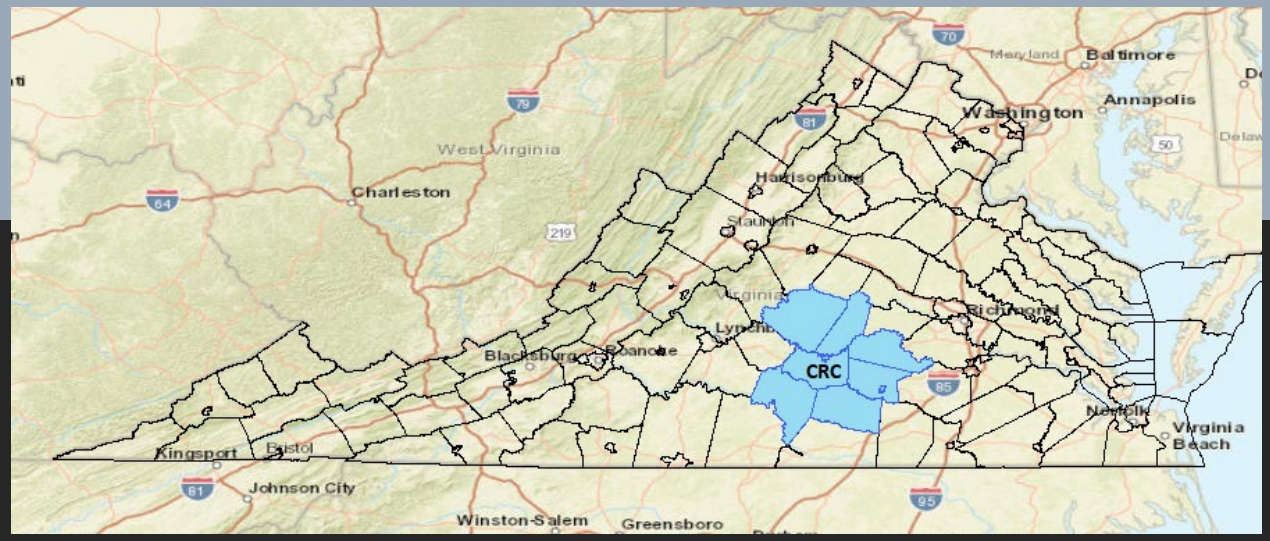
COMMONWEALTH REGIONAL COUNCIL CYBER INCIDENT

The Commonwealth Regional Council represents 7 counties and 11 towns in rural Southern Virginia. We routinely assist localities in applying for grants and administering the grants once funded. We also on some occasions apply for regional grants on behalf multiple jurisdictions.



CYBER INCIDENT

It was during one occasion recently that we had applied for and received a regional $15 million dollar grant for several of our jurisdictions. The localities also had to provide cash match for this grant that was going to utilized on the front end of the project to be paid to the vendor to get the project rolling.

CYBER INCIDENT

The vendor, as always in these cases, was ready to get the project started. They began work and sent an invoice for payment. To try and fast track payment the vendor asked if payments could be set up as ACH/Wire transfers.

Our staff reached out via email to all of our localities working on this project to pose this question and wait for responses.

CYBER INCIDENT

- In the meantime my staff who was working on this project started noticing something strange going on with their email. He would get responses from a locality to questions he had not asked? While odd, when you are busy and multi-tasking it is easy to set this aside to check into later (did I send that email and I forgot?).

- What really happened was the staff's email had been hacked and a hacker was monitoring the email account looking for anything they wanted to intervene by setting up "rules" of the email account to delete all correspondence once sent by the hacker (posing as the CRC staff) – that way the CRC staff member would not be able to see the emails in their sent folder.

CYBER INCIDENT

Two things happened next to set up the Cyber Incident:

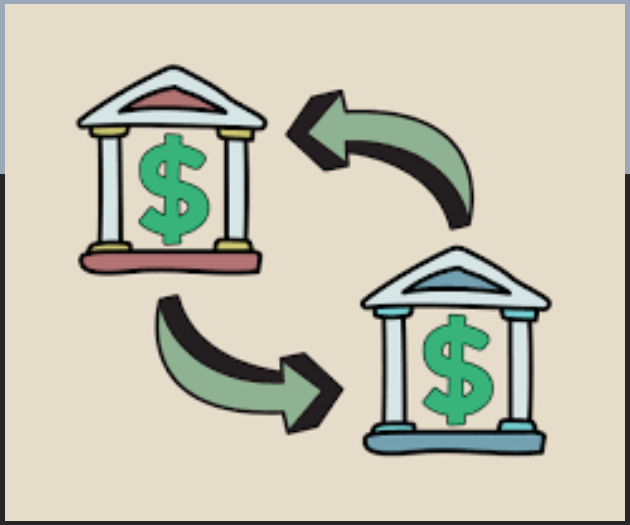
1. The Vendor, in hopes that one of the localities would agree to allow wire transfer, sent their banking information via email to the CRC. (Mistake #1 – never email sensitive financial information)

1. One of the localities responded they would agree to provide the vendor payment via wire transfer. They stated they would need the request on the vendor's letterhead and would need the vendor's banking information.

- At this point the hacker saw an opportunity and took over. They took the banking information provided by the vendor and transposed the banking information with their bank of choice and took a copy of the vendor’s letterhead and made a request for payment of an existing vendor invoice that was also located in an email thread to be sent to their new bank of choice.
- This was immediately sent to the locality. This all happened in an ongoing email thread with professional looking language that was only a little off from the normal dialogue of the CRC staff member.

CYBER INCIDENT

- The locality had received cyber training and knew to verbally check to make sure the request was real, so the vendor was called to verify the payment amount - however the account # was not verified. Since the vendor had requested a wire transfer and the locality had previously received a copy of an invoice that needed to be paid, the wire transfer was completed.



CYBER INCIDENT

Saving Grace…

- The locality had a Cyber Policy through VAcorp. The locality called their VAcorp representative who then in turn got the ball rolling to involve their immediate contact with the FBI. Because of this relationship, the FBI were able to put a hold on the funds once they were wired to the bank of choice by the Hacker. The locality also was able to get their funds returned to them over the next several weeks.

Lessons Learned:

- If you don't have a Cyber Policy – GET ONE!
- Utilize your insurance provider through your cyber policy to develop best practices internally in your office.
- Never email sensitive financial information (fax or hand deliver).
- If you do provide wire/ACH deposits, have staff call to verify verbally account # and amount.
- Have a policy that requires multiple signatures to verify wire transfers internally before they are released to allow multiple people to give it the smell test.
- If you do ever have a Cyber attack, call your Insurance Company immediately, the quicker they know the better the chance you can get it resolved.

CYBER INCIDENT