TLP:CLEAR

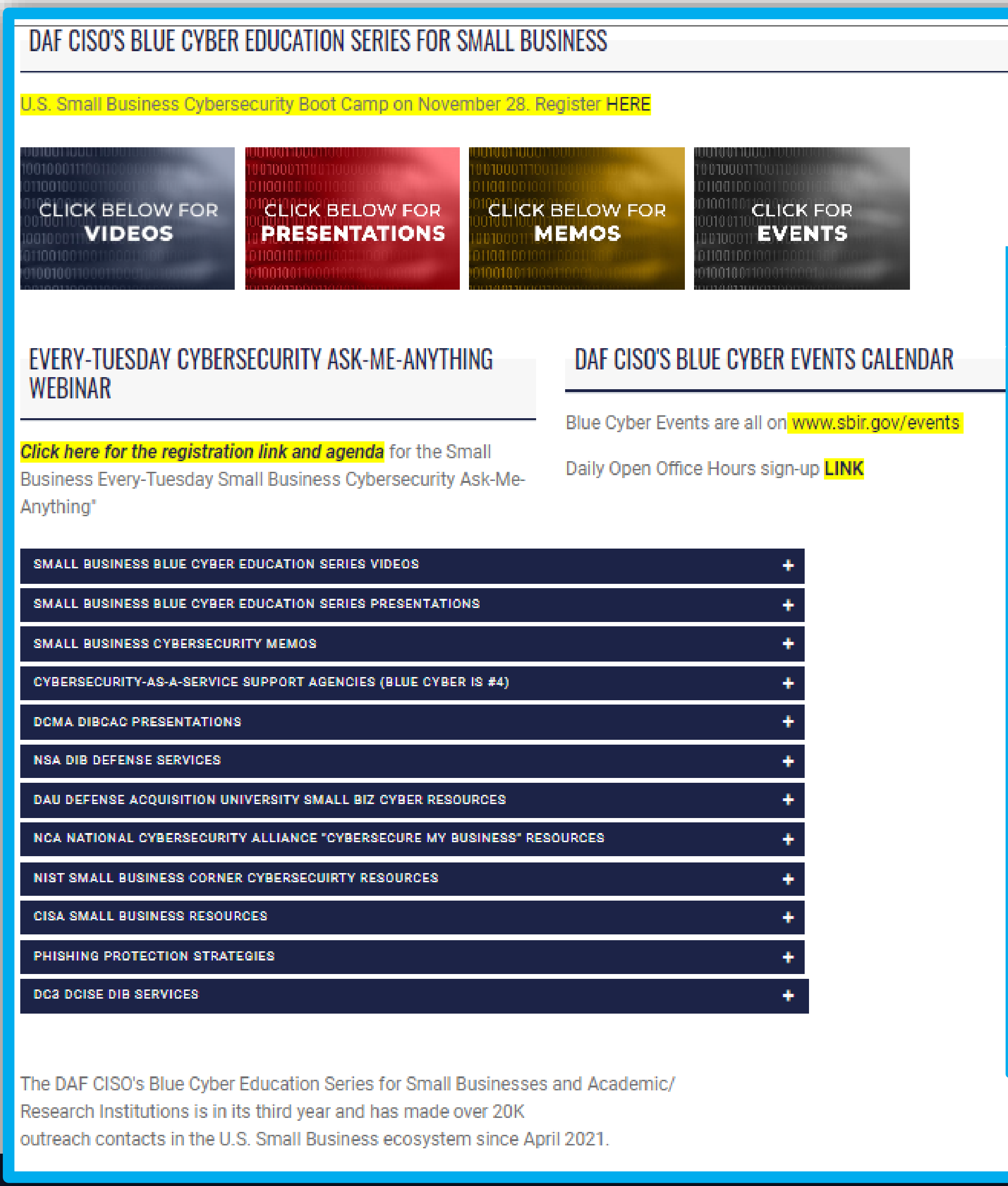
CISA

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

DAF CISO'S BLUE CYBER

Website
The Blue Cyber Education Series for Small Businesses webpage

Daily Office Hours
We have daily office hours for answering/researching your questions about Small Business cybersecurity and data protection!



