ELECTION SECURITY RISK IN FOCUS: PHISHING

Risks to Election Infrastructure

As the nation's **risk advisor**, the Cybersecurity and Infrastructure Security Agency's (CISA) mission is to ensure the security and resiliency of our critical infrastructure.

Major Risks Facing Election Officials

- Cyber
- Physical
- Mis-, Dis-, & Malinformation (MDM)
- Operational

What is Phishing?

Phishing is a form of social engineering that uses email or malicious websites to solicit personal information or to get you to download malicious software by posing as a trustworthy entity.

- Threat actors often mention current events, and times of year to capture attention and lure recipients to **click a link** or **download** a file containing malicious code
  - Holidays
  - Epidemics or health scares (e.g., H1N1, COVID-19)
  - Elections or other major political events
- Phishing attacks may also appear to come from legitimate organizations or businesses

Other Social Engineering 'ishing' Attacks

There are many methods attackers use to "catch" their victim

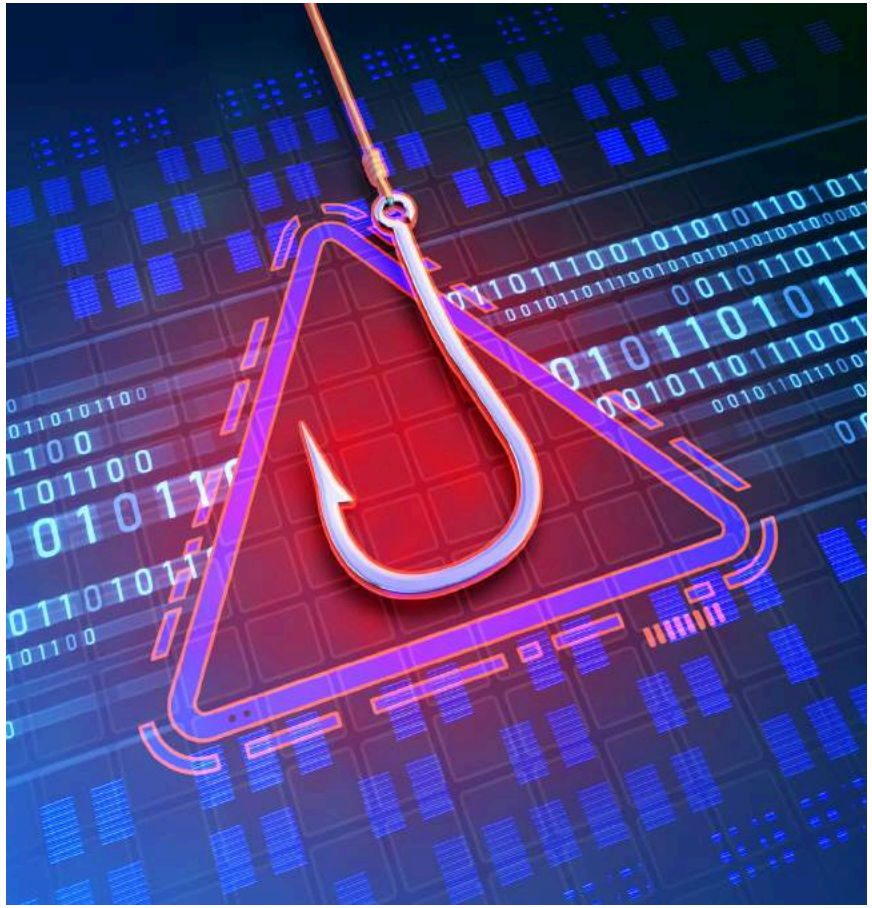
Spearphishing: Phishing targeted at an individual(s) by including key information about them

Whaling: Phishing targeted at high-profile individuals in order to steal sensitive and high-value information

Vishing: Phishing via voice communication to entice the victim to engage in conversation and build trust

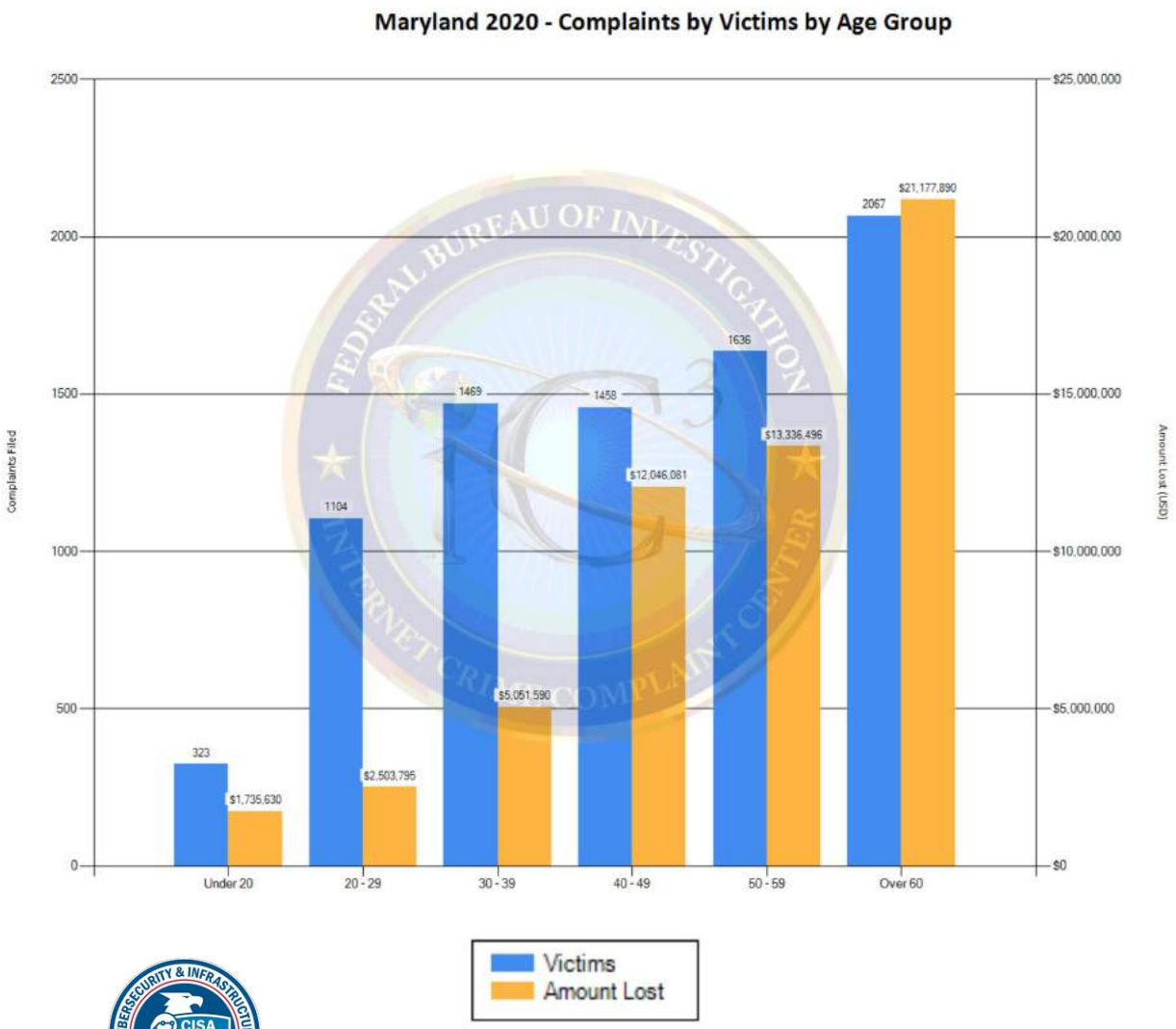
Smishing: Phishing via text messages to get you to click on a link, download files and applications, or begin a conversation

