BRIAN E. FROSH
ATTORNEY GENERAL

MEDIA CONTACTS:
PRESS@OAG.STATE.MD.US
410-576-7009

# PRESS RELEASE

## Consumer Alert: Increasing Reports of Extortion Scams

**BALTIMORE, MD (December 17, 2018)** – Maryland Attorney General Brian E. Frosh is warning consumers of an increase in reports of extortion scams, in which thieves are using email to threaten victims into paying a ransom to prevent certain personal information from being circulated online.

In this world of greater and greater connectivity, scammers are preying on fears that our safety, security, and privacy are at risk inside our own homes. In what is being called the "Internet of Things," many of our devices, including webcams, watches, smart TVs, smartphones, and even home utilities are connected to each other and to the Internet.

It's true that this connectivity makes those devices at risk for hacking and violations of privacy when it comes to what data the devices are collecting and storing. However, the chances that these devices are being used to secretly "spy" on your activities within your home are slim. Scammers are using this unfounded fear to try and extort money from individuals, usually through an email, by threatening to release "embarrassing" videos or photos to the victim's email contacts. Let's cut to the chase: this is a scam.

One of the tricks these scammers use is to tell you they have your password for a certain account, and then reveal the password in the email. You may have noticed that this is, in fact, a password that you use or have used in the past. Usually, the scammers have accessed these passwords by breaking into large corporate databases, and almost certainly have not actually accessed your email or other private accounts.

Under no circumstances should you pay any money, whether through wire transfer, online payment application, gift card, or Bitcoin, to any person or group that claims to have embarrassing videos, audio tapes, or photos of you or your family. If you do receive an email that tries to extort you in this way, follow these steps:

1. Change your email password immediately, and do not use a password that you have used previously.
2. Do not click on any links in the email; instead, just delete it.
3. If you have the option, block that sender from sending you further emails.
4. If you are worried about being seen through your webcam (although highly unlikely), do what the information technology professionals have been doing for years: put a piece of black tape over the camera and only take it off when you need to use the camera.

“If you get a threatening email like this, delete it,” said Attorney General Frosh. “It’s a numbers game for these thieves; only one person has to fall for it for the scammer to make thousands of dollars. Don’t fall for it; it’s a scam, plain and simple.”

This scam is hitting email users worldwide. If you have been a victim and paid a ransom to one of these crooks, please report the theft to your local police. You are definitely NOT the only victim, and by reporting your experience, you can help put these criminals out of business.