DAF CISO'S BLUE CYBER EDUCATION SERIES FOR SMALL BUSINESS

U.S. Small Business Cybersecurity Boot Camp on November 28. Register HERE

CLICK BELOW FOR VIDEOS

CLICK BELOW FOR PRESENTATIONS

CLICK BELOW FOR MEMOS

CLICK FOR EVENTS

EVERY-TUESDAY CYBERSECURITY ASK-ME-ANYTHING WEBINAR

Click here for the registration link and agenda for the Small Business Every-Tuesday Small Business Cybersecurity Ask-Me-Anything"

DAF CISO'S BLUE CYBER EVENTS CALENDAR

Blue Cyber Events are all on www.sbir.gov/events

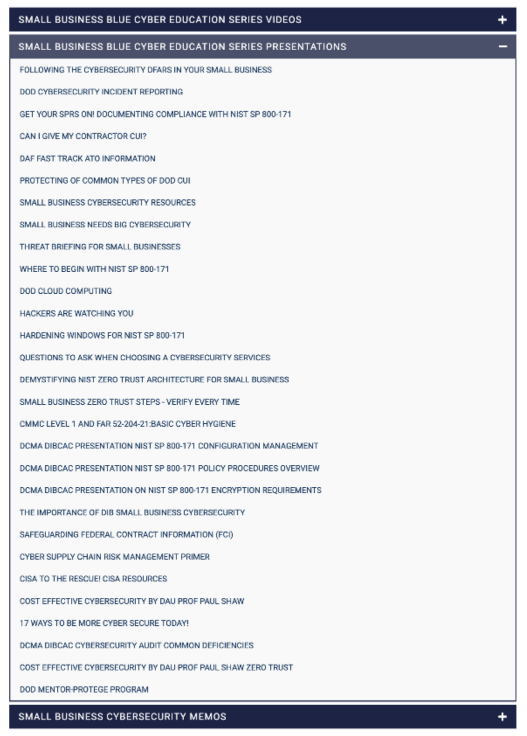
Daily Open Office Hours sign-up LINK

- SMALL BUSINESS BLUE CYBER EDUCATION SERIES VIDEOS +
- SMALL BUSINESS BLUE CYBER EDUCATION SERIES PRESENTATIONS +
- SMALL BUSINESS CYBERSECURITY MEMOS +
- CYBERSECURITY-AS-A-SERVICE SUPPORT AGENCIES (BLUE CYBER IS #4) +
- DCMA DIBCAC PRESENTATIONS +
- NSA DIB DEFENSE SERVICES +
- DAU DEFENSE ACQUISITION UNIVERSITY SMALL BIZ CYBER RESOURCES +
- NCA NATIONAL CYBERSECURITY ALLIANCE "CYBERSECURE MY BUSINESS" RESOURCES +
- NIST SMALL BUSINESS CORNER CYBERSECUIRTY RESOURCES +
- CISA SMALL BUSINESS RESOURCES +
- PHISHING PROTECTION STRATEGIES +
- DC3 DCISE DIB SERVICES +

The DAF CISO's Blue Cyber Education Series for Small Businesses and Academic/Research Institutions is in its third year and has made over 20K outreach contacts in the U.S. Small Business ecosystem since April 2021.

