PHISHING ELECTION ADMINISTRATORS

©2020, REV 072320

EXECUTIVE SUMMARY

We are at the 100-day mark until the 2020 presidential elections, and Americans are wondering whether the cybersecurity protections and processes implemented over the preceding four years will uphold the integrity of our democracy.

The continuous drumbeat of the cybersecurity doom narrative has led some to say our democracy is no safer from cyber attacks than it was four years ago. Foreign cyber actors continue to interfere with elections in the United States and around the world via cyberspace. The targeting of candidates and political committees is well documented. Social media influence on the electorate remains a flashpoint. The integrity of voting systems has yet to be assured. On top of this, the global computing infrastructure is permeated with deep vulnerabilities. Dangerous inconsistencies in public policy approaches to encryption persist. And major internet companies, at the center of it all, have shown themselves not to be in control of their infrastructure.

People, as a result, have adopted a laissez-faire attitude towards the whole thing.

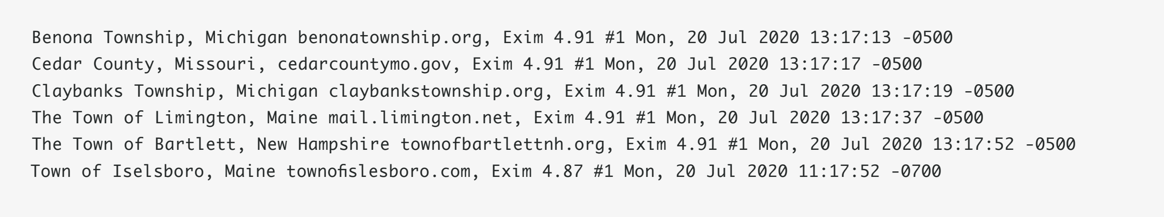
The administration of elections in the United States is complicated. The federal government has immense resources and capabilities, but little authority. Local officials who, with the most limited resources, find themselves in the crosshairs of nation-state cyber warfare without the knowledge or tools to fight back. A political theorist would deem the intertwined roles and responsibilities elegant by design. But from a cybersecurity perspective this complex system is a cluster[redacted] of vulnerability.

Area 1 Security and our partners at Americans for Cybersecurity undertook a research effort to analyze state and local election administrators susceptibility to phishing and their resulting cybersecurity damages and in doing so found:

1. Less than 2 in 10 election administrators (18.61%) have implemented advanced anti-phishing cybersecurity controls.
2. A little less than 3 in 10 (28.14%) election administrators have basic controls to prevent phishing.
3. Greater than 5 in 10 (53.24%) election administrators have only rudimentary or non-standard technologies to protect themselves from phishing.
4. A surprisingly large number (5.42%) of election administrators use personal email addresses or technologies designed for personal email. Some, like polkcountyclerk@[redacted] used by officials in Polk County, Arkansas, likely are dedicated to avoid compliance or intermingling of personal emails, while others such as haveknifewilltravel[redacted] used by a local election official doesn’t appear as well prepared.

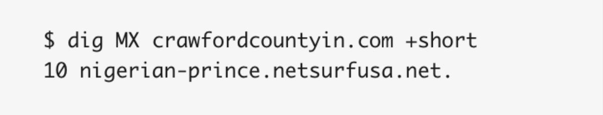
EXECUTIVE SUMMARY (CONT.)

5 A number of election administrators independently manage their own custom email infrastructure, including using versions of Exim known to be targeted by cyber actors linked to the Russian military that interfered in prior United States elections.[1]



