How to Respond to a Calendar Attack

🔴 Calendar Exploit Response Protocol

The Golden Rule: *Contain first. Then clean up.*

✅ IMMEDIATE ACTIONS

- **STOP:** Disable "Automatically add invitations."
- **ISOLATE:** Unpublish public booking links (Calendly, etc.).
- **INSPECT:** Review unknown subscriptions/shared calendars.
- **SAVE:** Screenshot the event details (sender, links) before removal.

⛔ CRITICAL ERRORS

- **NO CLICKING:** Never verify a link by clicking it.
- **NO DECLINING:** Declining confirms your email exists. Delete without notifying.
- **NO AI TRUST:** Read the raw event text; do not rely on AI summaries.
- **NO FORWARDING:** Do not spread the malicious payload to assistants.

Calendar attacks exploit speed. Slowing down is your best defense.

For more actions and insights, see our full blog post on calendar attacks.

⭕ Platform Settings Cheat Sheet

HARDENING YOUR CALENDAR: A Configuration Guide

⚫ **Google Calendar**

Goal: Stop Google from automatically placing unverified invites onto your visible schedule.

1. Open **Google Calendar** on a desktop browser.
2. Click the **Gear Icon** (top right) > **Settings**.
3. In the left sidebar, click **Event settings**.
4. Find **"Add invitations to my calendar"**.
5. Change the setting to: **"Only if the sender is known"** (Strict) or **"When I respond to the invitation in email"** (Moderate). *Do not leave it on "From everyone".*
6. (Optional) Scroll down to **"Events from Gmail"** and uncheck "Automatically add events from Gmail to my calendar."

⚫ **Microsoft Outlook (365 / Web)**

Goal: Prevent email parsing scripts from auto-generating events.

1. Open **Outlook on the web** (https://www.google.com/search?q=outlook.office.com).
2. Click the **Gear Icon** > **Calendar** > **Events from email**.
3. Select **"Don't show event summaries in email or on my calendar"** for all package types (flights, reservations, etc.).
4. Go to **Calendar** > **Automatic processing**.
5. Uncheck **"Automatically process meeting requests and responses to meeting requests and polls."** This forces you to manually accept an invite before it lands on the calendar.

⚫ **Apple Calendar (iCloud / iOS)**

Goal: Force invites to your email inbox so they can be marked as spam, rather than appearing as push notifications on your phone.

1. Log in to **iCloud.com** on a desktop browser.
2. Click **Calendar**.
3. Click the **Gear Icon** (bottom left) > **Preferences**.
4. Click the **Advanced** tab.
5. Under **"Receive event invitations as"**, select **"Email to [your address]"**.
   - *Why:* By default, Apple sends them as "In-app notifications." If you switch this to Email, your email provider's spam filter gets a chance to catch them first, and you can delete them without sending a "Decline" notification.

⭕ The Assistant's Protocol

FOR EXECUTIVE ASSISTANTS: The Gatekeeper Rules

If you manage the calendar for a principal, you are the firewall. Follow these rules:

1. **Verify Out-of-Band:** If an invite appears from a known contact but looks generic (e.g., "Urgent Discussion" with no agenda), text or Signal the sender to confirm. Accounts get compromised; calendars are often the first payload.
2. **No "Forwarding" to Check:** Never forward a suspicious invite to the Principal asking, "Is this real?" This puts the malicious link directly in their inbox. Screenshot it instead.
3. **The "External" Tag:** If your organization uses "External" tagging for emails, ensure your calendar invites also show this tag. Be deeply suspicious of any "Internal" meeting that lacks a clear internal organizer.

⭕ Anatomy of a Fake Invite

RED FLAGS: How to Spot a Poisoned Invite

- **The "Urgency" Title:** Events titled "Final Notice," "Account Suspension," or "Payroll Error." Calendars are for scheduling, not crisis management.
- **The Generic Description:** Descriptions that are vague but contain a link ("Click here to view agenda" or "Review documents securely").
- **The Mismatched Organizer:** An invite claiming to be from "HR Support" but sent from a generic Gmail/Hotmail address or a domain that is *slightly* misspelled (e.g., company-support@gmail.com).
- **The Massive Guest List:** You are CC'd with 50+ other people you don't know (often hidden in the BCC field of the invite metadata).