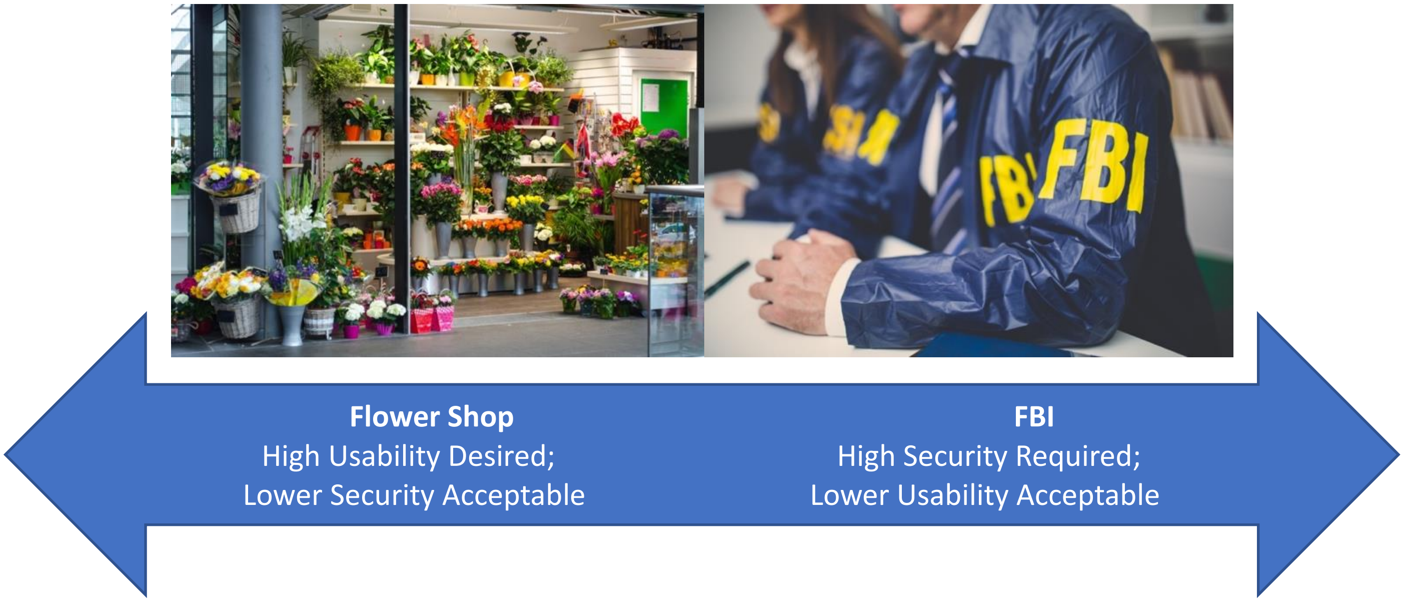
Ripped from the Headlines: Flower Shop or FBI? Your Security Settings in Zoom

DISCLAIMER: This is not an endorsement of any product or platform.

Zoom has experienced unprecedented growth in the past three months; in the first three months of 2020, Zoom added more users than in all of 2019.[1] Undoubtedly, this growth is suddenly testing Zoom's performance and security boundaries, and new users are thrust into quickly getting up-to-speed on this software.

In considering best practices for Zoom, each organization needs to assess its balance on the Usability-Security spectrum, lovingly known as the "Flower Shop to FBI" spectrum. Zoom's default settings bias toward onboarding users quickly and easily, rather than indexing on security as other platforms choose. If your organization considers itself anything other than "Flower Shop," it becomes important to consider common Zoom settings for security vs. the usability needs of your users.



Flower Shop
High Usability Desired;
Lower Security Acceptable

FBI
High Security Required;
Lower Usability Acceptable

For organizations left of the center on the spectrum toward "Flower Shop," considering the following Zoom settings with a usability-security lens are a good start. These options may have no/minimal impact to usability in many organizations, but are related to some of the recent media articles:

- *Join Before Host:* This feature is one of the ways to make Zoom meetings feel more "real" and live than virtual. It also allows reuse of personal meeting IDs by users who have previously joined a meeting or guess your meeting ID.

- *File Transfer:* If File Transfer isn't heavily used in your organization, turning it off can help avoid it being used for unintended file transfers.
- *Allow Removed Participants to Rejoin:* This ensures that any user who has been removed by the host or a co-host is not able to rejoin. The extra security may be worth any risk of accidental removal.
- *International Calling:* Turning off international calling for any user who doesn't need it regularly is a good way to ensure the feature can't be used in unintended ways.
- *Virtual Background:* The virtual background feature can be a fun addition to meetings, particularly very casual ones, and can be appreciated by users who didn't have a chance to clean up their office prior to the meeting or who are taking the call from a busy location. They are also an optional feature that can be turned off to prevent inappropriate or unwanted pictures from being shared with group members.

If your organization is right of center down the spectrum toward "FBI," you could also consider balancing the following features, depending on their impact to your organization's meeting styles:

- *Password:* Adding a password to meetings provides an additional layer of security that effectively eliminates the possibility of someone joining the meeting unless they were invited or forwarded the invitation. This feature, while useful, can be a barrier to entry for legitimate users at times.
- *Personal Meeting ID:* Use separate meeting IDs for all meetings rather than defaulting to your "personal meeting ID." This makes it less likely that someone who was previously invited to one of your meetings in the past might intentionally or accidentally "Zoom Bomb" your meeting. It can cause inconvenience for users who enter an incorrect Zoom ID through the inconsistency.
- *Mute All:* "Mute participants upon entry" can be set as the default for entrants to a meeting to minimize disruption, and further, participants can be prevented from unmuting themselves. This prevents disruptions during your meeting but can inconvenience users unfamiliar with the platform who struggle to unmute.
- *Chat:* There are a variety of options around chat that can be useful to add security without sacrificing much function depending on your style of meeting. Meeting owners can limit whether participants can message everyone in the meeting, just 1:1 to other participants, or just the host. Owners can also prevent users from saving the chat. If chat is disabled in meeting where participants are also muted, utilizing Nonverbal feedback can be a way to integrate safe user feedback. In some settings, availability of the chat option can be an easy way to share information with/among participants and would be missed by users.
- *Co-hosts:* Co-hosts can be a way to alleviate restrictions for specific users – for example, if you want a handful of users to be able to chat to everyone in the meeting, Co-hosts are able to do so. This is a powerful feature to combine with other restrictions to give permissions to trusted users.

Understanding your users' habits and which features are used regularly is critical to your decision-making in this process. The norms of different organizations and individuals vary – for some, International Calling or File Transfer might be a critical usability need, others may be fully reliant on Personal Meeting IDs or Chat. Being thoughtful about the use of these features in your culture and respectful of the critical or majority needs of the organization to understand the necessary balance for your users.

[1] https://www.cnbc.com/2020/02/26/zoom-has-added-more-users-so-far-this-year-than-in-2019-bernstein.html