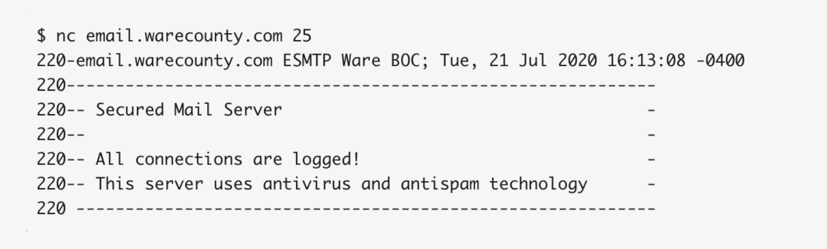
```
Benona Township, Michigan benonatownship.org, Exim 4.91 #1 Mon, 20 Jul 2020 13:17:13 -0500
Cedar County, Missouri, cedarcountymo.gov, Exim 4.91 #1 Mon, 20 Jul 2020 13:17:17 -0500
Claybanks Township, Michigan claybankstownship.org, Exim 4.91 #1 Mon, 20 Jul 2020 13:17:19 -0500
The Town of Limington, Maine mail.limington.net, Exim 4.91 #1 Mon, 20 Jul 2020 13:17:37 -0500
The Town of Bartlett, New Hampshire townofbartlettnh.org, Exim 4.91 #1 Mon, 20 Jul 2020 13:17:52 -0500
Town of Iselsboro, Maine townofislesboro.com, Exim 4.87 #1 Mon, 20 Jul 2020 11:17:52 -0700
```

6 Some network administrators, like in Crawford County, Indiana, which has 17 precincts and 8,947 registered voters brought a bit of humor to our data analysis.



```
$ dig MX crawfordcountyin.com +short
10 nigerian-prince.netsurfusa.net.
```

7 While others let us know they were watching and made us think twice about if they were on to cyber actors.



```
$ nc email.warecounty.com 25
220-email.warecounty.com ESMTP Ware BOC; Tue, 21 Jul 2020 16:13:08 -0400
220-----------------------------------------------------------
220-- Secured Mail Server                                     -
220--                                                         -
220-- All connections are logged!                             -
220-- This server uses antivirus and antispam technology      -
220 -----------------------------------------------------------
```

Take that Fancy Bear!

Nobody should take these insights from the observable data as an indictment of election administrators. It's their job to ensure that every citizen has access to making their voice heard in our democracy. The data does reveal that diffuseness and complexity in election administration does nothing to ensure elections are free from cyberattacks, of which 9 in 10 begin with phishing.

We hope that this may serve as a catalyst for an optimistic all-out assault, that ensures elections in the United States are free, fair and full of cybersecurity.

OREN J. FALKOWITZ | AREA 1 SECURITY

[1] Area 1 Security has identified at least 44 candidates for public office in the 2018 United States Elections that were running vulnerable Exim servers, and at least 50 candidates for public office in the 2020 United States Elections currently running Exim servers. Incumbent candidates' in the 2020 elections were assuredly susceptible to CVE-2019-10149 during the 2018 elections, and prior to February 2019. https://cdn.area1security.com/reports/Area-1-Security-EximReport.pdf

What is Phishing?

A phishing attack is an attempt to mislead the user of a computer to take an action that unwittingly causes harm. That action could be the downloading of a file, clicking on a link, visiting a website, completing an online form, or transferring sensitive data. The result of these actions can include installation of malware, theft of credentials, loss of data, theft of intellectual property and financial assets, and brand and reputation damage. Ninety-five percent of cybersecurity breaches worldwide begin with phishing.

EXAMPLES OF PHISHING IN U.S. ELECTIONS:

- During the 2016 election cycle, foreign cyber actors launched phishing attacks against election-sensitive organizations. These included state boards of election, secretaries of state, the Democratic Congressional Campaign Committee (DCCC), the Democratic National Committee (DNC), and Hillary Clinton's campaign.[2]
- During the 2018 election cycle, foreign cyber actors continued launching phishing attacks against election-sensitive organizations. These included political candidates, think tanks, and nonprofits. [3]
- In the current 2020 election cycle, foreign cyber actors have targeted election-sensitive organizations via phishing attacks. [4 & 5]

[2] *See United States v. Netyksho*, No. 1:18-cr-00215-ABJ (D.D.C. filed Jul. 13, 2018), ***available at*** https://www.justice.gov/file/1080281/download.

