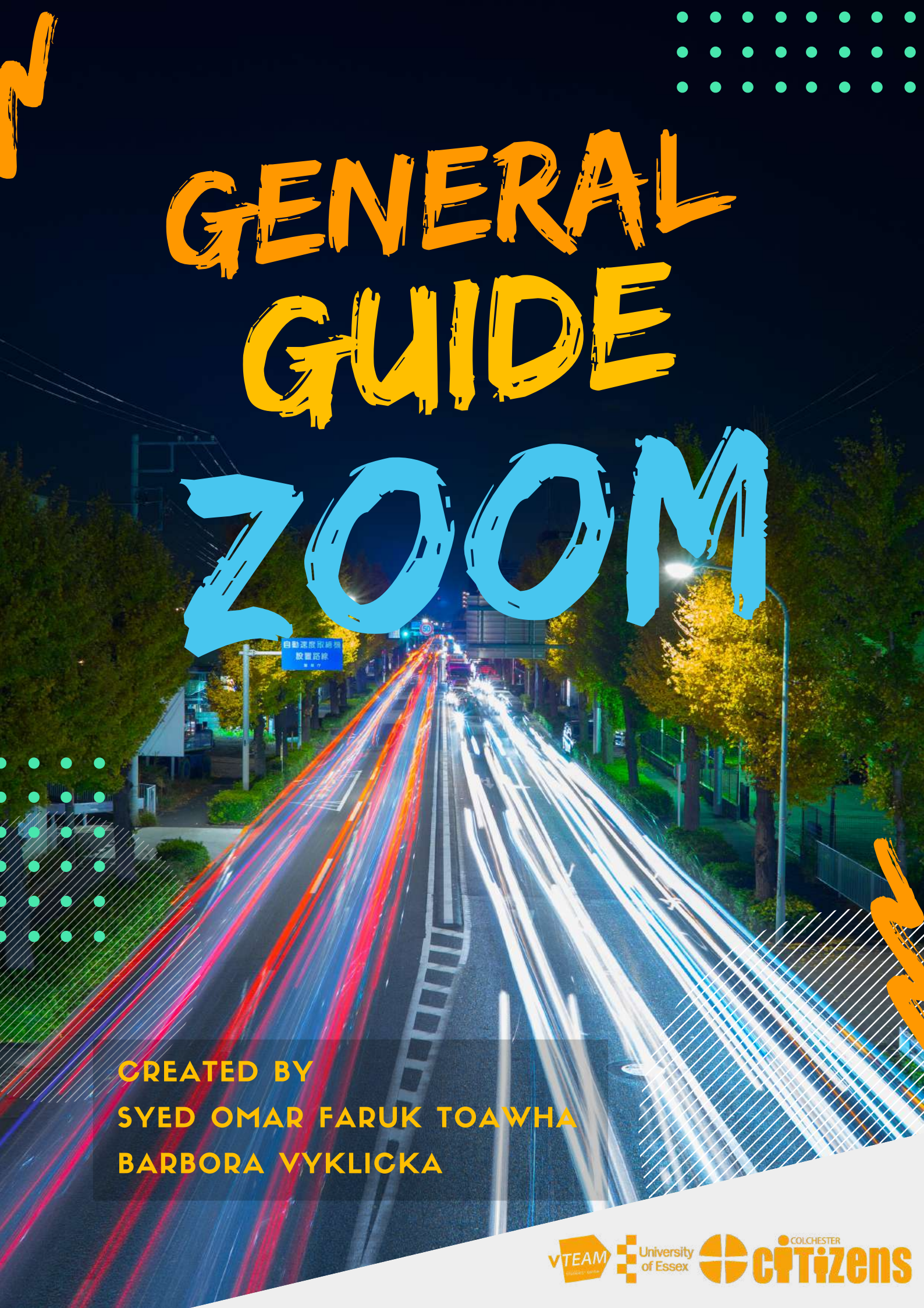
GENERAL GUIDE ZOOM



CREATED BY
SYED OMAR FARUK TOAWHA
BARBORA VYKLICKA

vTEAM
University of Essex
COLCHESTER citizens


KEEP
YOURSELF
SAFE WHILE
USING ZOOM

Zoom Safety

Zoom Meeting URL Security

Never open a Zoom meeting URL/link from an unknown person!

