VIRGINIA COALITION
FOR OPEN GOVERNMENT

To: The FOIA Council Subcommittee on Phishing
Re: Comments on the proposals offered as a starting point for conversations
Date: Monday, August 5, 2019

Dear Subcommittee Members:

What follows is a detailed response from the Virginia Coalition for Open Government to the problem of phishing that has been defined by the patron of HJR 628, Del. Steve Heretick, and the City of Portsmouth.

The proposals offered to combat the problem would be harmful to public access, with no offsetting security benefit. There is no reason to believe that any connection exists between phishing and requests for public records. The proposed changes would throttle back on public access to government information without solving any phishing problem.

More effective solutions to the problem would include improved security of computer systems and employee training.

At the request of subcommittee member Rives, VCOG also offers discussion about the public value of access to contact information for citizens, the non-work accounts of government employees/officials, and the government-issued accounts of government employees/officials.

Here, VCOG notes that all contact information has public value. Contact information can say something about who is influencing government or asking government to intervene, as well as who is carrying out public business outside official channels of communication.

Thank you for your time and attention to this issue. I am happy to discuss the proposals and VCOG's response to them in advance of the Aug. 21 subcommittee meeting.

Most truly yours,

Megan Rhyne, Executive Director

Virginia Coalition for Open Government
P.O. Box 2576, Williamsburg VA 23187
P 540-353-VCOG
mrhyne@opengovva.org

The problem: phishing, spoofing, whaling

As defined by Merriam-Webster, online, **phishing** is "a scam by which an Internet user is duped (as by a deceptive email message) into revealing personal or confidential information which the scammer can use illicitly."

A typical scenario would be for a bad actor to send an email to a target that looks like it is being sent by someone the target knows or engages with (this is called **spoofing**), for instance a co-worker, boss, friend, family member or company the target does business with. The message might say there is a problem with the target's account — financial or otherwise — and to click on the provided link in order to fix it. Because the message appears to be from a trusted source, targets may click the link and be directed to a site that has been made to look like an official business or organization. Once on this site, the target is asked to enter sensitive personal information, e.g., Social Security number, credit card numbers, other financial account numbers, dates of birth, passwords, user names, answers to security questions, etc. The bad actor uses the ill-gotten information to usurp the target's identity and/or compromise the target's accounts to steal money.

Sometimes the target is someone high up in an organization and is asked by the bad actor to reveal sensitive information about the organization. This practice is called **whaling**.

Phishing, spoofing and whaling are crimes in Virginia under § 18.2-152.5:1.

> A. It is unlawful for any person, other than a law-enforcement officer, as defined in § 9.1-101, and acting in the performance of his official duties, to use a computer to obtain, access, or record, through the use of material artifice, trickery or deception, any identifying information, as defined in clauses (iii) through (xiii) of subsection C of § 18.2-186.3. Any person who violates this section is guilty of a Class 6 felony.
>
> B. Any person who violates this section and sells or distributes such information to another is guilty of a Class 5 felony.
>
> C. Any person who violates this section and uses such information in the commission of another crime is guilty of a Class 5 felony.

Portsmouth's experience

At the first meeting of the FOIA Council Subcommittee on Phishing, July 15, 2019, the City of Portsmouth explained that city employees have been phished by bad actors pretending to be the employees' supervisor (e.g., the fire chief) or other city employees, (e.g., a human resources manager.)[1]

Though some employees were said to have clicked on these messages, the city did not describe harm that any employee suffered, only that "a number of different actions" were taken.

---

1 An audio recording of the city's presentations is available on VCOG's shared Google Drive: https://drive.google.com/file/d/1Qy6DTSuLSQ2lPXeABKPozZLte6zZb1c-/view?usp=sharing

Officials from the city testified that the source of the fake fire chief's email could be traced to Virginia Beach and perhaps to Texas.

Alluding to the constant barrage of attempts to infiltrate the city's servers (100 times in a week), the city also expressed concern that a **ransomware attack**[2] could be unleashed upon the city's servers, as happened in Atlanta, Baltimore and Lake City, Florida.

Though acknowledging that troves of personally identifiable information is available on the so-called **Dark Web**,[3] the city concluded that public records that are required to be disclosed under the Freedom of Information Act present the primary threat. Specifically, the city identified two types of records:

1. Salary data, which must include name, title and rate of pay[4]; and
2. Employee email addresses and phone numbers.[5]

The city also expressed concern that the contact information citizens share with the city may be accessed through FOIA, presumably making them targets for phishing attacks, too.

The city's proposals

To encourage the further discussion of the problem of phishing, the city offered five proposals.