Signs of Phishing



- **Suspicious sender's address** that may imitate a legitimate business
- **Generic greetings and signature** and a lack of contact information in the signature block
- **Spoofed hyperlinks and websites** that do not match the text when hovering over them
- **Misspelling,** poor grammar or sentence structure, and inconsistent formatting
- **Suspicious attachments** requesting a user download and open an attachment
- **Requests, threats, and a sense of urgency** are tactics used to get the victim to act without thoroughly reviewing the email

Phishing Victims



FBI's Internet Crime Complaint Center (IC3) 2020 Internet Crime Report

- More phishing complaints than any other type of cyber crime
- Total Complaints - 241,342
- Adjusted losses - over $54 million

State Specific Data

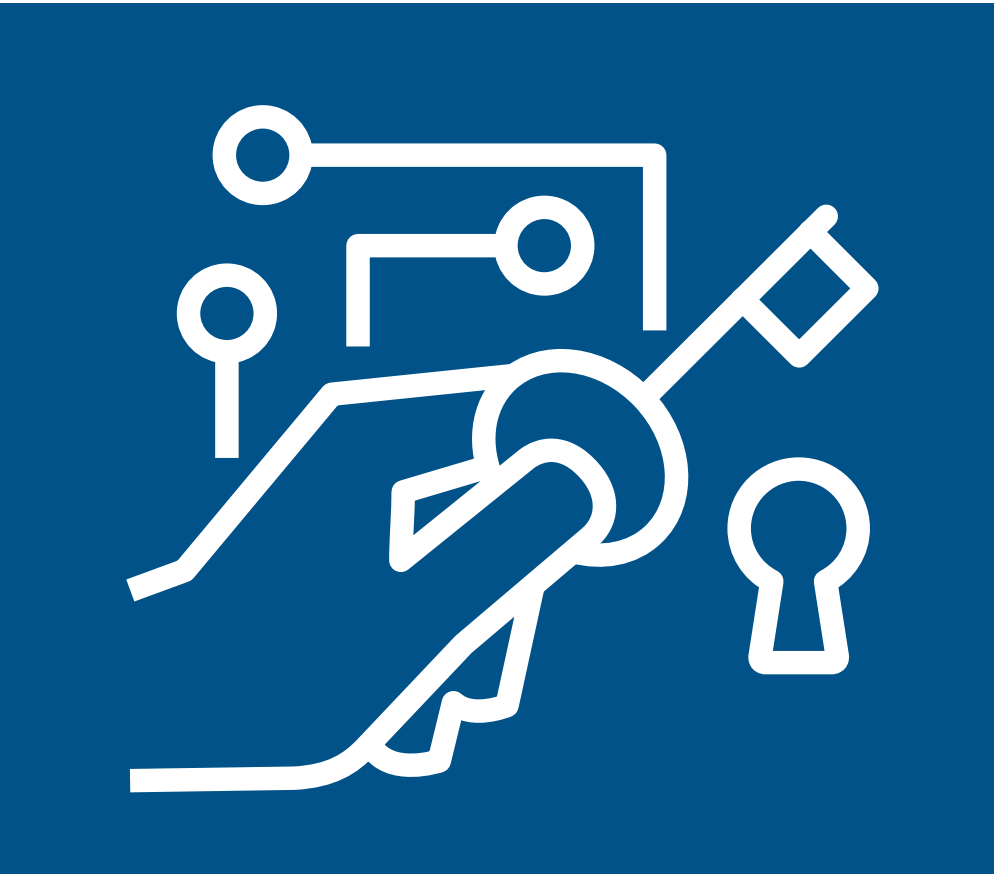
- Maryland Victim Count – 517
- Maryland Victim Loss - $895,383

Risk of Phishing: Malware

Source:
CISA Counter-Phishing Recommendations for Non-Federal Organizations

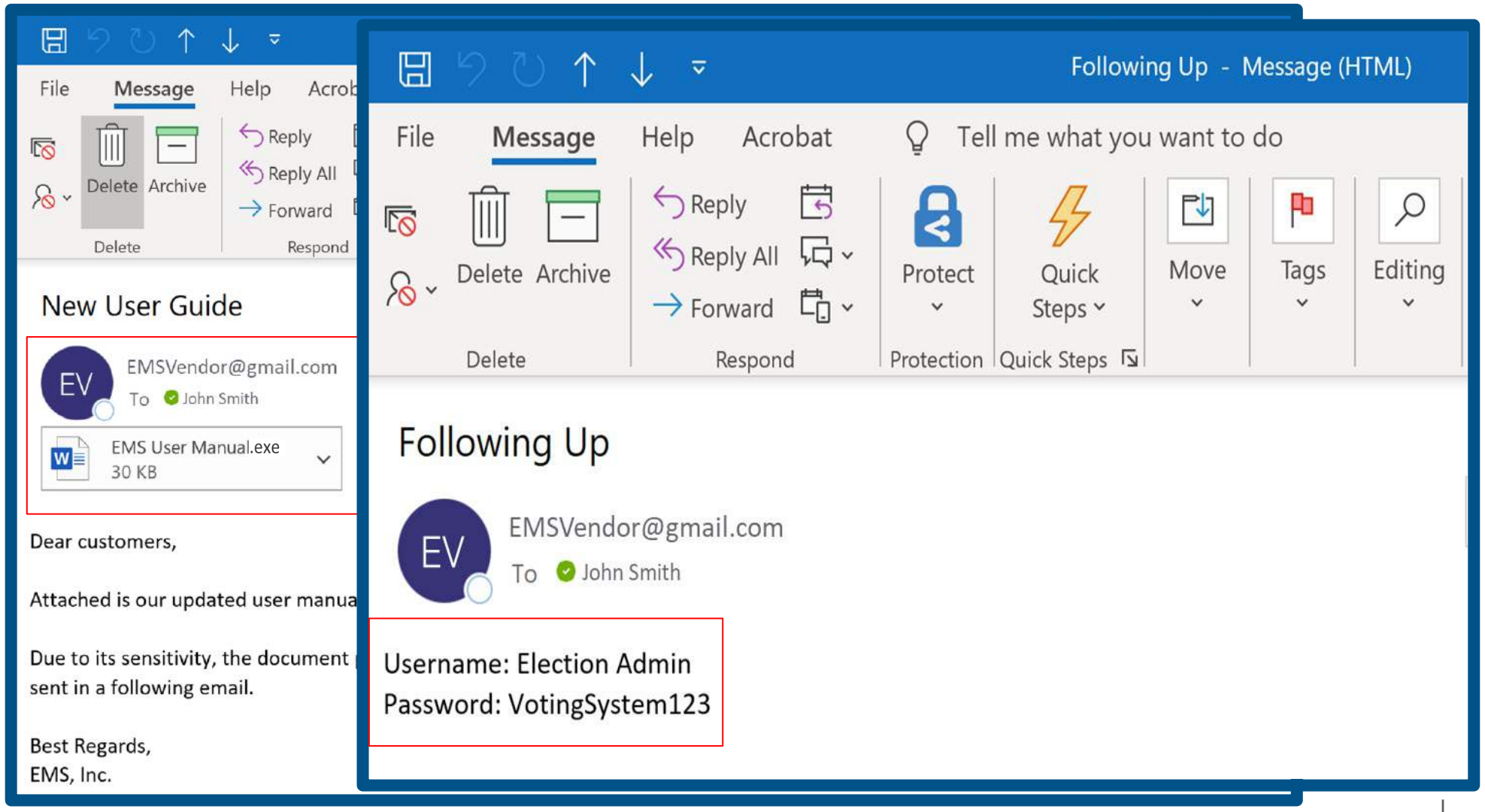
- Email systems are the preferred attack vector for malicious phishing campaigns
- Successful phishing attacks can devastate an organization with malware that:
  - Destroys computer files;
  - Provides adversaries with access to intellectual property;
  - Installs ransomware that holds information hostage in exchange for money; and/or
  - Deploys viruses that spread throughout a network like a flu and damage files and/or operating systems
- Election officials are public servants – it is your duty to communicate with your constituents – this adds complexity and risk that others don't have to face