Always double check for https on your meeting URL!

If you get the Zoom meeting URL with an URL shortener, open it in a private window of your browser.

URL Shortener hack

You can expand the shortened URL. Open the shortened URL with the following process to reveal the original URL and see if anything is suspicious with that URL.

If it is *Bit.ly*, add **+** after the URL

e.g: https://bit.ly/essex
to
https://bit.ly/essex+

If it is *TinyURL*, add ***preview*** before the URL

e.g: https://tinyurl.com/essex
to
https://preview.tinyurl.com/essex

If it is *Goo.gl*, add **+** after the URL

e.g: https://goo.gl/essex
to
https://goo.gl/essex+

If it is I*s.gd*, add - after the URL
e.g: https://is.gd/essex
to
https://is.gd/essex-

Zoom Screen Sharing Security

Check your privacy before sharing your screen on a meeting. Always double check if there is any personal item on the screen.

A few tips while sharing screen.

- Do not share your screen unprepared
- Disable email notifications, calendar alerts or chat windows
- Don't have a messy desktop with lots of icons and files here and there
- Close any social network site opened on any of your browser tab
- Disable update/upgrade messages
- Mute your PC unless sharing the PC's sound.
- Always check if you are sharing the screen with the right person you intend to share.
- Always make a new space before sharing a screen. For example, create a new folder and new desktop so that no personal item is there.
- Disable pop ups of your browser.
- Check if YouTube or Spotify or some other audio services are running in the background.
- Choose a formal wallpaper of your desktop.
- Hide the software icons from your desktop so that the viewers do not get the idea of what kind of software you use on your computer.

Zoom Meeting Privacy

Always password protect your meetings:

The simplest way to prevent unwanted attendees and hijacking is to set a password/passcode for your meeting.

Passwords/passcode can be set at the individual meeting, user, group, or account level for all sessions.

In order to do so, first sign in with your account at the Zoom web portal. If you want to set up a password at the individual meeting level, head straight over to the "Settings" tab and enable "Require a password when scheduling new meetings", which will ensure a password will be generated when a meeting is scheduled.

All participants require the password to join the meeting. Subscription holders can also choose to go into "Group Management" to require that everyone follows the same password practices.

Authenticate users:

When creating a new event, you should choose to only allow signed-in users to participate.

Stop participants joining before the host:

Do not allow others to join a meeting before you, as the host, have arrived. You can enforce this setting for a group under "Account Settings."

When someone is waiting the host receives an email saying people are waiting to join if they eneter the meeting prior to the host

Lock your meetings:

Once a session has begun, head over to the "Manage Participants" tab, click "More," and choose to "lock" your meeting as soon as every expected participant has arrived. This will prevent others from joining even if meeting IDs or access details have been leaked.

Turn off the participant screen sharings:

No-one wants to see pornographic material shared by a Zoom bomber, and so disabling the ability for meeting attendees to share their screens is worthwhile. This option can be accessed from the new "Security" tab in active sessions.

Use randomly generated meeting IDs:

You should not use your personal meeting ID if possible, as this could pave the way for pranksters or attackers that know it to disrupt online sessions. Instead, choose a randomly generated ID for meetings when creating a new event. In addition, you should not share your personal ID publicly.

Use Meeting Waiting Room feature:

The Waiting Room feature is a way to screen participants before they are allowed to enter a meeting. While legitimately useful for purposes including interviews or virtual office hours, this also gives hosts greater control over session security.

Avoid file sharing on Zoom:

Be careful with the file-sharing feature of meetings, especially if users that you don't recognize are sending content across, as it may be malicious. Instead, share material using a trusted service such as Box or Google Drive. At the time of writing, Zoom has disabled this feature anyway due to a "potential security vulnerability."

Remove unknown users:

If you find that someone is disrupting a meeting, you can kick them out under the "Participants" tab. Hover over the name, click "More," and remove them. You can also make sure they cannot rejoin by disabling "Allow Removed Participants to Rejoin" under the "Settings: Meetings - Basic" tab.

Install Authentic Zoom Software:

Never install the Zoom software from an unknown source, always make sure you download it from https://zoom.us


THANK
YOU