1. Require FOIA requesters to provide a state ID when requesting employment data (defined as name, title, salary, email, telephone) for more than five employees in a single request or in the aggregate;
2. Allow government to require written requests for information with an accompanying state ID if the request is made electronically;
3. Explicitly exempt government from liability should it provide requester information to law enforcement agencies;
4. Allow government to provide "opt-out" agreements to protect citizens' personal identifiable information from all FOIA requests; and
5. Commit to conducting a broad study to arrive at other recommendations and actions.

---

[2] Ransomware: "A type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website." *Source: Department of Homeland Security's Cyber-Infrastructure Agency,* https://www.us-cert.gov/Ransomware.

[3] The Dark Web is a connection of networks that relies on the Internet but that requires special software, configurations or authorization to access. The Dark Web allows users to share files confidentiality, including the trafficking in illegal goods or services, as well as data used in phishing and other scams. Source: Wikipedia, "Dark Web," (https://en.wikipedia.org/wiki/Dark_web). Last accessed July 25, 2019.

[4] Section 2.2-3705.1(1).

[5] Though there are several specific instances when employee contact information may be withheld under FOIA, there is no catch-all exemption for that data.

Proposal 1: State ID for employment data requests

Requiring all requesters to present a state ID, not just a name and address, poses several problems:

1. FOIA already allows name and address data to be collected;
2. It requires in-state requesters to disclose information about themselves (driver's license numbers, hair/eye color, whether they are organ donors, etc.) that does not facilitate the FOIA transaction;
3. Copies of the ID, or information collected from them, become public records the government must manage and possibly disclose under FOIA;[6]
4. Requesters are treated differently based on which records they've asked for; and
5. It puts citizens who do not have state-issued identification at a disadvantage.

The U.S. Supreme Court ruled in *McBurney v. Young*, 569 U.S. 221 (2013), that Virginia could limit FOIA's use to Virginians and media broadcasting or circulating in Virginia. Local and state government agencies can refuse to provide records requested by someone or some business from another state. And to discern who is making a request from inside the state versus outside the state, current law says "the custodian may require the requester to provide his name and legal address." (2.2-3704(A)).

Government is not required to rebuff out-of-state requests, but it may. If it chooses to fill an out-of-state requests, government does so outside the scope of FOIA, essentially on its own terms. As explained by the FOIA Council:

> Because the procedural rules of FOIA are not mandatory when dealing with out-of-state requests, you may collect payment in advance (whereas with a Virginia or media requester you may only collect payment in advance if the charges are likely to exceed $200), and you may respond in a reasonable time frame (rather than being held to the five working day limit to respond as you would with a Virginia or media requester).[7]

Government can ask out-of-state requesters to provide additional contact information.

The proposal treats requests for salary different from others. The Freedom of Information Act has long made clear that salary data is not a personnel record that can be withheld under the discretionary

[6] As noted in FOIA Council Advisory Opinion AO-08-06, "Once information becomes a part of a public body's records, then absent a statutory exemption, these public records must be released if requested." http://foiacouncil.dls.virginia.gov/ops/06/AO_08_06.htm

[7] "Responding To Requests From Out of State," FOIA Council policy publication: http://foiacouncil.dls.virginia.gov/out%20of%20state%20requests.pdf

personnel exemption of 2.2-3705.1(1). Salary data, including employee names, must be disclosed upon request,[8] a policy decision the General Assembly reaffirmed in 2017 when the required-disclosure section was amended to explicitly require employee names[9].

If Norfolk's experience is anything similar to Portsmouth's, requests for salary data are actually few in number and may come from local media.[10]

Salary records are not the only records that must be disclosed under FOIA.

FOIA's policy statement says that all public records "shall be presumed open,"[11] and the introductory language for each category of exemptions refers to some records being "excluded from mandatory disclosure."[12]

Proposal #1 would not stop the threat of phishing because requesters are still entitled to the mandatory release of many other kinds of records that could and do contain email addresses.

Proposal 2: Written requests with state ID for requests made electronically

Proposal #2 suffers from many of the same problems as #1, and then compounds that problem by treating requests made by electronic means differently from those made in-person or by mail.

Again, the information that would be collected under this proposal — beyond the name and address already allowed under existing law — would not facilitate in the transaction, and the government would be required to manage and safeguard any copies made of the submitted ID. Further, requests, no matter how they end up in the hands of government, are to be answered under the same procedures outlined in § 2.2-3704 of FOIA.

Phishing attacks depend on knowing the email addresses of various employees. As discussed on Page 8, there are myriad ways to obtain employee email addresses, none of which would be stopped or even slowed by state ID-bolstered electronic FOIA requests.