Risk of Phishing: Credential Stealing



- Cyber actors can also use credential-based techniques to gain access to accounts in various ways:
  - **Password spraying** attacks rely on cyber attackers using a commonly used password against multiple usernames
  - **Brute-force** attacks rely on cyber attackers knowing the username and attempting several passwords
  - **Credential stuffing** attacks rely on cyber attackers using usernames and password combinations gained from data breaches against other accounts
- Once obtained your credentials can be used to:
  - Phish others by logging in and sending emails from your account
  - Access other accounts - if you reuse password
  - Move around the network to access critical data

Scenario: Malicious File Download



Scenario: Credential Stealing

Increased Se

BD ballotdefi

To

Dear customers,

We have increased implementing single sign on (SSO get to the site it will ask you to logi

Best Regards,

Voting System, Inc.

Forward •••

ed 4/7/2021 8:41 AM

Voting Systems, Inc.

https://portal.votingsystems/login

Voting Systems Customer Portal

The Customer Portal allows you to accomplish and manage these tasks involving your account:

- Review and update contact information
- Review and print order details and invoices
- Review your calendar for important election services timelines
- Request a new election
- Complete election forms
- Review election status progress
- Submit and track a new repair request
- Access technical manuals and product advisories

Need access? Request a new account.

Sign In

Reset my password

Scenario: Your Trusted Email to Steal PII

Action Required: Voter Registration Data Error...

File | Message | Help | Acrobat | Tell me what you want to do

Delete | Respond | Protect | Share to Teams | Quick Steps | Move | Tags | Editing | Read Aloud | Translate

Protection | Teams | Quick... | Speech | Language

Action Required: Voter Registration Data Error

RY

ryan@countyelections.gov

To

12:49 PM

Registered Voter,

During 2021 County, State, is conducting an audit of our voter rolls by reviewing the information in the statewide voter registration database. During the audit, an error in your registration data. In order to correct the error, please email us with your name, address, date of birth, drivers license number, and social security number.

Best Regards,
Ryan

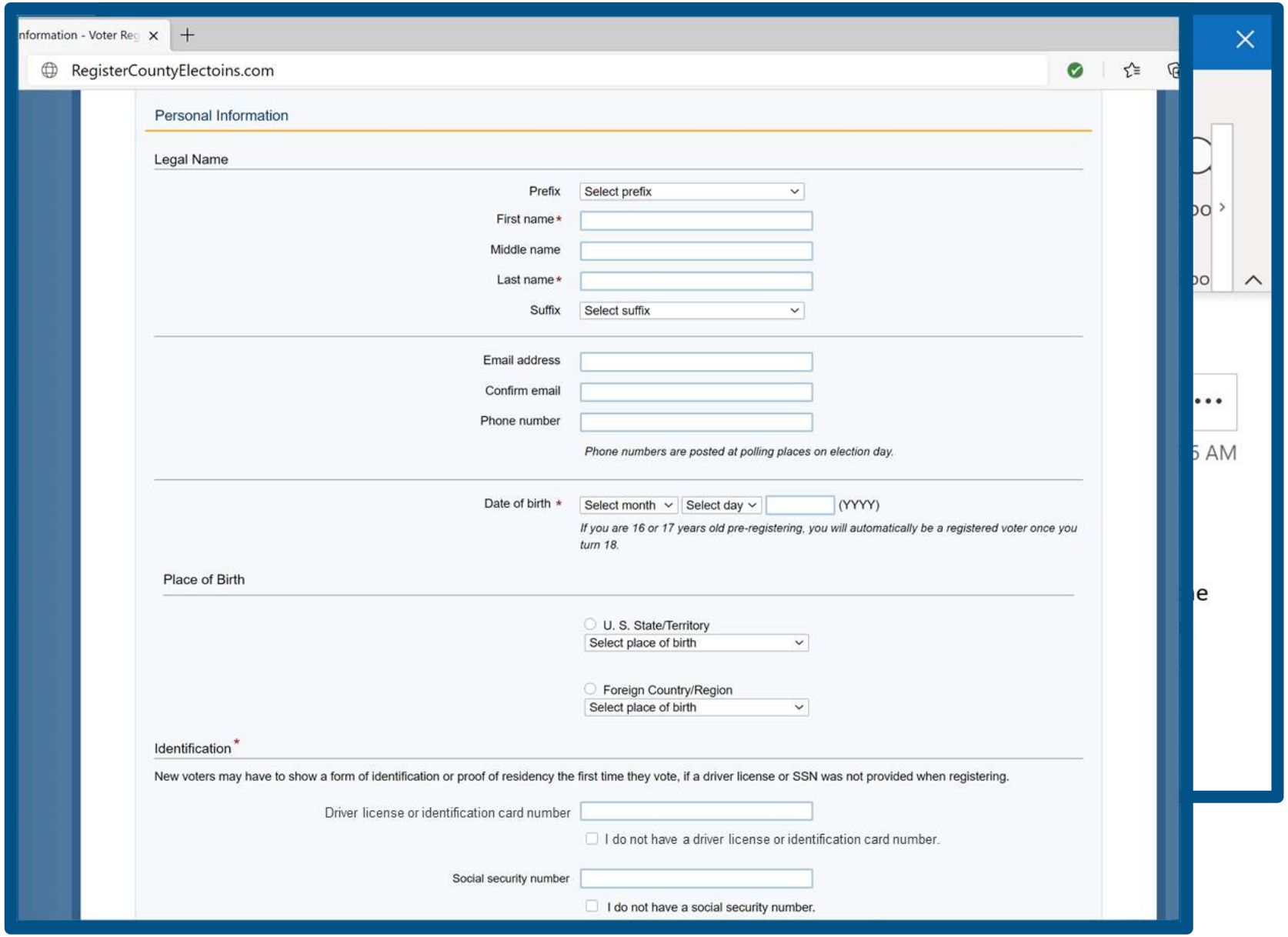
Scenario: Vishing & Smishing

- On Election Day you get a call from a “poll worker” who asks you to call them because there is a voter with an error in the epollbook.
- You call the poll worker back and ask what the issue is, and they say **Ryan Macias** is here and his address, DOB, and DL# do not match what is in the epollbook. The pollworker asks for you to provide the information in the voter registration database to see if maybe there is an error in the epollbook.
- You verbally provide the information for Ryan Macias and the poll worker – giving out a voter’s PII.