[3] *See* Brad Smith, ***We Are Taking New Steps Against Broadening Threats to Democracy***, Microsoft (Aug. 20, 2018), available at https://blogs.microsoft.com/on-the-issues/2018/08/20/we-are-taking-new-steps-against-broadening-threats-to-democracy; Natalie Andrews, McCaskill Says Senate Office Was Target of Phishing Scam, Wall St. J. (July 26, 2018), available at https://www.wsj.com/articles/mccaskill-says-senate-office-was-target-of-phishing-scam-1532656049; Andy Kroll, Documents Reveal Successful Cyberattack in California Congressional Race, Rolling Stone (Aug. 15, 2018), https://www.rollingstone.com/politics/politics-news/california-election-hacking-711202/.

[4] https://www.nytimes.com/2019/10/04/technology/iranian-campaign-hackers-microsoft.html

[5] *See* https://www.nytimes.com/2020/06/04/us/politics/china-joe-biden-hackers.html

Ratings System

Phishing campaigns come in all shapes and sizes. The majority of these campaigns begin with an innocuous email message that individuals are unable to distinguish as malicious. Consequently, the quality of email protection used by organizations and individuals has an inordinate bearing on their overall cybersecurity posture.

Our data identifies the current and observable email protections and controls elections administrators have. We have applied our rating system to evaluate the depth of email security in use by election administrators. The rating system assesses whether or not organizations are leveraging the native cloud provider controls as baseline; and anything above or in addition to that is rated higher, and anything below that is rated lower.

A summary of the rating systems is provided below:

5 **ADVANCED:**
Utilizing an independent email security service in addition to the basic protections provided by cloud email controls.

4 **BASIC:**
Utilizing the cloud provider's email controls only.

3 **LIMITED:**
Utilizing some measure of rudimentary cybersecurity control.

2 **NON-STANDARD:**
Utilizing their own email control based on open source software.

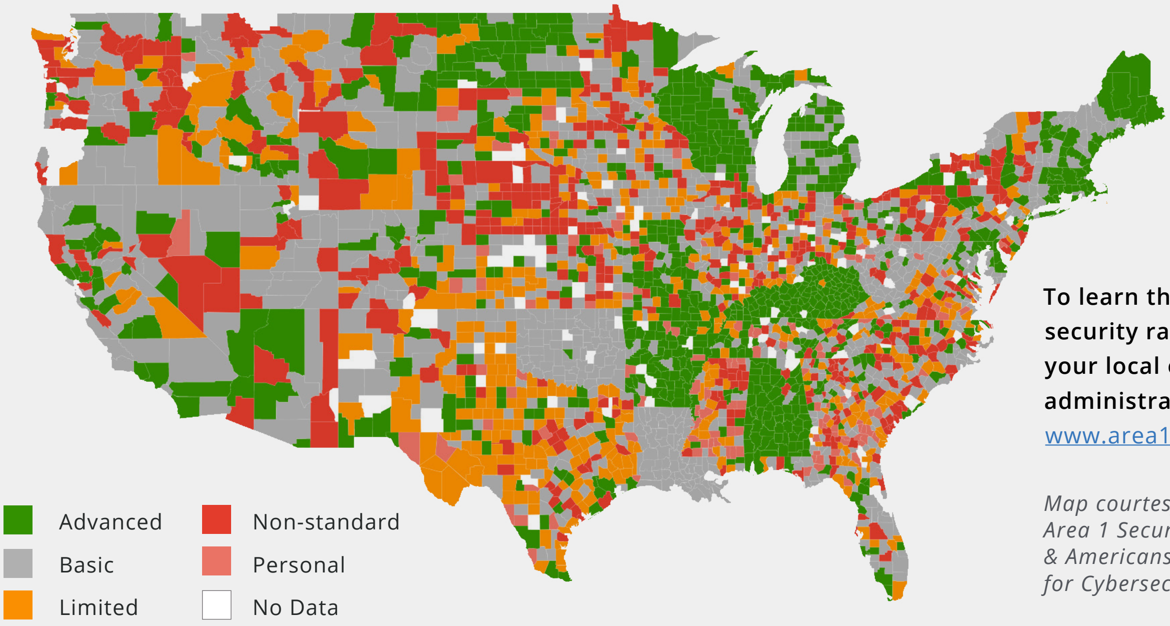
1 **NON-STANDARD (PERSONAL):**
Utilizing personal email or controls designed for personal email.

