Jun 18, 2020

Contact Kylie Mason

Phone 850-245-0150

OFFICE OF THE ATTORNEY GENERAL STATE OF FLORIDA

Florida Attorney General's Office News Release

AG Moody Asks Floridians to Report Zoombombing to Law Enforcement



TALLAHASSEE, Fla.—Attorney General Ashley Moody is working with Florida sheriffs, police chiefs and university police to stop child porn Zoombombing. Zoombombing occurs when hackers hijack internet video conferences, like those offered by the fast-growing platform Zoom. These hackers often present inappropriate, offensive material or otherwise disrupt video conferences. Recent reports indicate that hackers are crashing online meetings with child pornography. After learning of this criminal activity, Attorney General Moody began working with local law enforcement to thwart the offensive conduct and ensure local, state and federal law enforcement are coordinated in their efforts.

Attorney General Ashley Moody said, “It’s heartbreaking that anyone would exploit children in this manner, but child pornography is pervasive online. It’s disgusting and illegal. When hackers hijack meetings and force participants to view these disturbing images, we must ensure we have an immediate, aggressive and coordinated law enforcement response. That is why I am working with our great law enforcement agencies to track down Zoombombers and hold them accountable for the victimization of our children.”

Anyone experiencing Zoombombing with illegal images, or receiving child pornography by other means, should immediately report the crime to local law enforcement. To report child abuse, Floridians can also call the state child abuse hotline at 1(800) 962-2873.

Earlier this year, Attorney General Moody issued a Consumer Alert to inform Floridians about

steps they can take to prevent online meetings being hijacked. To increase privacy and guard against Zoombombing:

- Create separate passwords for each virtual meeting;
- Establish a Zoom waiting room for meeting participants;
- Lock down the meeting once everyone invited to attend has joined; and
- Do not publicly post meeting links on social media or any other public forum.

Zoom also offers privacy settings to provide hosts an additional layer of protection. To enable these extra security features, hosts should click on the settings menu, scroll to Screen Sharing, find Who Can Share? then click on Host Only. Finally, the user should save the changes.

After saving the new preferences, subsequent meetings should enable these enhanced privacy features by default. For more virtual meeting security tips, click here.

To view the Zoombombing Consumer Alert and other warnings, click here.