- A voter receives a text message that reads: “Your voter registration needs to be updated. Please go to the following link immediately to update your information. RegisterCountyElectoins.com"
- The voter visits the link and provides their PII to a malicious actor.

Your voter registration needs to be updated. Please go to the following link immediately to update your information. RegisterCountyElectoins.com

Scenario: Spoof YUOR Domain to Phish



Simple Tips

- **When in doubt, throw it out:** If it looks suspicious it's best to delete and/or mark it as "junk"
- **Think before you act**: Be wary of communications that implore you to act immediately, offer something that sounds too good to be true, or ask for PII
- **Make passwords long and strong**: Use a password manager to ensure you have unique, long, and strong passwords for each account

Simple Tips

Use multi-factor authentication (MFA): Enabling MFA can help prevent adversaries from gaining access to your systems even if your password is compromised

Be wary of hyperlinks: Avoid clicking on hyperlinks in emails; hover your cursor over links in the body of the email and if the links do not match the text that appears when hovering over them, the link may be spoofed

Install and update anti-virus software: Make sure all your computers are equipped with regularly updated antivirus software, firewalls, email filters, and antispyware

Risk Mitigation Using CISA & EI-ISAC Services

- Conduct Phishing Campaign Assessment (PCA) to determine the susceptibility of personnel to phishing attacks
- Leverage the .gov top-level domain (TLD) to make your emails easily identifiable, trustworthy, and secure
- Perform Remote Penetration Testing (RPT) to identify and validate exploitable pathways if someone gets into your network
- Implement Malicious Domain Blocking and Reporting (MDBR) to prevent systems from connecting to harmful domains
- Deploy sandboxing or detonation chambers to safely isolate malicious links such as EI-ISAC Malicious Code Analysis Platform (MCAP)

Election Official Challenges

- Election officials are public servants – they **must open emails from strangers**
- **Downloading attachments is a part of the job** – voters send registration forms, candidates send candidacy paperwork, etc.
- Most election workers are a part-time, temporary workforce – in many instances all **communications are via personal email and phone**
- **Personal identifiable information (PII) is required to be validated** verbally to authenticate voters in many aspects of the election process
- Election technology providers regularly **distribute critical files** (e.g., ballot definition files, ballot PDFs, instruction guides, etc.) **as attachments**

Reporting Suspicious Emails & Incidents

1

Notify IT Department & SBE

Notify IT Department & SBE of any suspicious emails.

2

If you got phished - follow incident reporting protocols.

Use CISA's Cyber Incident Detection and Notification Planning Guide templates to develop protocols if needed.

3

Report to EI-ISAC.

The Security Operations Center (SOC) is available 24/7 to assist at

866-787-4722 and **SOC@cisecurity.org**

Protecting Election Infrastructure from Phishing

CISA strongly recommends election infrastructure asset owners and operators prioritize protecting accounts from email-based attacks

- **Secure user accounts on high value services:** Require strong passwords using a password manager and multi-factor authentication (MFA)
- **Transition to a cloud-based email server (if using on-premise email servers):** Add advanced protection services (e.g., Microsoft Enhanced Account Protection* and Google Advanced Protection service)
- **Segment your email server from other critical assets:** If you are infected it won't harm other systems
- **Implement email authentication and other best practices:** Enable STARTTLS, implement SPF & DKIM, set a DMARC policy

*no cost to at-risk election-related organizations

Additional Protective Measures

CISA recommends four ways to add layers of protection against phishing

- **Secure email gateway capabilities:** Intercept phishing emails before they even get to an employee's inbox
- **Implement outbound web-browsing protections:** Prevent computer users from connecting to websites created for nefarious intent, even if they click a link in the email
- **Hardened user endpoints:** Configure computer and network settings correctly and keep them updated to mitigate the risk of an attackers from gaining entry
- **Implement endpoint protections:** An important layer of security for operating systems and browsers at the host level, such as antivirus software, a host-based intrusion detection system (HIDS), and an intrusion prevention system (HIPS)

Additional Resources

- CISA Insights: Actions to Counter Email-Based Attacks on Elections-Related Entities
- CISA Tip: Best Practices for Securing Election Systems
- CISA Capacity Enhancement Guide: Countering Phishing Recommendations for Non-Federal Organizations
- CISA Tip: Avoiding Social Engineering and Phishing Scams
- Microsoft Blog: New cyberattacks targeting U.S. elections

Additional Resources

Phishing

Phishing is a form of social engineering that uses email or malicious websites to solicit personal information or to get you to download malicious software by posing as a trustworthy entity.

Types of Phishing

- **Spearphishing**: Phishing targeted at an individual by including key information about them
- **Whaling**: Phishing targeted at a high-profile individual to steal sensitive and high-value information
- **Vishing**: Phishing via voice communication to entice the victim to engage in conversation and build trust
- **Smishing**: Phishing via text messages to get the victim to click on a link, download files and applications, or begin a conversation

Protecting Election Infrastructure

- ☐ **Secure user accounts on high value services**: Require strong passwords using a password manager and multi-factor authentication (MFA).
- ☐ **Transition on-premise email servers to a cloud-based email server**: Add advanced protection services (e.g., Microsoft Enhanced Account Protection* and Google Advanced Protection service). *Available at no cost to at-risk election-related organizations
- ☐ **Segment your email server from other critical assets**: If you are infected it won't harm other systems.
- ☐ **Conduct Phishing Campaign Assessment (PCA)**: Determine the susceptibility of personnel to phishing attacks.

Signs of Phishing

- **Suspicious sender's address** that may imitate a legitimate business
- **Generic greetings and signature** and a lack of contact information in the signature block
- **Spoofed hyperlinks and websites** that do not match the text when hovering over them
- **Misspelling**, poor grammar or sentence structure, and inconsistent formatting
- **Suspicious attachments** or requests to download and open an attachment

As the nation's **risk advisor**, the Cybersecurity and Infrastructure Security Agency's (CISA) mission is to **ensure the security and resiliency of our critical infrastructure.**

Contact CISA at Central@CISA.gov for assistance with:

- Phishing Campaign Assessment (PCA)
- Obtaining a .gov Domain
- Remote Penetration Test (RPT)

Register for the EI-ISAC at learn.cisecurity.org/ei-isac-registration.

Visit cisa.gov/election-security to learn about CISA's role in election security.

Phishing Simple Tips

- ☐ **When in doubt, throw it out**: If it looks suspicious, it's best to delete and/or mark it as "junk."
- ☐ **Think before you act**: Be wary of communications that implore you to act immediately, offer something that sounds too good to be true, or ask for PII.
- ☐ **Make passwords long and strong**: Use a password manager to ensure you have unique, long, and strong passwords for each account.
- ☐ **Use multi-factor authentication (MFA)**: Enabling MFA can help prevent adversaries from gaining access to your systems even if your password is compromised.
- ☐ **Be wary of hyperlinks**: Avoid clicking on hyperlinks in emails; hover your cursor over links in the body of the email and if the links do not match the text that appears when hovering over them, the link may be spoofed.
- ☐ **Install and update anti-virus software**: Make sure all your computers are equipped with regularly updated antivirus software, firewalls, email filters, and antispyware.

Reporting Incidents

1. Notify Your IT Department

Ph: _____

E: _____

2. Follow Incident Reporting Protocols

Use CISA's Cyber Incident Detection and Notification Planning Guide templates to develop protocols if needed: cisa.gov/publication/protect2020-cyber-incident-guide.

