CarmenZoom Best Practices
Talking Points for Passwords and Meeting Security

This document will highlight the importance of passwords for CarmenZoom meetings, options for using passwords and resources to help you set up secure meetings.

Why Meeting Passwords?

- **Layer of Protection:** Zoom bombers have been randomly guessing meeting IDs. Adding a password creates another hurdle for hackers to overcome.
- **Personal Information:** Your Zoom meetings may include personal or sensitive information. You should use a password just like you would for your personal smartphone or online bank account.
- **It's Easy:** When creating new meetings in CarmenZoom, passwords are added by default*, making the additional security simple to attain.

How to Use Passwords in CarmenZoom

It is recommended that all Ohio State faculty, staff and students use passwords when using CarmenZoom to help protect our community from unwanted intrusions. While new meetings scheduled through Zoom will require passwords by default*, it is also strongly encouraged that any existing meetings be rescheduled to include a password.

You have a few options for using passwords with CarmenZoom meetings:

Embed in the URL

- By default* when creating a new meeting, CarmenZoom generates long, unique passwords and embeds them within the meeting invite URL.
- Adding an embedded password to the meeting URL makes it even harder for hackers to guess, thus keeping unwanted guests out of your meetings.
- Keeping this default feature on retains the “one-click” nature of Zoom, making it easy for your participants to join.

Send separately to meeting participants

- You can turn off embedded passwords in your user account settings at carmenzoom.osu.edu and then send passwords to participants separately.
• Rather than joining in one click, participants will need to enter the password to join the meeting, making your meetings even more secure.

In combination with Personal Meeting ID
• Ohio State does not recommend using Personal Meeting IDs for scheduled get-togethers, as these are easier for hackers to deduce compared to randomly generated meeting IDs.
• If using a Personal Meeting ID, you should still include a password to which only your participants have access.

Create persistent pop-in rooms
• Instead of using your Personal Meeting ID, you can schedule a recurring meeting with No Fixed Time to create a stable meeting room to use whenever you need it. This way you can take advantage of the auto-generated meeting ID and a unique password to make your recurring discussions more secure.
• This method can be used in combination with GO links to make it easier for participants to remember your meeting room ID.

Creating short links
• If you would prefer a shorter link for participants to join a meeting in one click, create a GO link at go.osu.edu, using the full URL with embedded password.

Sharing Zoom Meetings
Remember, it is recommended that you do NOT share meeting links publicly on websites or through social media. If your Zoom meeting link must be publicly available (a free webinar, an open forum, etc.), you should use one of the methods below to protect your meeting from unwanted visitors:

• Registration: Use Zoom’s registration option for your meeting or webinar. You can customize the fields for your attendees to complete; Zoom will send them the meeting link and password (separate or embedded). Using Zoom’s registration option or your own system will also give you the opportunity to reach out to attendees later for feedback or include them on a newsletter.
• Waiting Room: The Waiting Room is a virtual staging area that stops your guests from joining until you're ready for them. This way you can screen participants and only allow those you are expecting to join.
• **Authentication:** If your meeting will involve only those associated with The Ohio State University (persons with a `name.#@osu.edu` email address), you can select **Only authenticated users can join** in your meeting settings. This setting is turned OFF by default to accommodate our Extension offices and other groups with frequent contact outside Ohio State.

**Resetting Defaults**

If you have modified your default settings to turn off the password requirement or make other adjustments, there is an easy way to reset those settings. Resetting to Ohio State’s carefully chosen defaults is the easiest way to secure your meetings and classes.

1. Navigate to carmenzoom.osu.edu and log in to your account.
2. Select **Settings** from the side menu.
3. Scroll through your settings to find those you have changed, designated by the word **Modified** on the right-hand side.
4. Next to the word **Modified**, you will see a **Reset** link. Click **Reset** on those settings that you have modified.

**Resources**

• **ODEE Resource Center** – here you will find articles, videos, FAQs and known issues for Ohio State’s eLearning tools, including CarmenZoom
  o **Zoom Meeting Security** – this article reiterates the best practices above and provides more details on other security measures, such as waiting rooms and authenticated user settings.
• **Cybersecurity 4 You** – this platform provides education opportunities around security best practices, including use of Zoom at Ohio State
• **go.osu.edu** – use this tool to create short, custom links

*Users who have modified their default settings may have a different experience.*