The rating system focuses on **publicly observable email security controls**; and does not assess whether or not an organization has additional internal controls (e.g., AV, Multi-factor Authentication, Access Control) that aren't publicly visible. Any of these additional controls will help bolster the security posture of the organization but do not effectively counter phishing attacks, Business Email Compromise campaigns or credential harvester campaigns. We recommend all organizations enforce the strongest level of security measures across various facets of their infrastructure, applications and data.

The rating system does not factor an organization's SPF / DKIM / DMARC policies and their records. Having robust DMARC policies ensures that organizations are protecting their brand and domain for outbound emails; but is insufficient and ineffective against inbound phishing attacks. We recommend that all organizations widely adopt and enforce DMARC policies as a matter of cybersecurity hygiene.

The rating system is vendor-agnostic; and any additional control that an organization has for supplementing their cloud email controls is rated as '**Advanced**'. At the time of this survey, none of the ratings are the result of Area 1's email security controls being in use.

The below map shows our rating system applied to every county in the United States. Where there is more than one election administrator in a county we have assigned the highest rating observed. **Appendix A** shows the complete counts of ratings for election administrators by state. The highest rating does not mean there are not severe cybersecurity risks to phishing in a given county based on our rating system. Further it only takes one to cause significant damage.



To learn the email security rating of your local elections administrators, visit www.area1security.com.

Map courtesy of Area 1 Security & Americans for Cybersecurity

ELECTION ADMINISTRATION AT STATE AND LOCAL LEVELS

Early in the history of elections in the United States, responsibilities of election administrators were occasional and clerical. With the move from ballots provided by parties to a secret ballot, adoption of voting machines, the enactment of the National Voter Registration Act of 1993 and the Help America Vote Act of 2002, states and election administrators earned greater responsibility — including IT management — as election technology advanced.

Despite the tremendous growth in responsibilities over the past century, election administration in states today is decentralized and contains a great deal of variation.

Today, there are more than 10,000 election administration officials in the United States. The size of their jurisdictions vary from a town of only a few hundred registered voters and to the largest counties with millions of people.

No state administers elections in the exact same way. Elections can be administered by a single individual, a board or commission of elections, or a combination of entities.

From an offensive cybersecurity standpoint, the dispersed nature of U.S. elections makes it impossible for cyber actors to hack elections nationally. However, we observe from the data and based on prior and ongoing cyber interference that the disparate approaches to cybersecurity by state, local and county officials is such that should a cybersecurity incident occur in one small town, whether in a "battleground state" or not, even if statistically insignificant, could cause troubling ripple effects that erode confidence in results across the entire country.

Recommendations

1 **VOTE!**

2 Our elections are important. They need to be resilient against whatever crisis the moment throws at us and that requires resources and planning. States are in different stages of cybersecurity readiness. Most are not very close to be able to ensure a safe election and it is only going to be exacerbated the longer it takes for them to get the resources and expertise needed to make changes. Congress is considering proposals to get states $3.6B and they need to act quickly before 3 November 2020.

3 Given the government's guidance to update Exim to mitigate CVE-2019-10149 and other vulnerabilities including but not limited to CVE-2019-15846 and CVE-2019-16928, we're urging election administrators to cease use of Exim. Upgrading alone does not mitigate exploitation. Prior Russian cyber activities directed towards U.S. elections, make use of Exim ill-advised. If you must continue running Exim, update to the latest version; running a version prior to 4.93 leaves a system vulnerable to disclosed vulnerabilities. Administrators can update Exim Mail Transfer Agent software through their Linux distribution's package manager or by downloading the latest version from https://exim.org/mirrors.html.

4 Running your own custom email infrastructure requires network administrators to be perfect every single day. We recommend the use of cloud email infrastructure such as Google's GSuite or Microsoft's Office 365 in combination with a cloud email security solution.

5 Under no circumstances should elections administrators use personal email for the conduct or administration of elections.