3. Report to EI-ISAC

The Security Operations Center (SOC) is available 24/7 to assist at 866-787-4722 and SOC@cisecurity.org.

ELECTION SECURITY RISK IN FOCUS: RANSOMWARE

Initiative On Ransomware

> In collaboration with state, local, and Federal partners, and the private sector, CISA continues to make progress in addressing cyber risk, particularly the risk of ransomware, and will work to maintain the availability of critical services to the American people under all conditions.
>
> **- Director Easterly**

What Is Ransomware?

- Ransomware is a type of **malicious software designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption.**
- If ransom demands are not met, the system or encrypted data remains unavailable, or data may be deleted.
- In elections this could be used to deny access to or delete Voter Registration and/or Vote Tabulation data.

Serious Risks To Paying Ransom

CISA recommends you do NOT pay the ransom

- Paying a ransom **does not guarantee** an organization will **regain access** to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom.
- Some victims who paid the demand have reported being **targeted again** by cyber actors.
- After paying the originally demanded ransom, some victims have been **extorted to pay more**.
- **Decide before** an incident occurs as to whether you will pay or not and include in Cyber Incident Response Plans.
- Paying could inadvertently encourage this **Criminal Business Model**.

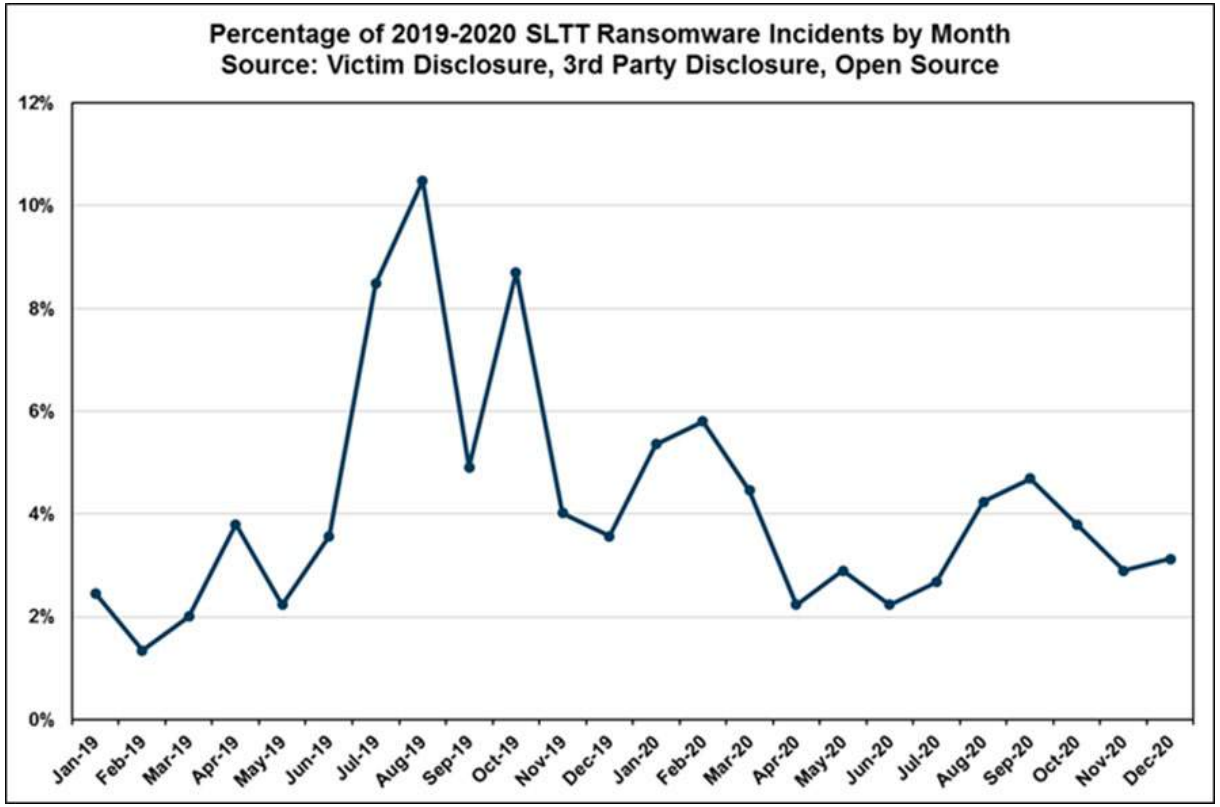
Ransomware Considerations

- Organizations should be aware of and address three areas of concern that can lead to the successful delivery of ransomware:
  - Phishing attempts
  - Unpatched public-facing systems
  - Weak password policy enforcement
- If you fall victim to a ransomware attack, ask for help – reach out to CISA or our FBI and U.S. Secret Service colleagues.

Ransomware in Critical Infrastructure

SLTT Government Reported Incidents

- Ransomware has become increasingly prevalent among SLTT entities and critical infrastructure organizations.
- From 2018-2019, there was a **153% increase** of reported SLTT ransomware attacks to MS-ISAC.
- 2019-2020, the SLTT reported ransomware attacks **decreased** by **20%**.



Scenario: Voter Information Released

INCIDENT

After ransomware attack, voter records and user credentials **are leaked by the cyber threat actor because the jurisdiction did not pay the ransom**.

IMPACT

Voting public and media lose confidence in the voting process because they see their personal information released publicly, sowing distrust in the voting process. Voters begin calling election officials to verify their voting records creating a burden on operations for state and local election officials.