Events
All FREE and PUBLIC
www.sbir.gov/events

40 Presentations
Vides and PowerPoints



- SMALL BUSINESS BLUE CYBER EDUCATION SERIES VIDEOS +
- SMALL BUSINESS BLUE CYBER EDUCATION SERIES PRESENTATIONS –
  - FOLLOWING THE CYBERSECURITY DFARS IN YOUR SMALL BUSINESS
  - DOD CYBERSECURITY INCIDENT REPORTING
  - GET YOUR SPRS ON! DOCUMENTING COMPLIANCE WITH NIST SP 800-171
  - CAN I GIVE MY CONTRACTOR CUI?
  - DAF FAST TRACK ATO INFORMATION
  - PROTECTING OF COMMON TYPES OF DOD CUI
  - SMALL BUSINESS CYBERSECURITY RESOURCES
  - SMALL BUSINESS NEEDS BIG CYBERSECURITY
  - THREAT BRIEFING FOR SMALL BUSINESSES
  - WHERE TO BEGIN WITH NIST SP 800-171
  - DOD CLOUD COMPUTING
  - HACKERS ARE WATCHING YOU
  - HARDENING WINDOWS FOR NIST SP 800-171
  - QUESTIONS TO ASK WHEN CHOOSING A CYBERSECURITY SERVICES
  - DEMYSTIFYING NIST ZERO TRUST ARCHITECTURE FOR SMALL BUSINESS
  - SMALL BUSINESS ZERO TRUST STEPS - VERIFY EVERY TIME