---

[8] The Office of Attorney General opined as far back as 1978 said that names were required to be released in relation to salary data. See Attorney General's Opinion 1978-79 #310: https://www.opengovva.org/foi-opinions/79ag310.

[9] See 2017 Acts of Assembly Chapter text CHAP0778 for HB 1539: http://lis.virginia.gov/cgi-bin/legp604.exe?171+ful+CHAP0778

[10] On July 25, 2019, VCOG requested all FOIA requests made in Norfolk since Jan. 1, 2019, for aggregated salary data. Of the seven responsive records provided, three were made by *The Virginian-Pilot*, two were from a Richmond man (a quick Google search showed him to be an attorney who formerly worked in the Attorney General's office), one was a Fairfax-based member of the advocacy group American Transparency, and one was from a Suffolk citizen (a quick Google search shows him to be employed at the Naval Medical Center in Portsmouth and a former FOIA officer in Hampton).

[11] Section 2.2-3700(B).

[12] Section 2.2-3705.1 through 2.2-3705.7.

Proposal 3: Exempt the government from liability when it gives information to law enforcement about FOIA requesters

This proposal is deeply troubling, as it contemplates government reporting individuals who have exercised a right expressly granted to them by statute.

If the proposal is not specifically limited to situations where the requester is suspected of criminal activity, it will chill to the very bones anyone — citizen, news media or company — who asks for any records whatsoever. Government would have carte blanche to report any FOIA requester, secure in the knowledge that it would not have to answer for any unwarranted police attention the referral prompted.

At the July 15 meeting, the city expressed concern over liability for subsequent use of data required to be disclosed under FOIA. This is not a new concern, as the possibility that information can be somehow misused has always existed. The General Assembly can outlaw specific misuse of information, as it has in § 18.2-152.5:1, but general attempts to limit subsequent, legal use of information have been consistently rejected.

Proposal 4: Give citizens an opt-out agreement to protect their personal identifiable information from being disclosed in a FOIA request

As explained by the city, the suggestion here is that electronic requests for information would "encounter a page providing Virginia's FOIA regulations for requesting information including notice to citizens regarding their right to not have their information disseminated in a related FOIA request by checking an "opt-out" agreement box."

To the extent that this proposal seeks blanket protection for a person's personal identifiable information, it goes too far.

Since 2002, § 2.2-3705.1(10) has allowed citizens signing up to receive notices from the government to opt out of having their contact information disclosed in a FOIA request. The section was revised in 2017 to add and define the term "personal contact information": "home or business (i) address, (ii) email address, or (iii) telephone number or comparable number assigned to any other electronic communication device."

The theory behind the exemption is that a citizen or business forced to give up contact information in order to receive information about government plans or services should not have to disclose to the world that contact information. As discussed on Page 9, however, there are policy reasons for keeping contact information accessible.

Proposal 5: Continue a broad study of phishing

The law is always evolving. Continued study is a reasonable suggestion, provided that further discussions evolve, as well.

Public interest in contact information: email addresses, phone numbers

At the July 17 FOIA Council meeting, Sterling Rives, the local government representative to

the council, said he would be interested in hearing from the Virginia Coalition for Open Government and the Virginia Press Association as to the public value in having access to personal contact information for three categories of individuals: (1) government employee work contact information, (2) government employee non-work contact information, and (3) citizen contact information.

Government employee work contact information

Citizens have been able to interact with government by telephone for decades. Phone numbers to government departments were published in the free telephone directory "blue pages." Phone numbers — general numbers and direct lines — are routinely published on websites and added to email signature lines. Phone numbers are shared on business cards and on the forms citizens fill out for various services.

Official email addresses — general and direct — are at least as available as telephone numbers. And every time a government employee sends an email outside the government's domain, the recipient now knows the email address and can forward it or otherwise share it with others.

There is nothing personal or confidential about government-issued numbers or addresses. These are the public-facing contact points that citizens, media and business rely on to communicate with government.

This contact information is useful to FOIA requesters who seek records about who may be responsible for — or has participated in — decision-making that impacts the public. Sometimes, too, a citizen may have only an email address, but no name attached. The address assists that citizen (a) as an identifier, to keep track of who is who and who is saying what, and (b) in making future FOIA requests that ask for communication to or from the email address itself.

Government has discretion over how to present employee contact information on government websites. A balance will likely be struck between protecting contact information there versus limiting the public's ability to interact with government or taking advantage of e-government services.

Government employee non-work contact information

At first blush, there is little public value in granting public access to a government employee's personal information. Government employees are certainly entitled to personal lives. In today's connected and synced world, however, it is not unusual for government employees to use their personal cell phone number or personal email address to conduct the public's business.

