

**CISA Tabletop Exercise Package Elections – Early Voting**

[Enter Organization Name]

<Exercise Date>

Updated January 2024

Cybersecurity and Infrastructure Security Agency

Table of Contents

[Handling Instructions 3](#_Toc148091287)

[Exercise Overview 5](#_Toc148091293)

[General Information 6](#_Toc148091294)

[Module 1 8](#_Toc148091295)

[Module 2 11](#_Toc148091296)

[Appendix A: Additional Discussion Questions 13](#_Toc148091297)

[Appendix B: Acronyms 16](#_Toc148091298)

[Appendix C: Case Studies 17](#_Toc148091299)

[Appendix D: Malicious Activity 18](#_Toc148091300)

[Appendix E: Doctrine and Resources 20](#_Toc148091301)

# Handling Instructions

**Delete instructions that are not applicable.**

TLP:CLEAR

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):CLEAR*”: Recipients can spread this to the world, there is no limit on disclosure. This designation is used when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. **Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.**

This document may be disseminated publicly pursuant to TLP:CLEAR and <exercise sponsor name or other authority> guidelines.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:GREEN

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):GREEN*”: Limited disclosure, recipients can spread this within their community. This designation is used when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. **Note: When “community” is not defined, assume the cybersecurity/cyber defense community.**

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:GREEN and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:AMBER

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):AMBER”:* Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. This designation is used when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:AMBER and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:AMBER+STRICT

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as *“Traffic Light Protocol (TLP):AMBER+STRICT*: Limited disclosure, recipients can only spread this on a need-to-know basis within their organization. Note that “*TLP:AMBER+STRICT”* restricts sharing to the organization only. This designation is used when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization involved. Recipients may share TLP:AMBER+STRICT information with members of their own organization, but only on a need-to-know basis to protect their organization and prevent further harm.

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:AMBER+STRICT and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:RED

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):RED*”: For the eyes and ears of individual recipients only, no further disclosure. This designation is used when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.

This document should be disseminated to applicable partners and stakeholders on a strict need-to-know basis pursuant to TLP:RED and <exercise sponsor name or other authority> guidelines due to the extreme sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

# Exercise Overview

|  |  |  |
| --- | --- | --- |
| Exercise Name | Exercise Name | |
| Exercise Date, Time, and Location | Exercise date  Time (e.g., 9:00 a.m. – 12:00 p.m.)  Exercise location | |
| Exercise Schedule | Time | Activity |
| 20 Minutes | Threat Briefing and Opening Remarks |
| 60 Minutes | Module 1 |
| 20 Minutes | Break |
| 60 Minutes | Module 2 |
| Purpose | Examine identification, protection, and response capabilities for cyber incidents impacting elections infrastructure. | |
| National Institute of Standards and Technology Cybersecurity Framework Functions | Govern, Identify, Protect, Detect, Respond, Recover | |
| Objectives | 1. Assess election officials’ ability to identify, respond to, and recover from and cybersecurity incidents. 2. Examine information sharing processes among state and local election officials. 3. Explore processes for sharing accurate elections information. 4. Inform the development or refinement of policies, plans, and procedures to address threats and increase resilience among <state/county/municipality> elections infrastructure owners and operators. | |
| Threat or Hazard | Distributed Denial of Service (DDoS) | |
| Scenario | * Disruption and alteration of voter registration information systems * Foreign influence operations and disinformation * Distributed Denial of Service (DDoS) attacks and web defacements impacting elections infrastructure | |
| Sponsor | Exercise Sponsor | |
| Participating Organizations | Overview of organizations participating in the exercise (e.g., federal, state, local, private sector, etc.). | |
| Points of Contact | |  |  | | --- | --- | | **Insert Organization POC(s)**  Contact info | **National Cyber Exercise Program** [cisa.exercises@cisa.dhs.gov](mailto:cisa.exercises@cisa.dhs.gov) | | |

# General Information

## Building Resilience

The purpose of the National Cyber Exercise Program’s CISA Tabletop Exercise Packages (CTEPs) is to increase your organization’s resilience by assessing and validating capabilities and identifying areas for improvement. The National Institute of Standards and Technology (NIST) defines cyber resilience as “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.”[[1]](#footnote-2)

## Using this Situation Manual

Modules 1 and 2 contain the scenario injects and discussion questions you will use to conduct the exercise. There are footnotes with corresponding resources throughout the modules to guide your preparedness efforts. The appendices provide the following information to tailor the exercise discussion:

* Appendix A: Additional discussion questions that can replace or augment the existing Module 1 and 2 discussion questions.
* Appendix B: Reference section for acronyms used within this situation manual.
* Appendix C: Case studies that provide real-world examples of the threats presented in this scenario.
* Appendix D: An explanation of the threats presented in this scenario.
* Appendix E: Additional cybersecurity preparedness and response resources.