  - CMMC LEVEL 1 AND FAR 52-204-21:BASIC CYBER HYGIENE
  - DCMA DIBCAC PRESENTATION NIST SP 800-171 CONFIGURATION MANAGEMENT
  - DCMA DIBCAC PRESENTATION NIST SP 800-171 POLICY PROCEDURES OVERVIEW
  - DCMA DIBCAC PRESENTATION ON NIST SP 800-171 ENCRYPTION REQUIREMENTS
  - THE IMPORTANCE OF DIB SMALL BUSINESS CYBERSECURITY
  - SAFEGUARDING FEDERAL CONTRACT INFORMATION (FCI)
  - CYBER SUPPLY CHAIN RISK MANAGEMENT PRIMER
  - CISA TO THE RESCUE! CISA RESOURCES
  - COST EFFECTIVE CYBERSECURITY BY DAU PROF PAUL SHAW
  - 17 WAYS TO BE MORE CYBER SECURE TODAY!
  - DCMA DIBCAC CYBERSECURITY AUDIT COMMON DEFICIENCIES
  - COST EFFECTIVE CYBERSECURITY BY DAU PROF PAUL SHAW ZERO TRUST
  - DOD MENTOR-PROTEGE PROGRAM
- SMALL BUSINESS CYBERSECURITY MEMOS +

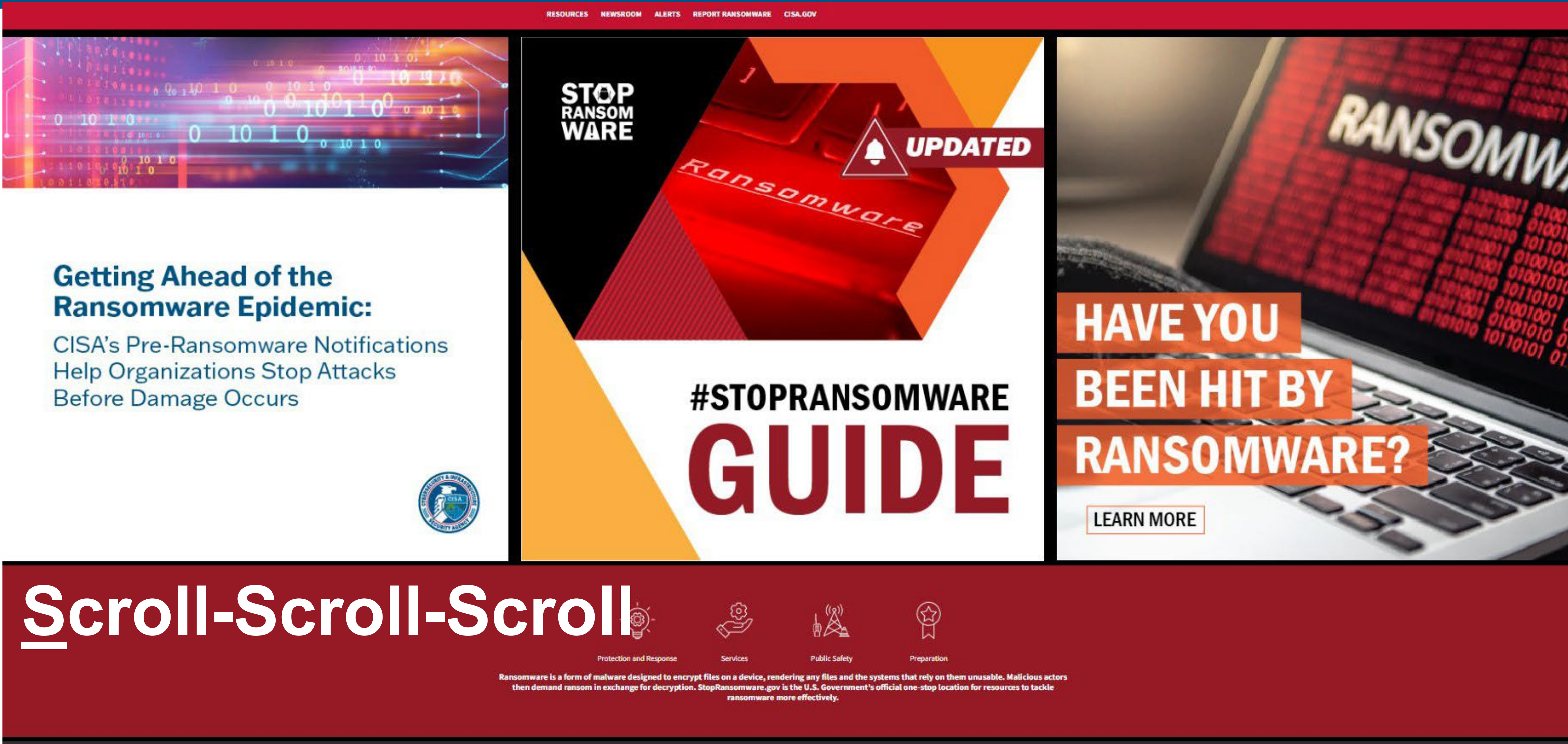
Distribution Statement A: Approved for public release. Distribution is unlimited. Case Number: AFRL-2023-5484, 31 October 2023.