APPENDIX A

STATE / POSSESSION	COUNT OF OFFICALS PER STATE	ADVANCED	BASIC	LIMITED	NON-STANDARD	PERSONAL
Alabama	236	106	79	34	7	10
Alaska	8	8	0	0	0	0
American Samoa	2	0	0	2	0	0
Arizona	37	15	7	13	0	2
Arkansas	115	74	20	4	12	5
California	141	60	57	24	0	0
Colorado	139	40	54	29	4	12
Connecticut	654	39	248	279	38	50
Delaware	10	10	0	0	0	0
District of Columbia	2	0	0	2	0	0
Federated States of Micronesia	0	0	0	0	0	0
Florida	148	38	64	37	1	8
Georgia	262	37	70	103	38	14
Guam	2	0	2	0	0	0
Hawaii	9	3	4	2	0	0
Idaho	89	24	23	34	0	8
Illinois	199	34	46	106	10	3
Indiana	196	25	42	114	2	13
Iowa	219	27	113	76	0	3
Kansas	154	21	46	71	4	12
Kentucky	178	164	0	13	1	0
Louisiana	82	0	79	3	0	0
Maine	636	55	113	308	100	60
Marshall Islands	0	0	0	0	0	0
Maryland	59	16	39	4	0	0
Massachusetts	498	71	176	196	9	46
Michigan	1945	138	465	670	544	128
Minnesota	170	25	59	74	0	12
Mississippi	126	15	17	57	9	28
Missouri	204	92	50	37	9	16

APPENDIX A

STATE / POSSESSION	COUNT OF OFFICALS PER STATE	ADVANCED	BASIC	LIMITED	NON-STANDARD	PERSONAL
Montana	90	16	40	34	0	0
Nebraska	124	9	24	87	2	2
Nevada	30	12	9	7	1	1
New Hampshire	338	32	125	101	46	34
New Jersey	91	25	13	46	2	5
New Mexico	71	17	27	26	1	0
New York	233	66	69	92	2	4
North Carolina	179	32	59	81	2	5
North Dakota	77	64	10	3	0	0
Northern Mariana Islands	0	0	0	0	0	0
Ohio	232	232	107	64	21	11
Oklahoma	123	123	0	0	0	0
Oregon	73	73	27	34	0	3
Palau	0	0	0	0	0	0
Pennsylvania	117	18	39	57	0	3
Puerto Rico	1	0	1	0	0	0
Rhode Island	72	6	33	32	0	1
South Carolina	95	21	35	35	4	0
South Dakota	89	21	21	39	2	6
Tennessee	143	60	30	28	10	15
Texas	413	66	71	235	21	20
Utah	53	8	29	16	0	0
Vermont	331	21	112	124	44	30
Virgin Islands	5	0	5	0	0	0
Virginia	212	26	75	95	11	5
Washington	92	13	24	55	0	0
West Virginia	89	7	66	8	7	1
Wisconsin	2370	446	525	640	671	88
Wyoming	35	5	12	16	0	2
TOTALS	12298	2289	3461	4247	1635	666
%		18.61%	28.14%	34.53%	13.29%	5.42%

About Area 1 Security

Area 1 Security is the only company that preemptively stops Business Email Compromise, malware, ransomware and targeted phishing attacks. By focusing on the earliest stages of an attack, Area 1 stops phish — the root cause of 95 percent of breaches — 24 days (on average) before they launch. Area 1 also offers the cybersecurity industry's first and only performance-based pricing model, Pay-per-Phish.

Area 1 is trusted by Fortune 500 enterprises across financial services, healthcare, critical infrastructure and other industries, to preempt targeted phishing attacks, improve their cybersecurity posture, and change outcomes.

To learn more, visit **www.area1security.com**, follow us on **LinkedIn** or subscribe to the **Phish of the Week** newsletter.

About Americans for Cybersecurity

Americans for Cybersecurity is a 501 (c) 4 addressing critical areas of cybersecurity public policy, including eliminating policy zero-days, making sure that government law and policy is consistent with cybersecurity interests, standard reporting and metrics, making sure there is a baseline of knowledge as to the root causes and risks and Cyber 311, a national effort that gives citizens the ability to seek answers about cybersecurity challenges. Cybersecurity is the defining issue of our lifetime. As a tool for waging war, disrupting trade, stealing property, conducting espionage, and compromising elections, cybersecurity is the defining policy issue of the 21st century.