This is not to suggest that these employees are trying to hide anything. Instead, it is meant to recognize how easy it is to confuse which one of multiple accounts or numbers is in use when writing or responding to a message or making a call.

If a record requested through FOIA contains an employee's personal contact information, then it has the same public value as if it were sent from a government number or address: (a) as an identifier, to keep track of who is who and who is saying what, and (b) in

making future FOIA requests that ask for communication between one person and the email address itself.

To the extent that such contact information is found on insurance cards, emergency contact sheets and other materials found in a personnel file, those records can be withheld under § 2.2-3705.1(1).

Citizen personal contact information

Though there is generally less value in having access to the personal contact information of citizens, there is still some.

Citizens interact with government sometimes because they are forced to, and sometimes because they choose to. They may be asking for a service that is available to anyone and may use a general phone number or email address or contact point; or, they may not need or want to communicate with a specific, identifiable person. If they are asked for their contact information, or if their email address will be visible to the government recipient, there is a case to be made for not requiring disclosure of that contact information. Again, that was the theory behind passage in 2002 of what is now 2.2-3705.1(10).

On the other hand, sometimes an individual contacts a specific government employee or official with an expectation that the employee will do something specifically for him or her: A lobbyist contacting an elected official, a developer contacting a county administrator, or a business owner contacting an accounts payable department. All may want to engage with government in a transactional way. Citizens, too, may contact an employee or official who the citizen wants to intervene in his or her particular problem.

There is public value in knowing who has an expectation of action being taken on his or her behalf. Having the contact information is also valuable for the same reason as in the above two categories: (a) as an identifier, to keep track of who is who and who is saying what, and (b) in making future FOIA requests that ask for communication between one person and the email address itself.

In 2017, the General Assembly repealed a 5-year-old exemption for "names, physical addresses, telephone numbers, and email addresses contained in correspondence between an individual and a member of the governing body, school board, or other public body of the locality in which the individual is a resident."[13]

The exemption said it would not apply when the correspondence related to the transaction of public business, an acknowledgement that correspondence in the government's possession is not subject to disclosure under FOIA if it is not about public business. Because a public record is already defined as one used in the transaction of public business, the exemption was considered redundant and was thus eliminated.

Truly personal correspondence with government that includes contact information is not a public record and will not have to be released through FOIA. But citizens interacting with government about government business should not have an expectation that they can do so anonymously.

[13] Former § 2.2-3705.7(30), enacted in 2012: http://lis.virginia.gov/cgi-bin/legp604.exe?121+ful+CHAP0726+hil

Existing solutions

The threat of ransomeware attacks in Atlanta, Baltimore and Lake City, Florida, was offered as one of the justifications for the above proposals. As of July 2019, the cause of the attacks has not been determined, but there has been no suggestion by the localities that the email address carrying the virus was obtained through a request for public records.

Keep in mind that phishing attacks, especially those seeking to infect computer networks, originally targeted businesses. Businesses are not required to disclose records that contain email addresses, yet bad actors have obtained access to them nonetheless.

Email addresses are easily found in any number of places and from multiple sources. Armed with one address in a network, bad actors can easily guess what the addresses of others will be, considering addresses within a network tend to follow particular naming conventions, e.g., first initial + last name, or firstname.lastname. Someone intent on doing harm won't mind taking the time to try multiple variations of the same pattern, knowing that many attempts will be wrong, but also knowing that many will be right. And it only takes one.

In the cat-and-mouse game of trying to thwart bad actors, it must be acknowledged that any possible benefit these proposals might generate would be only temporary. Bad actors will continue to seek cracks in systems, exploit vulnerabilities, create work-arounds and develop new tricks to con the unsuspecting.

Steps taken internally in government are ultimately more effective, including:

- Constant improvement of government network security;
- Network and data redundancies that can be accessed should data be breached or held hostage;
- Training employees not to divulge personal information or click on suspicious looking links without first checking with the purported sender; and
- Using unique identifiers when communicating with citizens who are required to share their contact information; and
- Enforcing existing laws prohibiting misuse of data obtained by deception.

Conclusion

Legislative proposals are best when they address well-documented problems with surgical precision. Legislative proposals should be narrowly crafted to avoid overreach and unintended consequences.

The proposals currently being offered to address phishing are overly broad, they do not solve — even partially — the problem of phishing, and they run counter to the overall policy statement of FOIA that the statute exists to "ensure[ ] the people of the Commonwealth ready access to public records in the custody of a public body or its officers and employees."[14]

[14] Section 2.2-3700.