Cybersecurity and Infrastructure Security Agency (CISA)

As America's Cyber Defense Agency and the National Coordinator for critical infrastructure resiliency and security, CISA leads the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day.

TLP:CLEAR

https://www.cisa.gov/stopransomware



Getting Ahead of the Ransomware Epidemic:
CISA's Pre-Ransomware Notifications Help Organizations Stop Attacks Before Damage Occurs

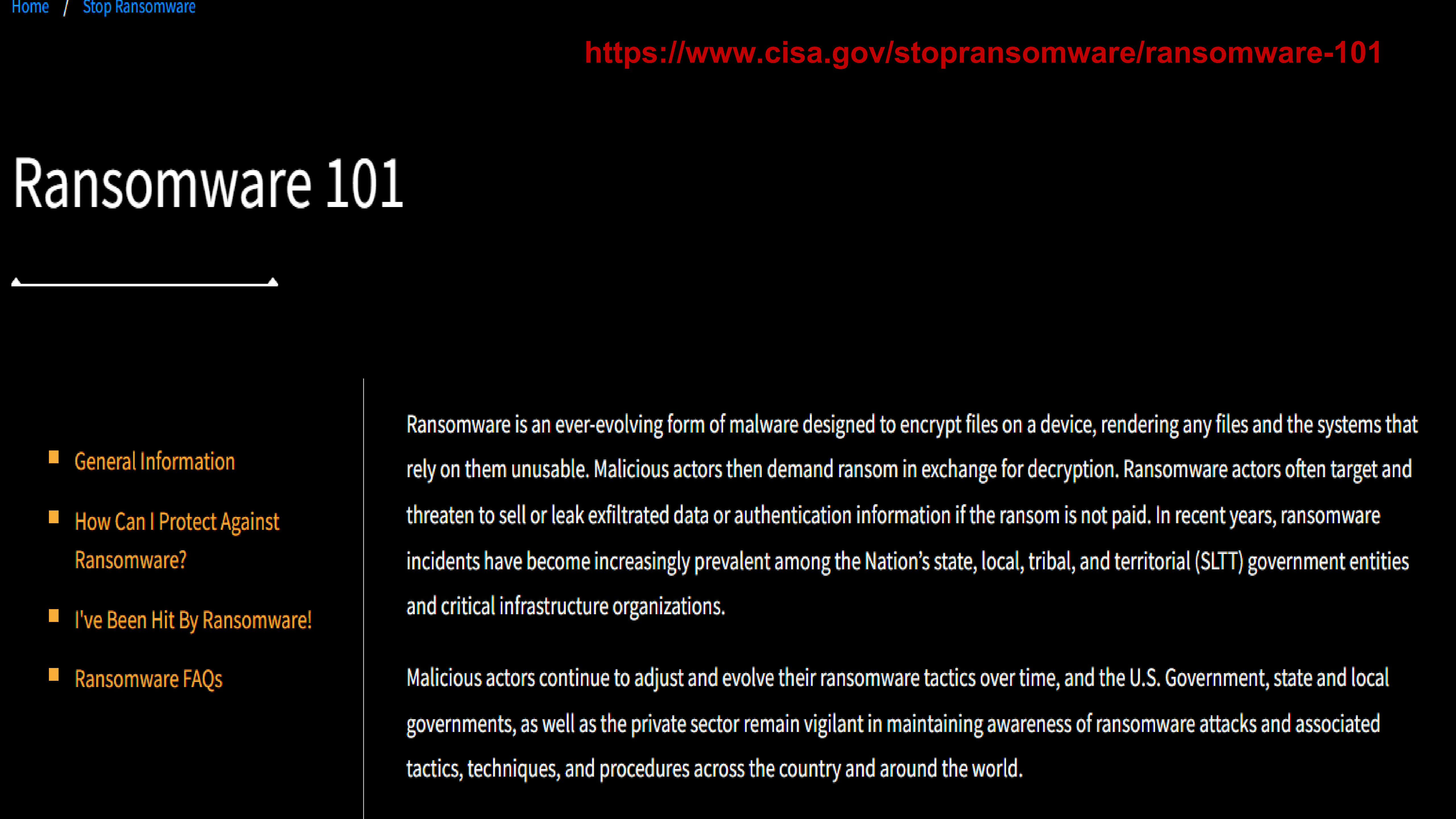
#STOPRANSOMWARE GUIDE

HAVE YOU BEEN HIT BY RANSOMWARE?

Ransomware is a form of malware 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. StopRansomware.gov is the U.S. Government's official one-stop location for resources to tackle ransomware more effectively.