Scenario: Voter Registration Database Attack

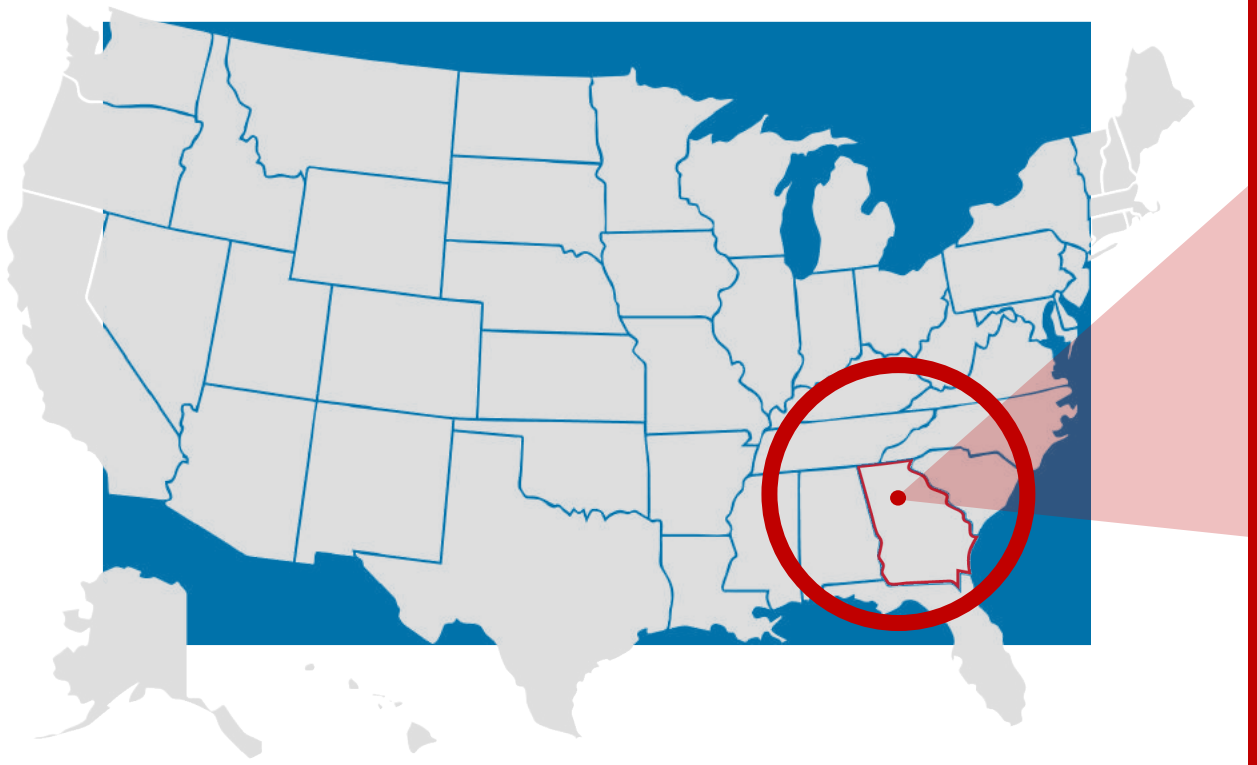
INCIDENT

A Voter Registration Database system **loses availability** on September 27, 2022, National Voter Registration Day.

IMPACT

It is so close to Election Day and poll books need to be printed that the **ransom is paid**. However, the data provided was from months prior and had been altered, **losing many registrants and changing others**.

Hall County, Georgia[1]



Hall County, GA

- **Date**: Disclosed October 7, 2020
- **Affected systems**:
  - Voter signature database
  - Voting precinct map
- **Data leaked:**
  - Stolen data was publicly released after county decided not to pay

[1] **Source:** https://www.cnn.com/2020/10/22/tech/ransomware-election-georgia/index.html

Chenango County, New York[2]

Chenango County, NY

- **Date**: October 18, 2020

  Six days before early voting and 16 days before Election Day

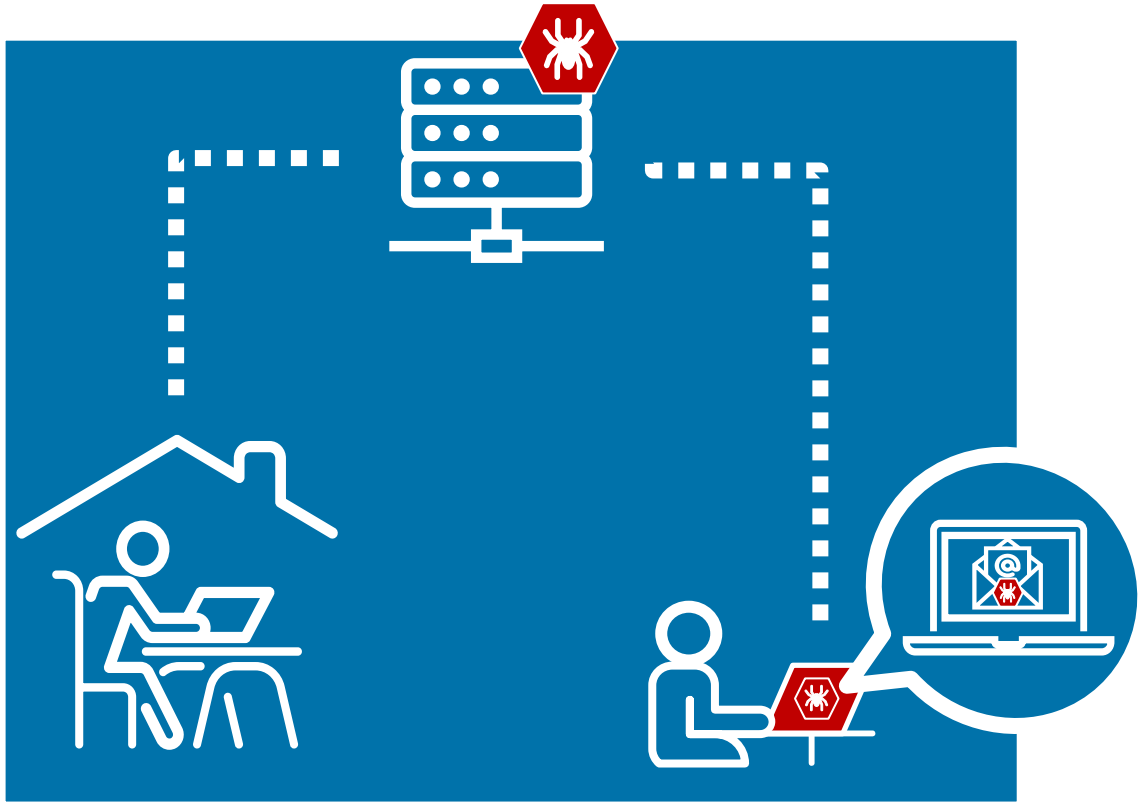
- **Affected systems**: Countywide email systems

- **Requested ransom:** Approximately **$90,000** total ($450/machine)

- **Recovery cost: $200,000** approved by County Board of Supervisors

[2] **Source:** https://www.govtech.com/security/Chenango-County-NY-Computers-Hit-with-Ransomware-Attack.html

Ransomware Vectors of Attack



- Escalation of **big game hunting** increasing the demand amounts.
- **Ransomware as a Service (RaaS)** allowed for an expansion of criminal enterprises.
- **Remote access software** and **email/ phishing** are consistently the most common infection vectors.
- Leveraging trusted relationships, **managed service providers (MSPs)** are used to target multiple entities.

Governance

It starts with you.

- Educate policymakers and budget holders about **necessary resources.**
- Collaborate with **asset owners** to ensure everyone understands their responsibilities.
- Train staff on **Cybersecurity Best Practices** and **Phishing Campaigns.**
- Develop cross-jurisdictional partnerships to **prepare and plan for an incident.**

But we all have a role.

Practical Suggestions

- Cyber Hygiene Services
  - Evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.
- Phishing Campaign Assessment
  - Provides an opportunity for determining the potential susceptibility of personnel to phishing attacks. This is a practical exercise intended to support and measure the effectiveness of security awareness training.

Practical Suggestions—continued

CSET Ransomware Readiness Assessment (RRA)

- Helps organizations evaluate their cybersecurity posture, with respect to ransomware.
- Guides asset owners and operators through a systematic process to evaluate their operational technology (OT) and information technology (IT) network security practices against the ransomware threat.
- Provides an analysis dashboard with graphs and tables that present the assessment results in both summary and detailed form.

