



Virginia Freedom of Information Advisory Council

Phishing Study Subcommittee

August 21, 2019, at 10:00 a.m.

Pocahontas Building, House Committee Room 400A

foiacouncil.dls.virginia.gov

The Phishing Study Subcommittee (the Subcommittee) of the Virginia Freedom of Information Advisory Council (the Council) met in Richmond.¹ The meeting began with introductions and opening remarks followed by presentations and discussion. Materials presented at the meeting are accessible through the [Council's subcommittee meetings webpage](#).

Presentation and Public Comment: 2019 House Joint Resolution 628 (Heretick)

First Sergeant Mitchell Smith, Virginia State Police

Joshua Heslinga, Legal Compliance Manager, and Michael Watson, Chief Information Security Officer, Virginia Information Technologies Agency

First Sergeant Mitchell Smith from the Virginia State Police (VSP) presented background information on phishing and how it affects different agencies. He noted that the number one issue in regard to phishing scams comes in the form of direct deposit scams where a bad actor utilizes email to try to gain access to someone's bank account or communicates with Human Resources from a spoofed email address pretending to be an employee with the purpose of getting the employee's paycheck deposited in a different account—that of the bad actor.

Sterling Rives referenced a recent article in the *New York Times* regarding the dangers of releasing cell phone numbers and asked if there are similar threats on a state level in Virginia. Sergeant Smith noted that any amount of information that is released can lead to someone being able to access additional information that can then be used for nefarious purposes. Mark Vucci asked if the intended victims of phishing scams are those with “deep pockets,” such as an agency or agency director, or if the intended victims are lower level employees. Sergeant Smith said that both are at risk of attack, especially since it's so easy to get agency information online. Dr. Sandra Treadway asked what type of advice, if any, does the VSP provide in regard to prevention measures. Sergeant Smith noted that the VSP works with the Virginia Fusion Center (the Center). Agencies can sign up to work with the Center, which gives advice on how to better protect agency information from cyber attacks. The Center also provides training for state agencies and employees. Sergeant Smith also noted that any agency that signs up to work with the Center is protected by a nondisclosure agreement, which serves to protect specific information relative to any cyber security attacks that an agency may have experienced and is seeking help with investigating.

Joshua Heslinga, the Legal Compliance Manager at the Virginia Information Technologies Agency (VITA), gave an overview of phishing as well as how VITA responds to such attacks. Mr. Heslinga noted that VITA's best practices when it comes to security standards include

¹ **Members Present:** Sandra Treadway (Chair), Shawri King-Casey, Sterling Rives, III, Mark Vucci
Members Absent: Lee Bujakowski

mandatory security training, periodic phishing tests, and working with IT vendors to procure security services.

Michael Watson, the Chief Information Security Officer for VITA, noted that VITA works similarly to the Virginia Fusion Center. Shawri King-Casey asked for Mr. Watson to explain what “doxing” is. He explained that doxing is when people search for and post online as much personal information about a person as possible, often for nefarious reasons. He noted that “swatting” is typically a response that escalates from doxing (once someone’s personal information is online). Swatting is when someone calls the police or SWAT units to another person’s address after reporting a fake crime or incident. Dr. Treadway asked why VITA has never recommended that state agencies not make public employee names or email addresses. Mr. Watson explained that VITA only gives recommendations that are in step with current law so as not to violate FOIA and other relevant laws.