Scroll-Scroll-Scroll

https://www.cisa.gov/stopransomware/ransomware-101



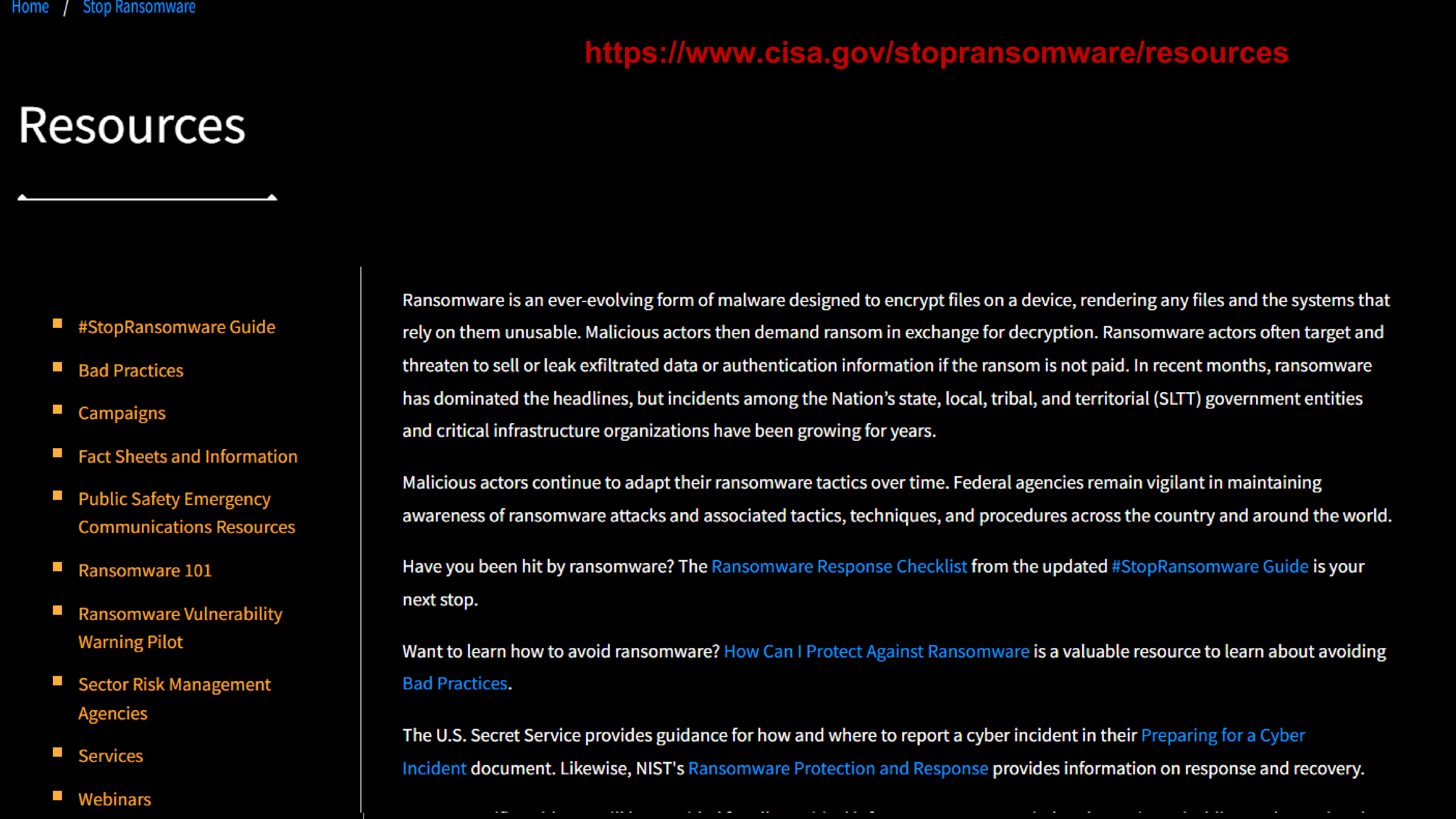
Home / Stop Ransomware

Ransomware 101

- General Information
- How Can I Protect Against Ransomware?
- I've Been Hit By Ransomware!
- Ransomware FAQs

Ransomware is an ever-evolving form of malware 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. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. In recent years, ransomware incidents have become increasingly prevalent among the Nation's state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations.

Malicious actors continue to adjust and evolve their ransomware tactics over time, and the U.S. Government, state and local governments, as well as the private sector remain vigilant in maintaining awareness of ransomware attacks and associated tactics, techniques, and procedures across the country and around the world.



Home / Stop Ransomware

https://www.cisa.gov/stopransomware/resources

Resources

- #StopRansomware Guide
- Bad Practices
- Campaigns
- Fact Sheets and Information
- Public Safety Emergency Communications Resources
- Ransomware 101
- Ransomware Vulnerability Warning Pilot
- Sector Risk Management Agencies
- Services
- Webinars

Ransomware is an ever-evolving form of malware 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. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. In recent months, ransomware has dominated the headlines, but incidents among the Nation's state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations have been growing for years.

Malicious actors continue to adapt their ransomware tactics over time. Federal agencies remain vigilant in maintaining awareness of ransomware attacks and associated tactics, techniques, and procedures across the country and around the world.

Have you been hit by ransomware? The Ransomware Response Checklist from the updated #StopRansomware Guide is your next stop.

Want to learn how to avoid ransomware? How Can I Protect Against Ransomware is a valuable resource to learn about avoiding Bad Practices.

The U.S. Secret Service provides guidance for how and where to report a cyber incident in their Preparing for a Cyber Incident document. Likewise, NIST's Ransomware Protection and Response provides information on response and recovery.

TLP:CLEAR

Ransomware Vulnerability Warning Pilot (RVWP)

- The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), signed into law in March 2022, required CISA to establish the RVWP
- CISA accomplishes this work by leveraging its existing services, data sources, technologies, and authorities, including
  - CISA's Cyber Hygiene Vulnerability Scanning service
  - Administrative Subpoena Authority
- CISA Regional staff members, located throughout the country, make notifications and may provide resources to mitigate the vulnerability.