## Participant Roles and Responsibilities

**Players** have an active role in discussing or performing their primary roles and responsibilities during the exercise. Players discuss or initiate actions in response to the scenario. Suggested players include representatives from the IT, elections, communications, and legal departments, and any personnel with real-world cyber incident response roles. Players should bring a copy of their Cyber Incident Response Plan (CIRP) and any other incident related plans, policies, and procedures to the exercise.

**Observers** do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise. Observers may include representatives from the IT, elections, communications, human resources (HR), and legal departments as well as leadership who do not have assigned real-world cyber incident response roles but may be involved in response efforts or have a need-to-know.

**Facilitators** provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members may also assist with facilitation as subject matter experts during the exercise.

**Note-takers** are assigned to observe and document exercise activities. Their primary role is to document player discussions, including how and if those discussions conform to plans, policies, and procedures.

## Exercise Structure

This exercise is intended to be a facilitated exercise. Players will participate in the following:

* Cyber threat briefing (if desired)
* Scenario modules:
  + **Module** **1:** This module introduces a cybersecurity alert and cybersecurity events that could impact voter registration and ePollbooks.
  + **Module 2:** This module introduces impacts to voting procedures at polling locations.
* Hotwash
* ***Structure Note:*** *Modules, timeline dates, and discussion questions included in each module may be modified as desired. Additional discussion questions for each module can be found in Appendix A.*

## Exercise Guidelines

* This exercise is intended to be held in an open, no-fault environment. Varying viewpoints are expected.
* Respond to the scenario utilizing your knowledge of existing plans and capabilities, along with the valuable insights derived from your training and experience.
* Decisions are not precedent-setting and may not reflect your local government’s final position on a given issue. This exercise is an opportunity to discuss and present multiple options, possible solutions, and suggested actions to resolve or mitigate a problem.
* There is no hidden agenda, and there are no trick questions. The resources and written materials provided are the basis for discussion.
* In any exercise, assumptions and artificialities are necessary to complete play within the given time, achieve training objectives, and account for logistical limitations. Please do not allow these factors to negatively impact your participation in the exercise.

## Exercise Hotwash and Evaluation

The facilitator will lead a hotwash with participants at the end of the exercise to address any ideas or issues that emerge from the exercise discussions.

# Module 1

### 30 Days Before Early Voting

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) release a technical alert forwarded by the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) regarding malicious cyber incidents targeting elections infrastructure nationwide. Observed activity includes attempts to take down or deface public-facing voting related websites and theft of voter registration information.[[2]](#footnote-3)

### 12 Days Before Early Voting

A special interest group posts a deep fake video on their blog of a candidate allegedly accepting illegal campaign contributions from a foreign country and <state/county/municipality> election officials accepting bribes to alter ballots. The post goes viral on social media.

### 10 Days Before Early Voting

<Before the end of the voter registration period or three weeks before Election Day>, a popular blog posts a story claiming residents can register to vote through their website via a link that is not an authorized voter registration site. Social media posts circulate on various platforms advertising the illegitimate registration site.

### 7 Days Before Early Voting

The legitimate <online voter registration or other elections website> is subject to sporadic distributed denial-of-service (DDoS) attacks over the course of a week before the <new voter registration deadline or two weeks before Election Day>. As a result, the site is intermittently inaccessible.[[3]](#footnote-4)

## Discussion Questions

Discussion questions included in each module are designed to explore different aspects of your operational resilience. The questions may be modified as desired. Additional questions can be found in Appendix A.

