

Calendar Phishing Attacks

What Is Calendar Phishing?

Calendar phishing uses meeting invitations or calendar events as the delivery method for a scam. Instead of a suspicious email, the attacker sends a calendar invite, or an email with an .ics file attached, that puts a malicious link, fake meeting, or deceptive message directly onto the victim's calendar.

How does it work?

1. **The invite is sent.** The attacker sends an invite from a spoofed or compromised account, often with a title like "Payroll Update," "Account Verification Required," or "Urgent: Review Document."
2. **It lands on the calendar automatically.** Many calendar apps (Google Calendar, Outlook, and others) can add invites without the recipient accepting them. The event can appear on the calendar, trigger a reminder, and sit there looking like a legitimate appointment.
3. **The bait is in the event.** The description or location field contains a link to a fake login page, a "join meeting" link that leads to a credential-harvesting site, a malicious attachment, or a phone number for a fake support line.
4. **The victim acts.** They click the link, enter credentials, call the number, or approve something they shouldn't.

Why does this work?

1. **It bypasses email filters.** Security tools are typically tuned to scan email bodies and the messages, and calendar invites can slip through.
2. **It feels trusted.** People treat their calendar as their own space, so an event on it seems pre-vetted.
3. **Reminders add urgency.** A pop-up notification right before a "meeting" creates pressure to act quickly.
4. **Mobile views hide details.** On a phone, sender information and full link addresses are harder to inspect.

5. **Persistence.** Unlike an email that gets deleted, the event stays on the calendar and may recur.

What are the common variations?

1. **Fake meeting links:** "Join" buttons that lead to spoofed Microsoft, Google, or Zoom login pages.
2. **Fake security alerts:** Events claiming unusual login activity or an expiring password.
3. **Payment or invoice lures:** Events referencing a pending charge, with a "dispute" number to call (a vishing setup).
4. **Spam and scam events:** Prize or crypto offers aimed at personal calendars.
5. **Executive impersonation:** An invite that appears to come from a leader, scheduling an "urgent" call.

What are some Red Flags?

1. An invite from someone you don't know, or an unexpected invite from someone you do
2. Vague or urgent titles about accounts, payroll, or security
3. Links or phone numbers in the description of an event you didn't expect
4. Attachments on an invite
5. A sender address that doesn't quite match the real one
6. Invites that appeared without you accepting them

What should I do?

Individuals

1. Don't click links or call numbers in unexpected invites.
2. Verify with the supposed sender through a separate, trusted channel.
3. Report the invite using your organization's phishing reporting tool, then delete the event.
4. If you did click or enter credentials, report it immediately and change your password.

Organizations

1. Set calendars to **only show invites from known senders** or require manual acceptance of invites from external parties. In Google Calendar and Outlook, this setting is configurable by admins and users.
2. Disable automatic adding of external invites.
3. Apply link and attachment scanning to calendar content, not just email.
4. Enforce Phishing-resistant MFA so stolen credentials are less useful.
5. Include calendar phishing in awareness training and phishing simulations.
6. Make sure users know how to report a suspicious event, since the standard "report phishing" button doesn't always appear on calendar items.