Department of Justice

United States Attorney Scott W. Brady
Western District of Pennsylvania

FOR IMMEDIATE RELEASE
APRIL 7, 2020
WWW.JUSTICE.GOV/USAO/PAW

U.S. Attorney Scott Brady and Pennsylvania Attorney General Josh Shapiro Warn Against Zoom-Bombing and Hacking Teleconferences During Coronavirus Pandemic

PITTSBURGH - Scott W. Brady, United States Attorney for the Western District of Pennsylvania, and Pennsylvania Attorney General Josh Shapiro today warned against hacking teleconferences during the coronavirus pandemic. The Western Pennsylvania COVID-19 Task Force will investigate, disrupt and prosecute such hacking.

Many Pennsylvania residents have turned to video-teleconferencing platforms, such as Zoom, to stay connected during the COVID-19 pandemic. Unfortunately, as the FBI has reported, there has been a rise in so-called "Zoom-bombing," or video hacking across the United States, where uninvited hackers disrupt conferences and online classrooms with pornographic images, hate images and/or threatening language. These attacks have also targeted religious communities, minority groups, and vulnerable populations, such as Alcoholics Anonymous meetings. Some hackers have planned coordinated attacks through websites and social media, including Discord and Instagram, in violation of the terms of use. Pennsylvanians have seen several instances of such hacking within the past week.

Western Pennsylvania's chief federal, state, and local law enforcement officials are joining together to warn that anyone who hacks into a teleconference can be charged with state or federal crimes. Charges may include: disrupting a public meeting, computer intrusion, using a computer to commit a crime, hate crimes, fraud, or transmitting threatening communications. When hackers work together on coordinated attacks, they can also be charged with conspiracy. All of these charges are punishable by fines and imprisonment.

U.S. Attorney Brady said, "Hackers are disrupting business and community meetings for sport and targeting specific groups, including addiction recovery meetings, in order to mock, harass and interfere with treatment. This is another low point in this crisis. We are better than this. DOJ will use all of our resources to find, expose and prosecute these low-lifes."

"At a time when people need internet conferencing technology to do essential business or to connect with loved ones, it's vital that we make these platforms safe from hackers," Attorney General Josh Shapiro said. "People need confidence in the services they are relying upon during

this emergency. Through my Office's partnership with the Western Pennsylvania COVID-19 Fraud Task Force, we will be able to investigate and prosecute hackers."

"The COVID-19 pandemic has led to a spike in businesses and employees teleworking to communicate and share information over the internet," said Acting FBI Pittsburgh Special Agent in Charge Eugene Kowel. "Cyber criminals see this as an easy way to take advantage of vulnerable members of our community and to exploit telework software vulnerabilities to obtain sensitive information. The FBI encourages users to safeguard their user information and prevent these malicious cyber actors from eavesdropping or stealing sensitive information. We ask anyone with information about criminal activities, especially those exploiting the disruptions caused by the Coronavirus, to contact us."

"Over the course of the next several weeks, the United States Secret Service's primary investigative priorities will be to mitigate any efforts by criminals that target citizens for cyber-enabled crimes and identity theft as it relates to COVID-19 scams," said Tim Burke, Special Agent in Charge, United States Secret Service Pittsburgh Field Office. "In doing so, we at the Secret Service are grateful to be joining our fellow law enforcement partners on the COVID-19 Fraud Task Force. Together, the COVID-19 Task Force will enable us to focus our resources to uncover, investigate, and prevent these crimes more effectively in a unified front."

"Every community and their leadership are appreciative of the efforts that all of the Federal agencies are putting forth in addressing the issues of Zoom-bombing," added Bruce A. Fromlak, West View Borough Chief of Police and President of the Western Pennsylvania Chiefs of Police Association. "As we conduct business each and every day we are presented with new challenges. This is clearly a new challenge however this too will be dealt with in cooperation with all of our law enforcement partners and professional law enforcement organizations. We will approach and address all malicious attacks in an expeditious and professional manner in order to bring any and all unscrupulous individuals to justice."

As individuals continue the transition to online lessons and meetings, law enforcement recommends exercising due diligence and caution in your cybersecurity efforts. The following steps can be taken to mitigate teleconferencing threats:

- Do not make the meeting or classroom public. In Zoom, there are two options to make a meeting private: require a meeting password or use the waiting room feature and control which guests are admitted.

- Do not share a link to a teleconference or classroom on an unrestricted publicly available social media post. Provide the link directly to specific people.

- Manage screen sharing options. In Zoom, change screen sharing to "Host Only."

- Ensure users are using the updated version of remote access/meeting applications. In January 2020, Zoom updated their software. In their security update, the teleconference software provider added passwords by default for meetings and disabled the ability to randomly scan for meetings to join.

- Understand the features of your specific teleconference platform, including how to close a conference call in the middle and how to kick out people who are disrupting. Zoom has posted these steps on their blog.

- Lastly, ensure that your organization's telework policy or guide addresses requirements for physical and information security.

If you were a victim of a teleconference hijacking, or any cyber-crime for that matter, report it to the FBI's Internet Crime Complaint Center at https://www.ic3.gov/default.aspx. Click here for more information regarding teleconference hijacking: https://www.ic3.gov/media/2020/200401.aspx.

Additionally, if you receive a specific threat during a teleconference, please report it to the FBI at https://tips.fbi.gov/ or call the FBI Pittsburgh Division at (412) 432-4000.

To contact Secret Service directly call (412) 281-7825.

If you believe you have been a target or victim of any COVID-19-related frauds, please report them the Western Pennsylvania COVID-19 Fraud Task Force's Toll Free Hotline: 1-888-C19-WDPA or 1-888-219-9372, or email the Task Force at usapaw.covid19@usdoj.gov or the Pennsylvania Attorney General at scams@attorneygeneral.gov.

###