1. What are the greatest cyber threats to the elections process?
2. Discuss <state/county/municipality>’s cyber resilience planning.[[4]](#footnote-5)
   1. What risk assessments have you conducted to identify specific cyber threats, vulnerabilities, and critical assets?[[5]](#footnote-6)
   2. Describe your asset management plan and how you prioritize critical assets.
   3. What improvements have been implemented to enhance cyber resilience following recent risk assessments?
   4. Do you apply Zero Trust Architecture (ZTA)/zero-trust concepts? How could the <state/county/municipality> use the CISA Zero Trust Maturity Model guide to help facilitate a gradual transition to this more secure type of environment?[[6]](#footnote-7)
3. What cybersecurity threat information does <state/county/municipality> receive?
   1. What sources do you receive cybersecurity threat information from?
   2. What cyber threat information is most useful?
   3. How is information disseminated across your organization and by whom?
   4. What actions would your organization take following an alert like the one presented in the scenario?
4. Describe the <state/county/municipality> cybersecurity training program for employees.[[7]](#footnote-8)
   1. How often are employees required to complete this training?
   2. Is training required during employee onboarding before granting system/network access?
   3. What additional training is required for employees who have system administrator-level privileges?
   4. What type of training methods or approaches have you found most beneficial?
5. What tools and capabilities do you have to protect and defend against foreign influence operations and disinformation?
   1. How would you communicate accurate information to the public?
   2. What discussions has <state/county/municipality> had on the threats to the elections process posed by malicious use of generative artificial intelligence (AI) to create highly compelling deep fake video, audio or images?
   3. How would you respond to an incident involving a deepfake video, audio, or images that undermine the security or integrity of the elections process?
   4. How would this response change if the incident involved communicating incorrect information about the time, place or manner of voting?
6. How do employees and the public report suspected phishing attempts or other possible cybersecurity incidents?
   1. What actions does the IT department take when suspicious emails are reported?
7. How is the integrity of your critical voter data protected and validated?[[8]](#footnote-9)
8. What external entities have access to the database?
9. How would those entities report a breach of their systems to your office?
10. Do you have security software that detects anomalous activity in the voter registration database files?
11. Do you have logging activated on the database to record data changes and user access?
12. How would you address the illegitimate voter registration website?
13. What automated and manual methods of DDoS attack detection and mitigation does your <state/county/municipality> employ?
    1. Who is notified by the automated detection tools?
    2. How would you manually detect a DDoS attack?
    3. How often are these systems tested?
14. What DDoS protections are included in your Terms of Service agreements with your outsourced service providers, such as your Internet Service Provider (ISP), Managed Service Provider (MSP), or Cloud Service Provider (CSP)?
    1. What additional protection against DDoS attacks might your agency consider?
    2. What gaps or limitations in coverage exist?
    3. Do you contact your service providers to inform them of key election operational windows when their services will be most important?

# Module 2

### 6 Days Before Early Voting

A breach of a vendor with access to the Voter Registration Database occurs and is reported by media outlets. An initial investigation confirms that voter registration data may have been altered by an account associated with the vendor.[[9]](#footnote-10)

### 5 Days Before Early Voting

Residents take to social media and post about their inability to register to vote despite repeated attempts. These concerns are shared by numerous accounts across social media and the hashtag #myvoteshouldcount becomes a trending topic.[[10]](#footnote-11)

### Early Voting Day 1 – Morning

On the first day of early voting, several <state/county/municipality> election websites display inaccurate information regarding early voting times and locations. IT staff are currently unable to access or correct the websites.[[11]](#footnote-12)

### Early Voting Day 1 – Early Afternoon

Later that day, a hacktivist group claims via social media to have “done their part” to protect the nation by successfully purging “all unnecessary voters” from the pollbooks. Election workers at 10% of early voting locations report a larger than normal number of voters arriving to vote and finding incorrect voter information in the pollbooks or no information at all.[[12]](#footnote-13)

### Early Voting Day 1 – Late Afternoon

The news media contacts <state/county/municipality> election officials to comment on rumors the state’s voter registration system was compromised and claims concerning the loss of election integrity.

