Zoombombing is when a malicious individual finds an open Zoom meeting link and enters the meeting to disrupt it verbally or by sharing inappropriate material. Below are simple actions you can take to protect your meetings.

Top four recommendations for securing your meetings against zoombombing:

1.Don’t publish your Zoom meeting ID or URL publicly

2.Add a passcode to your meetings

3.Set your meetings to only allow authenticated users (assuming you have no guests who are external to Haartz)

4.Set a waiting room for your meetings

Cisco Anyconnect VPN:

A couple of recommendations on VPN use:

- Please disconnect your VPN connection when you are not accessing network resources.
- When on the internet please use for the exclusive purpose of performing job responsibilities.
- Use of resources provided by the organization for personal activities, including social media and media streaming, is discouraged.

Symantec Endpoint Protection:

We would like ask that once a week you check to make sure that your SEP client is up to date and free of issues.

Double click on the SEP shield  in the lower-right hand corner of your screen.

This screen will show if there are any issues, if there are problems or dates are 5 days out of sync, please send a email to hardware@haartz.com we will assist you immediately.