Source: https://github.com/cisagov/cset/releases/tag/v10.3.0.0

CSET RRA—continued

- 10 Goals with 48 tiered practices; 18 Basic, 16 Intermediate, 14 Advanced
- Based off CISA Cyber Essentials, Ransomware Guide and leverages the MITRE ATT&CK Framework
- Structured to give organizations a clear path for improvement
- Complete with supplemental resources for each practice
  Several types of reports and charts depicting results
- Deficiency report highlighting weakest goals

Source: https://github.com/cisagov/cset/releases/tag/v10.3.0.0

CSET RRA—continued

- Robust Data Backup (DB)
- Web Browser Management and DNS Filtering (BM)
- Phishing Prevention and Awareness (PP)
- Network Perimeter Monitoring (NM)
- Asset Management (AM)
- Patch and Update Management (PM)
- User and Access Management (UM)
- Application Integrity and Allowlist (AI)
- Incident Response (IR)
- Risk Management (RM)

Source: https://github.com/cisagov/cset/releases/tag/v10.3.0.0

Risk Mitigation

- Create **backups** of your critical systems and data
- Implement **multi-factor authentication**
- **Patch Systems and Software**
- Develop **Incident Response Plan(s)** and **Business Continuity of Operation Plans**
- Conduct a **Cybersecurity Risk Analysis**
- **Segment** critical systems
- Implement **Application Allowlisting**
- Perform **Penetration Tests** on your systems

Incident Detection & Response

Use CISA's Incident Detection & Notification Planning Guide to build your team

Government Stakeholder Contacts Worksheet

Election Division INTERNAL System Leads

Partner/ Stakeholder	Name and Affiliation	Contact Information (Phone and Email)
Director	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
Deputy Director	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
Election Official	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]
Program Manager	**Primary:** [Insert Primary Name and Affiliation] **Backup:** [Insert Backup Name and Affiliation]	**Primary:** [Insert Primary Phone and Email] **Backup:** [Insert Backup Phone and Email]

Critical IT Observation Notification Plan

Phase	Action
Internal Alerting	**1a. Observer contacts Election Division IT Support Lead:** [Input Name and Contact Information] **1b. Observer notifies supervisor(s) and supervisory Election Official of the critical incident:** [Input Name and Contact Information] **1c. Election official identifies and assesses potential impacts to business systems and initiates business continuity plans as necessary:** [Plan #1 – Input Execution Considerations] [Plan #2 – Input Execution Considerations] **1d. Communications Director coordinates internal team to review and implement applicable emergency public relations and media communications strategies.**
Incident Escalation	**2a. Election Official immediately notifies appropriate state and federal partners of critical incident:** [Input State Election Authority Name and Contact Information] [Input State Information Sharing and Analysis Center Name and Contact Information] [Input State Emergency Management Name and Contact Information] [Input CISA POC Name and Contact Information] [Input EI-ISAC POC Name and Contact Information] [Input Local FBI POC Name and Contact Information]

Report It Immediately

Contact SBE:
(410) 269-2840 or
info.sbe@maryland.gov

Inform CISA:
www.us-cert.gov/report

Notify law enforcement:
Local FBI Field Office **or**
Secret Service Field Office

Where To Start

It is better **to prepare for ransomware** than respond

Take these steps to receive important alerts about attacks on election infrastructure, have a better understanding of your internet-facing vulnerabilities, and know whether your staff need more training on phishing.

1

Establish contact with your Regional CISA Cybersecurity Advisors (CSAs) & Protective Security Advisors (PSAs)

2

Email Central@cisa.dhs.gov to sign up for Cyber Hygiene Services:

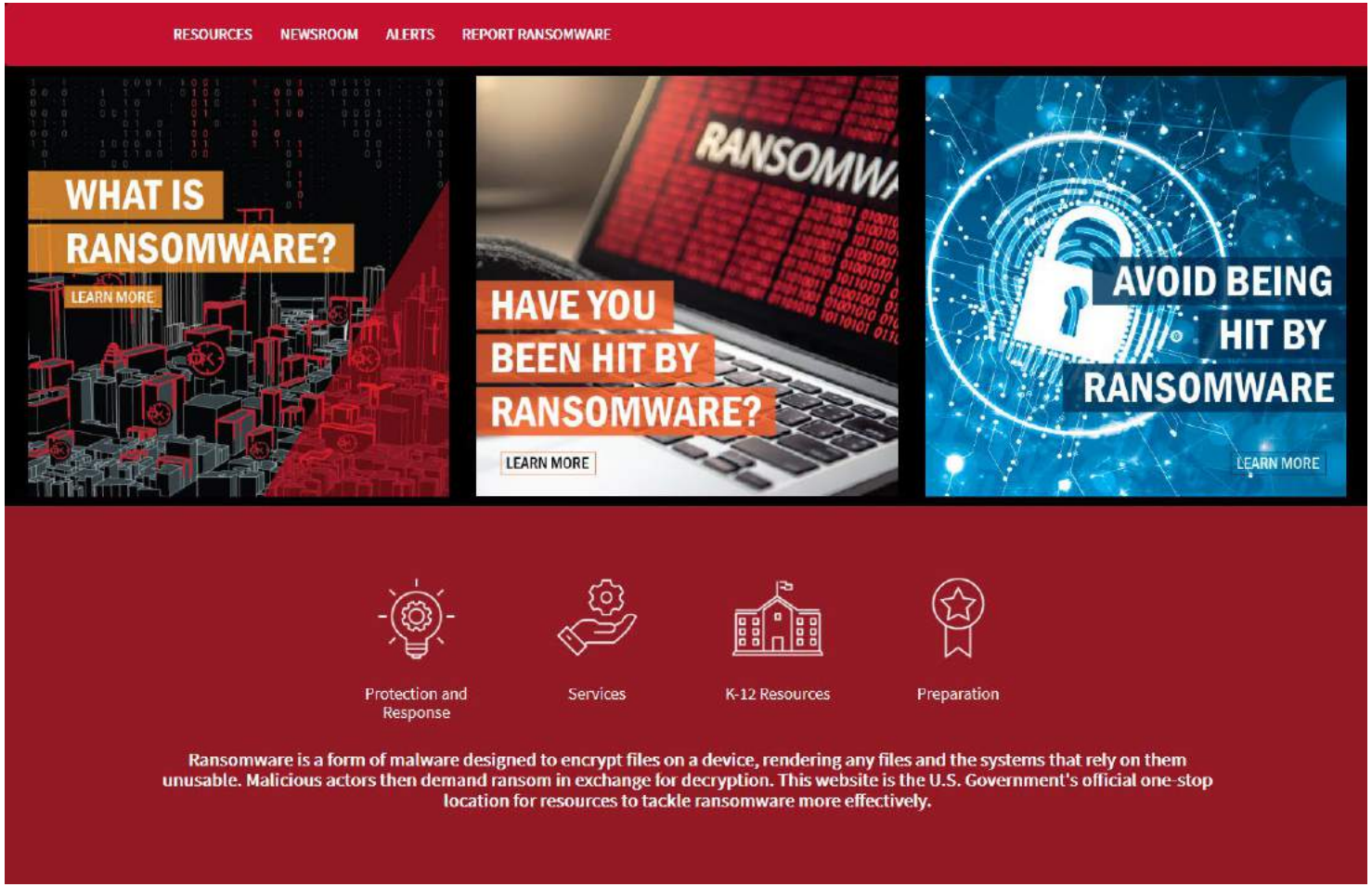
- ❑ Phishing Campaign Assessment
- ❑ Vulnerability Scanning
- ❑ Remote Penetration Test
- ❑ CSET RRA