## Discussion Questions

1. Using your Cyber Indecent Response Plan (CIRP), describe the actions <state/county/municipality> would take.[[13]](#footnote-14)
2. How often is the CIRP exercised with incident response personnel?
3. What guidance does the plan include on assessing the severity of the incident?
4. How does incident severity level dictate response?
5. How are critical systems and processes incorporated into your CIRP?
6. How are the voter registration database and/or voter registration portals secured?
   1. How would your organization implement continuity of operations plans if the voter registration database is unavailable during a critical voting period?
7. What actions would you take based on the initial investigation showing voter data may have been altered by an unauthorized user?
8. What capabilities and resources are required for responding to this scenario?
9. What additional resources outside of your organization would be necessary for responding to the cyber incident?
10. What are the processes or procedures for requesting additional resources?
11. What external partners (e.g., CISA, FBI) would you contact for assistance?
12. Describe your organizational processes to respond to the media reports and inquiries.
    1. How would public messaging be coordinated and disseminated during a cyber incident?
    2. How would you preserve and reinforce the public’s confidence and trust in your <state/county/municipality> during a significant incident?
13. In the event of a complete failure of the voter registration system, how would you continue with early voting?[[14]](#footnote-15)
14. How would you respond to the issue involving <ePollbook/pollbook> inaccuracies?
15. Based on discussion, what changes would you implement to increase the resilience of your organization?[[15]](#footnote-16)

# Appendix A: Additional Discussion Questions

The following section includes supplemental organizational resilience discussion questions designed to guide exercise play. Questions are aligned with the NIST functional areas and organizational roles and responsibilities. Exercise planners are encouraged to select additional, applicable discussion questions for the chosen scenario to bolster participant conversation. *This instructional paragraph, as well as undesired discussion questions, should be deleted.*

## Cyber Resilience

1. Discuss how cyber preparedness is integrated into your current all-hazards preparedness efforts.
2. How does <state/county/municipality> integrate cybersecurity into the system development life cycle (i.e., design, procurement, installation, operation, and disposal)?
3. Discuss your supply chain concerns related to cybersecurity infrastructure.
4. What cybersecurity language is included within third-party vendor contracts?
5. How do you evaluate the cybersecurity posture of your vendors?
6. How often are contracts reviewed?
7. How do your service level agreements address cyber incident notification?
8. What level of access do your third-party vendors have to the <state/county/municipality> network?
9. Describe your patch management plan.
10. What considerations (e.g., extended downtime, loss of data, impaired functionality, etc.) are addressed in the plan’s risk management strategy?
11. What is your method for tracking and identifying network vulnerabilities?
12. How are IT and business continuity functions coordinated with physical security?
13. What processes do you have to ensure that your external dependencies (e.g., contractors, power, water, etc.) are integrated into your security and continuity planning programs?
14. How is the integrity of your critical data protected and validated?
15. How would vendors report a breach of their systems to your office?
16. How does <state/county/municipality> maintain availability of key assets?
17. If primary communications are compromised, how do you provide information to internal and external entities?
18. What is your organization’s communications primary, alternate, contingency and emergency (PACE) communications plan?
19. What policies and procedures does <state/county/municipality> use to decide when and how to restore backed-up data?
    1. How does <state/county/municipality> incorporate measures for ensuring the integrity of backup data before restoration?

## Accounts & Privileges

1. Describe your <state/county/municipality>’s bring your own device (BYOD) policy.
2. What are <state/county/municipality>’s policies or procedures for IT account management?
3. What are the protocols for establishing, activating, modifying, disabling, and removing accounts?

## Incident Identification

1. How are cyber incidents reported within <state/county/municipality>?
2. What would trigger the reporting requirements established by regulation, law, and/or organization policy?
3. What training have employees received regarding reporting requirements and your CIRP?
4. What cybersecurity incident escalation criteria are defined in your CIRP?
5. Who is responsible and what actions would they take based on the scenario?
6. Who needs to be notified internally and externally according to the plan?
7. When is leadership notified?
8. When are other <state/county> offices notified?
9. Discuss <state/county/municipality>’s intrusion detection capabilities and analytics that alert you to a potential cyber incident.
10. What type of hardware and/or software does <state/county/municipality> use to detect and prevent malicious activity on your systems/network?
11. How often is <state/county/municipality>’s data integrity reviewed? How would you determine whether unauthorized manipulation of data has occurred?

## Incident Response

1. What are the roles of your network operations center/security operations center during a cyber incident?
2. What are your processes for collecting evidence and maintaining the chain of custody during a cyber incident?
3. At what point in the scenario would you contact law enforcement?
4. At what point would you contact the state’s chief election official (Secretary of State and/or State Election Director)?

## Recovery

1. What actions would <state/county/municipality> take if IT/incident response staff could not confirm the integrity of your systems/data?
2. What is the risk associated with re-activating critical business processes and systems?
3. How long and costly would the process be to completely rebuild these systems?
4. What factors do you consider when making these decisions?

