CYBER SAFETY ALERT

Remote On-Line Meeting Platform Compromises

To practice social distancing, many schools, law enforcement agencies, religious groups and other organizations, are increasingly using online meeting platforms. There have been reports of sessions being interrupted by actors who shout profanity, racial and religious slurs, and in some cases display disturbing and offensive images. Alternatively, unwelcomed participants may remain quiet and gather sensitive information.

Simple Steps to Keep Malicious Intruders Out of Your Meetings

Use Available Security Settings

Many platforms have settings that will help prevent intrusion. Use the latest versions and all available security settings to limit unwanted participants.

Develop Organizational Policies

Develop policies designed to prevent these incidents and educate your organization membership of what is expected of them.

Use Encrypted Platforms

Consider paying for robustly encrypted platforms or "paid" versions offering more security features.

Do not Publicly Post Meeting Links

Use emails to known individuals to share links to meetings – ask others not to share outside of the group.

Use Unique Meeting IDs

Use newly generated meeting IDs for all meetings. Do not reuse personal meeting IDs. Replace your personal ID if you believe it was compromised.

Require Passwords

Require a password from all participants for every meeting. If you have a paid account, lock the meetings down to "authenticated users" only.

Enable your Waiting Room

Use settings requiring the host to admit the participants.

Host Should Start the Meeting

Eliminate participants' access to the meeting before the "host".

Verify Attendees

At the start of the meeting verify all attendees are valid. Block others once the meeting starts.

Restrict Sharing by Participants

Restrict screen sharing to verified participants. Use host controlled mute buttons and limit chat and question capabilities.

Office of the Attorney General
www.nj.gov/oag