All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Calendar spam and how the calendar folks screwed it up again

As usual, the people designing a vastly deployed system that should be usable by anyone screwed it up by a lack of design consideration, then made it worse as it because exploited, and then will make it even worse by their likely next fix.

Calendar spam

As calendars became more widely used, email was added as a way to automatically invite people to events. You send an email with an invitation, they say YES, and the calendar is entered in their calendar for mutual benefit.

What could possibly go wrong?

Looking at history, email is used to spam. If we let spam email get into our calendars, it will end up populating our calendars with all sorts of spam invitations, overwhelming our calendar system, and leaving us with gobs of spam invitations to where we cannot find legitimate ones.

This should have been obvious to anyone in cybersecurity at least 25 years ago!

So it was ignored like every other cybersecurity thing we already knew about long ago.

So it started to happen

Undesired Google calendar invitations started appearing a few weeks ago in my calendar, not even reaching my inbox first, even though my setting should prevent this. I handle my multiple emails with their different calendars through calendar delegation so I can see the combined calendar and not have overlapping appointments across my various responsibilities. They are clearly spam, claiming bitcoin transfers and such and coming from email addresses with '@gmail.com' but without DKIM or SPM authentication, and sent to gmail which normally used these for its emails. And yet Google calendar accepted them and put them in my calendar.

Of course I had disabled automatic additions to my calendar long ago, but the new AI features apparently re-enabled them, even though I disabled the AI features as soon as they started to pester me. But I might have accidentally clicked on some prompt that flashed in front of me just as I was about to click on something else and enabled something that didn't even remain on the screen long enough to see it.[1]

I am up to about 5 a day at this point, poisoning my calendar. But that's not really the key issue here. The issue is how Google failed to anticipate and respond to it.

And of course the response was stupid security

Blame the victim! Even though the source of the spam email that triggered the calendar invitation appearing was not any of my email addresses, or even forged to claim such, the response to my marking the calendar invitations as spam (I had the option of stopping delegation of the account or stopping the specific message) was to accuse the victim:

1 For those of you who use our assessment processes, the following segment: "Question: Human factors: Disruption: How is disruption of work controlled?" addresses these issues.

> Your calendar event might be in violation of the Google Calendar Program Policies. For this reason, your event may not be visible on the calendars of the event's guests. It is still visible on your calendar, but it might be in your guests' Trash folder in Google Calendar.
>
> Event Title: Renewal Success — Geek Squad Approved
>
> If your event complies with Google Calendar Program Policies, you can contact your guests who use Google Calendar and tell them how to restore their copy of the event from their Trash folder.

Yes, they sent a warning about violating Google's policies to the delegated authority who was the victim of the spam. The violation was removing the spam from the calendar!

STOP IT!

Here are the stupid things they should stop doing:

- **Stupidity element 1:** Allowing Gmail forgeries to be received by Gmail and sent on to user accounts at all. Google knows they are not from Gmail because they control Gmail and include DKIM and SPM headers which were not present in the invitation emails. If you know they are not valid, do not send them to users or calendars.
- **Stupidity element 2:** Not following the settings by users and their administrators because you added a new feature that ignores them. When you add new features, don't get them to ignore the previous user settings – follow them!
- **Stupidity element 3:** The rapid interruption of input so that users doing things end up entering information into the wrong entry item and then removing it so they cannot even tell what they did is dangerous and bad engineering.
- **Stupidity element 4:** Forcing bad AI down our throats when we don't want it. Not that forcing good AI down our throats is a good thing, but to keep trying to trick us into saying yes or automatically saying yes after we said no previously, or making 18 different places and levels that keep changing so we can never actually be sure what you are doing is bad user interface, rude, and bad security engineering.
- **Stupidity element 5:** Blaming the victim is never a good idea. And sending unclear and somewhat threatening emails is an even worse idea. Violating a policy of Google for something typically gets your account shut off or stops services for some period. Stop the services to the bad folks, not the legitimate users, and if you support delegation, then support it, don't threaten those who use it.

Conclusions

I'm sure there is more stupid security in there, but these are so obvious that a high school student in one of our introductory classes could likely spot them. In fact, I am putting it on a flash quiz in office hours before this article hits the Internet, and will likely fail any student who fails to find at least 3 of these.

It's really obvious that anything that uses email may be subject to abuse and tha there are bad actors all over the world who will abuse it if you don't think through how to properly control it by default from first deployment. And if you did think of it and decided to accept the risk, start paying the price for your foolish decision and fix it now.