## Training & Exercises

1. What training does your cybersecurity incident response team undergo to detect, analyze, and report malicious activity?
   1. What additional training and/or exercise requirements do you require for your incident response staff?
2. How do <state/county/municipality>’s training and exercise efforts address both physical and cyber risks?
   1. Have senior staff participated in a cybersecurity exercise?

## Senior Leaders

1. As a leader in <state/county/municipality> what cybersecurity resilience goals have you set?
2. What cybersecurity training is required for senior leadership?
3. What is your role during a cyber incident?
4. What information do you need to support your decision-making process?
5. What are the gaps in your cybersecurity workforce?
6. How does your <state/county/municipality> recruit, develop, and retain cybersecurity staff?

## Public Information

* + - 1. What training is provided to employees regarding reporting any contact with the media to the appropriate public information personnel?
      2. How do you build and maintain trust with the public?

## Legal

1. What is the role of the legal department during a cyber incident?
2. What legal issues need to be addressed based on the scenario?
3. What legal documentation should <state/county/municipality> have for cyber incidents?

# Appendix B: Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| AI | Artificial Intelligence |
| CIRP | Cybersecurity Incident Response Plan |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CPG | Cross-Sector Cybersecurity Performance Goals |
| DDoS | Distributed Denial of Service |
| EI-ISAC | Elections Infrastructure Information Sharing and Analysis Center |
| FBI | Federal Bureau of Investigation |
| IT | Information Technology |
| NIST | National Institute of Standards and Technology |
| PII | Personally Identifiable Information |
| TLP | Traffic Light Protocol |
| URL | Uniform Resource Locator |
| ZTA | Zero Trust Architecture |

# Appendix C: Case Studies

## DDoS Attacks Against State and County Election Systems

Multiple United States counties were targets of DDoS attacks during the 2022 election cycle, with many of the attacks impacting Election Day. Mississippi suffered a statewide DDoS attack which disrupted their elections website and other state websites. The elections website was offline several times throughout Election Day due to increased traffic that overwhelmed the system.[[16]](#footnote-17) An Illinois county suffered a similar DDoS attack that aimed to impact county websites and computer server performance.[[17]](#footnote-18) Malicious actors targeted a third-party vendor, causing connectivity and performance issues on elections-related servers. While Election Day voting processes were slowed, they did not stop completely. No data or information was compromised, and elections remained secure.[[18]](#footnote-19) In both cases, state and county clerk's offices had been repelling repeated attempted DDoS attacks against elections related infrastructure prior to the election day incident.

## Voter Registration Spear Phishing Campaign

In October 2020, a voter registration ‘error’ phishing campaign conveyed to recipients that their voter registration applications were incomplete, luring them into sharing Social Security Numbers, driver license data, and other Personally Identifiable Information (PII) with threat actors. The fraudulent emails sent in this campaign appeared to come from the U.S. Election Assistance Commission and contained a malicious uniform resource locator (URL) leading to a spoofed web page that harvested PII. The page was designed to appear legitimate and included images pulled from the official state website.[[19]](#footnote-20)

# Appendix D: Malicious Activity

## Distributed Denial of Service

Distributed Denial of Service (DDoS) attacks overload bandwidth and connection limits of hosts or networking equipment, specifically through a network of devices (e.g., computers, cellphones, Internet of Things, etc.) making excessive connection requests. DDoS attacks unfold in stages. First, a malicious actor infects a computer with malware that spreads across a network. This infected computer is known as the “master” because it controls any subsequent devices that become infected. The other infected devices, known as “bots” or “zombies” carry out the actual attack and create what is known as a “botnet”. The “bots” receive a command from the “master” which includes the address of the target. Extremely high volumes (floods) of data are sent to the target which slows down web server performance and prevents acceptance of legitimate network traffic. The cost of a DDoS attack can be severe loss of revenue or reputation to the victim.