During the period for public comment, Solomon Ashby, Portsmouth City Attorney, emphasized the severity of the issue and pointed to an article from National Public Radio regarding 22 Texas towns that were hit by a ransomware attack. He noted that there is a tension between FOIA and cyber security measures and that the law must adapt with technology. Michelle Gowdy from the Virginia Municipal League agreed with Mr. Solomon’s sentiments. Megan Rhyne from the Virginia Coalition for Open Government noted that information used by bad actors is already “out there” and it is not being released solely through FOIA requests. She suggested that the response to the issue should be to increase security measures instead of making changes to FOIA because the current proposals² offered by Delegate Heretick and the City of Portsmouth quell the public’s access to information without addressing the root issue. Mark Hickman from the Virginia Press Association agreed with the comments made by Ms. Rhyne. Mr. Hickman also noted that reporters submit FOIA requests all the time, which is an integral part of freedom of the press and open government as a whole. He also mentioned that anything that impedes open government should be limited. Daniel Jones, the Chief Information Officer for the City of Portsmouth, explained that even though information is widely available through the public domain, a FOIA request that asks for certain information about an employee would essentially require a public body to compile and produce information, all the while doing the “leg work” for a bad actor who intends to use that information as an attack vector. Sherri Neil, Manager of Intergovernmental Affairs for the City of Portsmouth, noted that the recommendations offered by Delegate Heretick were only meant to start the conversation. She also explained that FOIA isn’t the only issue but is definitely part of the issue, and urged the Subcommittee to take a closer look at the possibility of adding language for an opt-out provision in FOIA, which would allow citizens to opt out of having their information disclosed under FOIA.

Mr. Vucci asked if there was an organization or agency like VITA, but for localities. Mr. Rives explained that there is no official organization, but information technology staff personnel for the different localities belong to statewide organizations that offer solutions. Mr. Watson also noted that VITA keeps in contact with IT staff for localities and that there is a nationwide organization called ISAC (Information Sharing and Analysis Center).

After further discussion of the issue, the Subcommittee decided that more time was needed to gather information and look at the proposals set forth by Delegate Heretick. Mr. Rives gave his views on the comments provided by the Virginia Coalition for Open Government. Mrs. King-

² http://foiacouncil.dls.virginia.gov/subcom_mtgs/2019/hjr628.pdf



Casey noted that sometimes people volunteer extremely personal information in order to obtain help or certain services from public agencies, and citizens are not always aware of how their information can be used within the context of FOIA. The Subcommittee decided that they were not prepared to give a recommendation to the full Council and that they will schedule further meetings to discuss the three main issues outlined by VCOG as well as Delegate Heretick's proposals. The Subcommittee agreed to provide the Speaker of the House with an update as requested in his letter, and to recommend that the full Council ask the Speaker for another year to further study this issue.

Presentation and Public Comment: FOIA Charges – Tolling Issue

Council Staff

Staff gave an overview of the issue regarding FOIA charge estimates and tolling and presented two draft bills. One draft (LD 20100265) contains language that mimics the advanced deposit language in subsection H of § 2.2-3704, but changes “advanced deposit” to “cost estimate.” The other draft (LD 20100269) incorporates a fifth response in subsection B of § 2.2-3704, which would give a public body five days to provide an estimate to a requester who requests an estimate and give the public body an additional five days to respond after the requester agrees to the estimate of the charges.

After some discussion, the Subcommittee agreed that LD 20100265 was the preferred bill. Mr. Vucci asked what would happen if a public body does not hear back from a requester within a certain amount of time. He also inquired whether the language in the bill should be more explicit to address such a scenario.

During the period for public comment, it was expressed that more clarity in the language of the bill is needed. Mr. Heslinga (VITA) noted that, in regard to stale requests, the Public Records Act prevents a public body from destroying a record if there is an outstanding FOIA request. Staff was instructed to prepare alternative drafts for the next Subcommittee meeting that would set an explicit time limit for responding to an estimate.

Next Meeting

The next meeting of the Subcommittee will be posted on the [Council's website](#) as soon as it is scheduled.

For more information, see the [Council's website](#) or contact the Division of Legislative Services staff:

Alan Gernhardt, Executive Director, Virginia Freedom of Information Advisory Council, DLS
agernhardt@dls.virginia.gov
804-698-1877

Ashley Binns, Attorney, Virginia Freedom of Information Advisory Council, DLS
abinns@dls.virginia.gov
804-698-1812

