



## PRESS RELEASE

---

### **AG Frosh Warns Consumers about Scam Spoofing OAG Email** *Phony email claims businesses must respond to OAG in response to complaints filed against them*

**Baltimore, MD (June 22, 2016)** -- In his ongoing effort to protect consumers, Attorney General Brian E. Frosh is alerting Marylanders about scammers' latest efforts to hack into consumers' personal computers to steal personal identifying information that can then be used for illicit purposes.

The scammers use an email address that looks like it might be from the Office of Attorney General, with a subject line: "The Office of Attorney General Complaint." The email then contains a note that claims a complaint has been filed against the consumers' business and they must click on a link that allegedly sends them to a PDF document in order for them to file a response, but actually sends them to a link with a zip file that installs malware. This practice is known as click-bait.

"This scam is particularly deceitful and hits too close to home as our office would never send complaints by email," said Attorney General Frosh. "It's always a good rule of thumb never to open emails that claim to be from an official government agency, if the email address does not end in .gov or .us. Consumers should always be vigilant with personal information so it doesn't fall into the wrong hands."

Marylanders who receive an unsolicited email from any individual or business should exercise caution and should not click on links or provide any personal information unless the email sender is known and reputable. Consumers should delete emails received from unknown parties.

Consumers with questions about how to handle such inquiries or those who think they have been the victim of a scam should contact the Consumer Protection Division at 410-528-8662 or toll free at 888-742-0023. Consumers can file a complaint at [here](#) or by mailing a hard copy of the complaint form found online, along with any supporting documents, to 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

For more information on email scams and hoaxes, consumers may find additional helpful information by visiting the following websites:

- Internet ScamBusters: [www.scambusters.org](http://www.scambusters.org)
- Federal Trade Commission: [www.ftc.gov](http://www.ftc.gov)
- U.S. Securities and Exchange Commission: [www.sec.gov/investor/pubs/cyberfraud.htm](http://www.sec.gov/investor/pubs/cyberfraud.htm)

A sample of what to watch out for in scam letters is [here](#).