Zoom-bombing Prevention

What is Zoom-bombing?

With the increase use of virtual meetings, we have also seen a rise of cyber-attacks on our virtual meeting spaces. Cyber-attackers are causing mayhem and confusion by randomly joining and taking control of these virtual workspaces.

This new cyber-attack type is commonly referred to as Zoom-bombing. In these instances, cyber-attackers have joined Zoom meetings by several different methods, with the following being some of the most common ways:

- Performing random meeting searches and joining
- Finding a meeting link publicly posted and joining
- By identifying a personal meeting ID and joining

What can be done?

The following tips can help protect your virtual meetings and keep them private:

- Change the screensharing options to “Host Only.”
- Make all of your Zoom meetings private by either requiring a password to join or by using the “Waiting Room” feature and control the entry of attendees yourself.
- Do not share links to your Zoom meeting on social media posts. Instead, send the link directly to those who need it.
- Use the latest version of Zoom. Zoom has continuously made updates addressing cybersecurity concerns, including adding passwords by default for meetings.
- Go through Zoom’s settings and configuration options

Final Thoughts

With the use of “new to you” technologies, it is always important to walk through the settings and configuration options. This allows you to customize the security of your meetings, regardless of the platform being used. Although the above steps are focused on Zoom and Zoom-bombing, the most popular virtual meeting platforms will offer similar ways to keep your virtual meetings private and secure.

Small Business, Big Threat is a program of the Michigan SBDC, developed with support from the Michigan Economic Development Corporation and the U.S. Small Business Administration.