Cyber Security is a Team Sport

- Threat Intelligence Sharing is Highly Valuable
- Sharing is caring
- Who all receives our report
  - US Department of Homeland Security (CISA and I&A)
  - EI-ISAC
  - State of Ohio Fusion Center/State Highway Patrol
  - Ohio National Guard
  - Private Sector Cyber Security Partners
Cyber Security is a Team Sport

Local Board of Election Reporting

Ohio SOS Analysis

Ohio SOS SAR

RAW Reporting from Board of Elections

Detailed Internal Cyber Reporting

Frank LaRose
Ohio Secretary of State
What we report

• Anything “suspicious”
• Phishing Campaigns
• SQL Injection Attempts
• Network traffic that isn’t “normal”
• Include as much information as possible!
• Look beyond your election related systems
Specific example of it making a difference

- Late in 2019, the Ohio Secretary of State filed a Suspicious Activity Report showing a high volume of scans against our Online Voter Registration System.
- Early in 2020, the Ohio Secretary of State received information from a trusted third party that the same addresses listed in the Suspicious Activity Report was also performing additional scans of another Secretary of State’s network.
- The affected State was contacted, and scanning was remediated.
Phishing Suspicious Activity Report Example

Received SPAM: None (protectet.outlook.com; ab shrihik.com does not designate permitted sender list)

Reply-To: not specified

Screenshot of email:

Full analysis was not able to be performed at this time.

Headers:
Authentication-Results: spf:none (sender IP is 74.208.4.197) smtp.mailfrom: ab shrihik.com; Ohio secretary of state.gov; dmarc=none (message not signed)
headers=none hsi:skipheader:refuse:refuse:header:from:ab shrihik.com; computo=softpass reason=none
Client: olivero (185.161.209.62)
From: 14 July, 2020 <office@ab shrihik.com>
Message ID: <86k6o44v77j3jU6SMoyGt5SwcRj38K2YM3M@home.com>
Originating IP: most perfom.net (74.208.4.197)

Any questions, please contact:

[Signature]

[New Address]

[New Phone Number]
Questions