

# A Zoom Security Checklist for Creating Your Exclusive Party

**Widespread remote-working relies heavily on online meeting platforms, like Zoom™. Use these tips to reduce your risks of Zoom meeting compromises by malicious intruders.**



## Secure the Door

Use “Generate Meeting ID Automatically” when scheduling a Zoom meeting. Don’t use your Personal Meeting ID, which can easily be compromised.



## Hire a Bouncer

Activate the “Enable waiting room” setting, which allows the host to admit to participants.



## VIPs Only

Require a password to join. Paid accounts should enable the “Only authenticated users can join” setting to allow only approved users who are logged into Zoom.



## Don't Start Without the Host

Deselect “Enable join before host” to prevent the meeting from starting before the host arrives.



## Shut Down Crashers

Restrict screen sharing to be a host-only privilege. Use “Advanced Sharing Options” once the meeting is in progress to lift the restriction.



## Check IDs

At the start of the meeting, verify attendees using the participants list.



## Keep it Tight

Never publicly post a Zoom meeting link.



## Avoid a Hangover

Evaluate the platform’s security regularly based on the sensitivity of the content you share and any disclosed vulnerabilities.