The days just before, on, and immediately after Election Day are the most likely time for adversaries to launch DDoS attacks.[[20]](#footnote-21) Beyond voter information portals and registration sites that provide voters information about voting hours or where they can vote, prime DDoS targets include election night reporting websites and communications between boards of elections and polling locations.[[21]](#footnote-22) According to CISA and the FBI, while attacks on election infrastructure can hinder access to voting information, “the underlying data and internal systems would remain uncompromised, and anyone eligible to vote would still be able to cast a vote.”[[22]](#footnote-23)

### Additional Resources

* No Downtime In Elections: A Guide to Mitigating Risks of Denial of Service Attacks <https://www.cisa.gov/resources-tools/resources/no-downtime-elections-guide-mitigating-risks-denial-service>
* Understanding and Responding to Distributed Denial-of-Service Attacks

<https://www.cisa.gov/sites/default/files/publications/understanding-and-responding-to-ddos-attacks_508c.pdf>

* CISA Understanding Denial-of-Service Attacks <https://www.cisa.gov/news-events/news/understanding-denial-service-attacks>

## Social Engineering and Phishing

One of the most prominent tactics attackers use to exploit network and system vulnerabilities is social engineering, the manipulation of users through human interaction and the formation of trust and confidence to compromise proprietary information. Techniques for uncovering this information largely involve the use of phishing. Phishing attacks use email, text messaging, and/or malicious websites to solicit personal information or to trick individuals into downloading malicious software. Social engineering is effective for breaching networks, evading intrusion detection systems without leaving a log trail and is completely dependent on the operating system platform. While technical exploits aim to bypass security software, social engineering exploits are more difficult to guard against due to the human factor. Organizations should take steps towards strengthening employee cybersecurity awareness training, to include training personnel to be cautious of suspicious emails, providing instruction on where to forward them, and keeping software and systems up to date. Organizations can also implement software designed to safeguard sensitive information, detect unsafe URLs, block phishing websites, and detect known phishing and malware.

### Additional Resources

* Cybersecurity Toolkit and Resources to Protect Elections (<https://www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections>)
* Phishing Guidance: Stopping the Attack Cycle at Phase One (<https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one>)
* Avoiding Social Engineering and Phishing Attacks (<https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks>)

Appendix E: Contacts and Resources

Federal Government Contacts

* CISA (contact: [central@cisa.gov](mailto:central@cisa.gov), <https://www.cisa.gov>)
* United States Secret Service (USSS) Field Offices and Electronic Crimes Task Forces (ECTFs) (contact <https://www.secretservice.gov/contact/field-offices>, <https://www.secretservice.gov/investigation/cyber>)
* Federal Bureau of Investigation (FBI)
* Field Office Cyber Task Forces (contact: <https://www.fbi.gov/contact-us/field-offices>)
* Internet Crime Complain Center (IC3) (contact: [http://www.ic3.gov](http://www.ic3.gov/))
* National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center (contact: [cywatch@ic.fbi.gov](mailto:cywatch@ic.fbi.gov); 855-292-3937)

Preparedness Resources

* CISA Cross-sector Cybersecurity Performance Goals (<https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist>)
* NIST Cybersecurity Framework Tools ([<https://www.nist.gov/cyberframework>](https://www.nist.gov/cyberframework))
* CISA Cybersecurity Toolkit and Resources to Protect Elections (<https://www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections>)
* CISA Guide to Operational Security for Election Officials (<https://www.cisa.gov/resources-tools/resources/guide-operational-security-election-officials>)
* SLTT:
  + State and Local Cybersecurity Grant Program (<https://www.cisa.gov/state-and-local-cybersecurity-grant-program>)
  + CISA Continuous Diagnostics and Mitigation (CDM) Program (<https://www.cisa.gov/resources-tools/programs/continuous-diagnostics-and-mitigation-cdm-program>)
  + CISA Find Help Locally (<https://www.cisa.gov/audiences/find-help-locally>)
* Elections Infrastructure Information Sharing and Analysis Center (<https://www.cisecurity.org/ei-isac>)

State Level Resources

* Multi-State Information Sharing and Analysis Center (MS-ISAC) (contact: [info@msisac.org](mailto:info@msisac.org); 518-266-3460)
* National Governors Association (NGA) Resource Center for State Cybersecurity (<https://www.nga.org/statecyber/>)
* DHS Fusion Centers (<https://www.dhs.gov/state-and-major-urban-area-fusion-centers>)
* National Association of State Chief Information Officers (NASCIO) (<https://www.nascio.org/>)

Additional Resources

* InfraGard (<https://www.infragard.org/Files/InfraGard_Redesign_2-24-2022.pdf>)
* Internet Security Alliance (<https://isalliance.org/>)
* Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) (<https://www.isao.org/information-sharing-groups/>)
* International Association of Certified ISAOs ([http://www.certifiedisao.org](http://www.certifiedisao.org/); contact: [operations@certifiedisao.org](mailto:operations@certifiedisao.org))
* National Council of ISACs ([https://www.nationalisacs.org](https://www.nationalisacs.org/))