3

Register for EI-ISAC at https://learn.cisecurity.org/ei-isac-registration

Elections Infrastructure ISAC™

STOP Ransomware Website

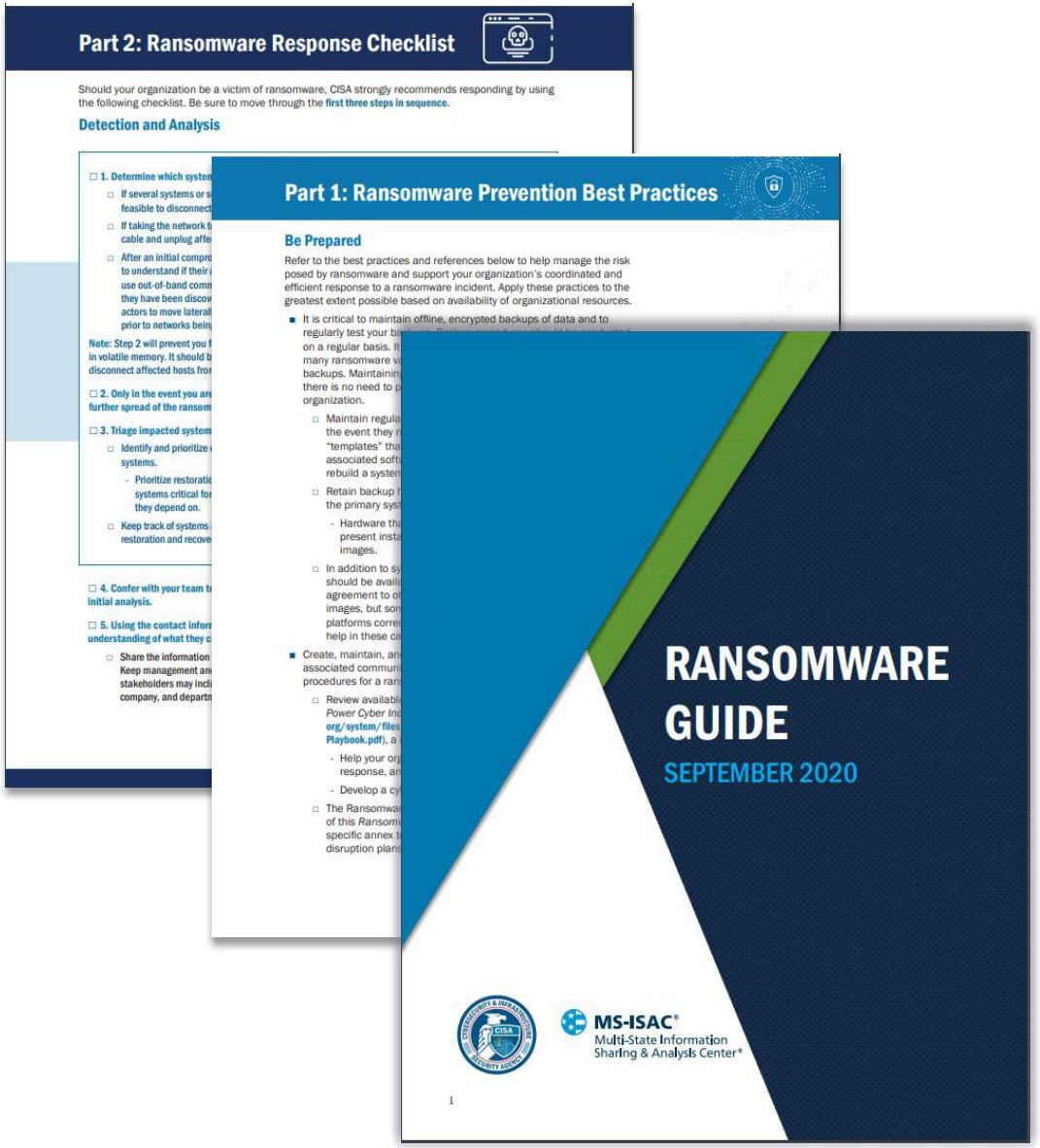


Source: https://stopransomware.gov/

Additional Resources

Joint CISA and MS-ISAC Ransomware Guide

This Ransomware Guide includes recommendations, best practices, recommended incident response policies and procedures, cyber hygiene services, and several checklists that organizations can use to help protect against or response to ransomware attacks.



Additional Resources

- CISA Ransomware Guide for Election Officials
- CISA Election Infrastructure Security Resource Guide
- CISA Elections Cyber Tabletop in a Box
- USG How to Protect Your Networks from Ransomware
- EI-ISAC Spotlight on Ransomware

Victims of ransomware should report it immediately to: CISA at www.us-cert.gov/report, a local FBI Field Office, or Secret Service Field Office

Additional Resources

Ransomware

Ransomware is a type of malicious software designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption.

Serious Risks to Paying the Ransom

- Paying the ransom **does not guarantee** an organization will regain access to its data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom.
- Some victims who paid the demand have reported being **targeted again** by cyber actors.
- After paying the originally demanded ransom, some victims have been **extorted to pay more**.
- **Decide before** an incident occurs as to whether you will pay or not and include in Cyber Incident Response Plans.
- Paying could inadvertently encourage this **Criminal Business Model**.

Vectors of Attack

- Escalation of **big game hunting** increasing the demand amounts.
- **Ransomware as a Service (RaaS)** allowed for an expansion of criminal enterprises.
- **Remote access software** and **email/phishing** are consistently the most common infection vectors.
- Leveraging trusted relationships, **managed service providers (MSPs)** are used to target multiple entities.

CISA RECOMMENDS THAT YOU DO NOT PAY THE RANSOM

Key Messages

- Keep Calm and Patch On
- Backing Up Is Your Best Bet
- Suspect Deceit? Hit Delete
- Always Authenticate
- Prepare and Practice Your Plan
- Your Data Will Be Fine if It's Stored Offline
- Secure Your Service Message Block (SMB)
- Paying Ransoms Doesn't Pay Off

As the nation's **risk advisor**, the Cybersecurity and Infrastructure Security Agency's (CISA) mission is to **ensure the security and resiliency of our critical infrastructure.**

Contact CISA at Central@CISA.gov for assistance with:

- Phishing Campaign Assessment (PCA)
- Vulnerability Scanning
- Remote Penetration Test (RPT)

Register for the EI-ISAC at learn.cisecurity.org/ei-isac-registration.

Visit cisa.gov/election-security to learn about CISA's role in election security.

Risk Mitigation

- ☐ **Create backups** of your critical systems and data.
- ☐ Implement **multi-factor authentication.**
- ☐ **Patch systems and software.**
- ☐ Develop **Incident Response Plan(s)** and **Business Continuity of Operations Plans.**
- ☐ Conduct a **cybersecurity risk analysis.**
- ☐ **Segment critical systems.**
- ☐ Implement **application allowlisting.**
- ☐ Perform **penetration tests** on your systems.

Incident Detection and Response

Use CISA's Cyber Incident Detection and Notification Planning Guide templates to develop protocols and to build your team: cisa.gov/publication/protect2020-cyber-incident-guide

Ransomware Guide

This Ransomware Guide includes recommendations, best practices, recommended incident response policies and procedures, cyber hygiene services, and several checklists that organizations can use to help protect against or response to ransomware attacks: cisa.gov/publication/ransomware-guide

Reporting: Important Contacts

Report to CISA
us-cert.cisa.gov/report

Find Your Local FBI Field Office
fbi.gov/contact-us/field/field-offices

Find Your Local Secret Service Field Office
secretservice.gov/contact/field-offices/

CISA
CYBER+INFRASTRUCTURE

Ryan Macias
SME Election Security Consultant
electionsecurity@hq.dhs.gov

Franco Cappa
Cybersecurity Advisor
franco.cappa@cisa.dhs.gov

Contact CISA:
Central@cisa.dhs.gov

CISA

CYBER+INFRASTRUCTURE