers, you will typically see FAIL or SOFTFAIL for one or more of these fields.

What should you do if you receive a phishing email from Evite?

- 1- ***Do not click on any links*** in the email.
- 2- If you already clicked a link, clear your browser's cookies and cache and run an anti-virus scan on your device.

- 3- Report the email as phishing in your email client. (GMAIL: three-dot menu + “Report phishing”).
- 4- Contact Evite customer support with questions or concerns.
- 5- If it appears the sender’s personal email account was hacked, notify the person so they secure their account.

To help protect yourself from phishing texts or mails:

- 1- **Keep security software updated.** Set your computer to update automatically so it will deal with any new security threats. Update your phone’s software regularly too.
- 2- **Use two-factor authentication.**
- 3- **Act quickly.** If you think your scammer has your email account information, change your password to create a new, strong password right away. Then go to IdentifyTheft.gov for specific steps to take based on other information you may have lost.
- 4- **Forward phishing emails to the Anti-Phishing Working Group at <https://apwg.org/reportphishing>** and texts to SPAM (7726). Then report the phishing attempt to the FTC at [ReportFraud.ftc.gov](https://reportfraud.ftc.gov).

Created August 2026