1. “Computer Security Resource Center Glossary: Cyber Resilience,” National Institute of Standards and Technology, accessed August 2, 2023, <https://csrc.nist.gov/glossary/term/cyber_resiliency>. [↑](#footnote-ref-2)
2. CISA Cybersecurity Alerts & Advisories, <https://www.cisa.gov/news-events/cybersecurity-advisories>. [↑](#footnote-ref-3)
3. NIST SP 800-53 Rev. 5.1.1 via NIST CPRT, “SC-5: Denial-of-service Protection,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=SC-05>. [↑](#footnote-ref-4)
4. NIST CSF 2.0 via CPRT, “ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.IM-04>. [↑](#footnote-ref-5)
5. NIST SP 800-53 Rev. 5.1.1 via NIST CPRT, “CP-02(08): Identify Critical Assets,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=CP-02>. [↑](#footnote-ref-6)
6. CISA Resources, “Zero Trust Maturity Model,” <https://www.cisa.gov/zero-trust-maturity-model> [↑](#footnote-ref-7)
7. NIST CSF 2.0 via CPRT, “PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.AT-01>. [↑](#footnote-ref-8)
8. NIST CSF 2.0 via CPRT, “PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.DS-01>. [↑](#footnote-ref-9)
9. NIST SP 800-53 Rev. 5.1.1 via NIST CPRT, “IR-2(3): Breach,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=IR-02>. [↑](#footnote-ref-10)
10. NIST SP 800-53 Rev. 5.1.1 via NIST CPRT, “ IR-4: Incident Handling,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=IR-04>. [↑](#footnote-ref-11)
11. NIST CSF 2.0 via NIST CPRT, “PR.IR-01: Networks and environments are protected from unauthorized logical access and usage,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.IR-01>. [↑](#footnote-ref-12)
12. NIST CSF 2.0 via NIST CPRT, “RC.RP: Incident Recovery Plan Execution,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=RC.RP>. [↑](#footnote-ref-13)
13. NIST CSF 2.0 via CPRT, “RS.MA: Incident Management,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=RS.MA>. [↑](#footnote-ref-14)
14. NIST CSF 2.0 via CPRT, “RC.RP: Incident Recovery Plan Execution,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=RC.RP>. [↑](#footnote-ref-15)
15. NIST CSF 2.0 via CPRT, “ID.IM: Improvement,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.IM>. [↑](#footnote-ref-16)
16. Nick Renyolds, “Mississippi Hit With Cyberattack After Russian Hackers Call for Strike,” Newsweek, November 9, 2022 <https://www.newsweek.com/mississippi-hit-cyberattack-after-russian-hackers-call-strike-1758094>. [↑](#footnote-ref-17)
17. Melissa Coyne, “Election 2022: Champaign County Clerk reports DDOS attacks slowed Election Day voting process - ABC7 Chicago,” ABC 7 Chicago, November 9, 2022, <https://abc7chicago.com/champaign-county-clerk-what-is-ddos-attack-meaning/12430547/>. [↑](#footnote-ref-18)
18. Chuck Goudie, “Champaign County Clerk reports cyber-attacks on servers,” WCIA, November 9, 2023, <https://www.wcia.com/news/champaign-county-clerk-reports-cyber-attacks-on-servers/>. [↑](#footnote-ref-19)
19. Catalin Cimpanu, “Phishing groups are collecting user data, email and banking passwords via fake voter registration forms,” ZDNET, October 23, 2020, <https://www.zdnet.com/article/phishing-groups-are-collecting-user-data-email-and-banking-passwords-via-fake-voter-registration-forms/>. [↑](#footnote-ref-20)
20. Tim Starks, “The lowly DDoS attack is still a viable threat for undermining elections” *Scoop News Group*, October 27, 2020, <https://www.cyberscoop.com/lowly-ddos-attack-still-viable-threat-undermining-elections/>. [↑](#footnote-ref-21)
21. Ibid. [↑](#footnote-ref-22)
22. FBI & CISA, “DDoS Attacks on Election Infrastructure Can Hinder Access to Voting Information, Would Not Prevent Voting,” September 30, 2020, <https://www.cisa.gov/sites/default/files/publications/PSA_DDoS_Final%20-%20CyD_508pobs.pdf>. [↑](#footnote-ref-23)