The latest Evite scams are phishing attacks sent via email or text message that mimic digital invitations to steal your login credentials, take over your email account, or install malware. Scammers often use compromised accounts or spoofed display names so the invite appears to come from someone you know.

How the Scam Works

- **Credential harvesting:** Clicking the invite leads to a fake login page asking for your email address and password—or a phone number and verification code—to view party details or RSVP. Real invitations do not require guests to log in with an email password.
- **Account takeovers & spread:** Once attackers get your login credentials, they can hijack your email account, set up hidden forwarding rules or filters, and send fake invites to your contacts.
- **Malware delivery:** Some links or attachments attempt to download malicious files or spyware onto your device to harvest sensitive data.
- **Generic details:** Fake invites often use vague wording (such as a generic celebration) rather than specific event details like a real venue, time, or host notes.

Red Flags to Check

- **Sender address:** Legitimate Evite emails come from evite.com and its verified subdomains—not personal addresses like @gmail.com or @yahoo.com, or misspelled domains. (Even if a friend's real address appears, their account may have been hacked.)
- **Link destinations:** Hover over links before clicking to see if they actually point to evite.com rather than an unrelated or suspicious URL.
- **Unexpected requests:** Be wary of any prompt asking for passwords, special codes to RSVP, or file downloads.

How to Protect Yourself & Respond

- **Verify outside the message:** If an invite looks unexpected, contact the host directly via a separate channel (like a text or phone call) before clicking anything.
- **Use strong security:** Keep devices and browsers updated, use unique passwords, and enable two-factor authentication (2FA). For more details on spotting fake emails, see Evite or guidance from the Identity Theft Resource Center.

- **If you clicked or entered info:** Change your password immediately, turn on 2FA, check account settings for unauthorized forwarding rules, filters, connected apps, or active sessions, and run a security scan. You can also report phishing attempts to the FTC at ReportFraud.ftc.gov and forward scam texts to 7726 (SPAM).