https://www.cisa.gov/stopransomware/Ransomware-Vulnerability-Warning-Pilot

TLP:CLEAR

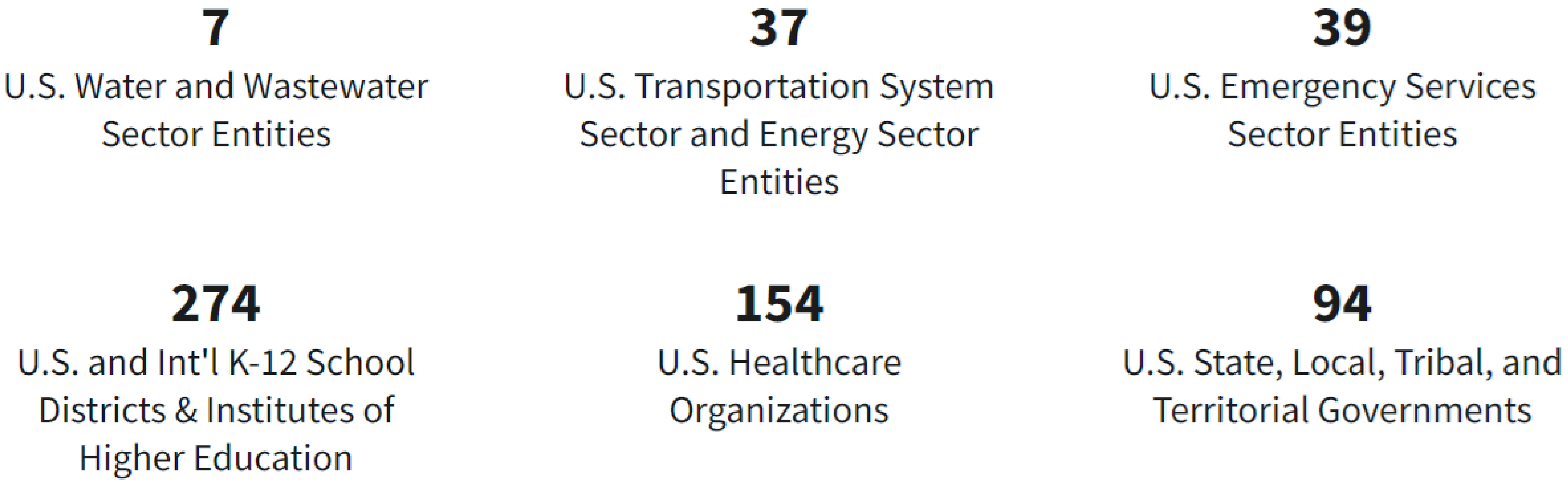
Ransomware Vulnerability Warning Pilot (RVWP)

- In 2023, CISA conducted more than 1,700 notifications to various organizations about open vulnerabilities on their networks that are specifically exploited by ransomware actors
- If you receive a notification, you can verify the identity of the CISA personnel through CISA Central: Central@cisa.gov or (888) 282-0870.

https://www.cisa.gov/stopransomware/Ransomware-Vulnerability-Warning-Pilot

2023 Pre-Ransomware Notifications

In 2023, CISA conducted more than 1200 pre-ransomware notifications to include:



7
U.S. Water and Wastewater Sector Entities

37
U.S. Transportation System Sector and Energy Sector Entities

39
U.S. Emergency Services Sector Entities

274
U.S. and Int'l K-12 School Districts & Institutes of Higher Education

154
U.S. Healthcare Organizations

94
U.S. State, Local, Tribal, and Territorial Governments

Driven by the cybersecurity research community, infrastructure providers, and cyber threat intelligence companies about potential early-stage ransomware activity.

https://www.cisa.gov/about/2023YIR

All CISA services and resources can be found by visiting www.CISA.gov

Questions?

Central@CISA.GOV
888-282-0870

Or

https://www.cisa.gov/about/regions

Or

Joseph "JD" Henry
Cybersecurity Advisor
Joseph.Henry@cisa.dhs.gov

Ransomware Protection and Response FROM NIST

https://csrc.nist.gov/Projects/ransomware-protection-and-response

Tips and tactics for **preparing your organization** for ransomware attacks are here!

- *Video: Protecting Your Small Business--Ransomware*
- *Fact sheet: How do I stay prepared?*
- *Infographic: Quick steps you can take **now***
- *Video: Tips to Help Your Company Protect Against Ransomware Attacks*

Thanks for helping shape our ransomware guidance!

- We've published the final NISTIR 8374,
- ***Ransomware Risk Management: A Cybersecurity Framework Profile*** and the
- ***Quick Start Guide**: Getting Started with Cybersecurity Risk Management | Ransomware*.
- Thanks for attending our ***July 14th Virtual Workshop** on Preventing and Recovering from Ransomware and Other Destructive Cyber Events*. *Please watch the recording HERE.*

Ransomware Protection and Response FROM NIST

https://csrc.nist.gov/Projects/ransomware-protection-and-response

- Cybersecurity resources for **small businesses**:
  Small Business Cybersecurity Corner
  Video: Protecting Your Small Business—Ransomware

- ***Protecting*** *the security of* ***business information and devices****:*
  Securing Data & Devices

- ***Preventing and recovering from*** *cybersecurity* ***incidents****:*
  Responding to a Cyber Incident

- In-depth information on **protecting data** against ransomware:
  Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events (SP 1800-25)

- **Preventing ransomware** and other malware **incidents**:
  Guide to Malware Incident Prevention and Handling for Desktops and Laptops (SP 800-83 Rev. 1)

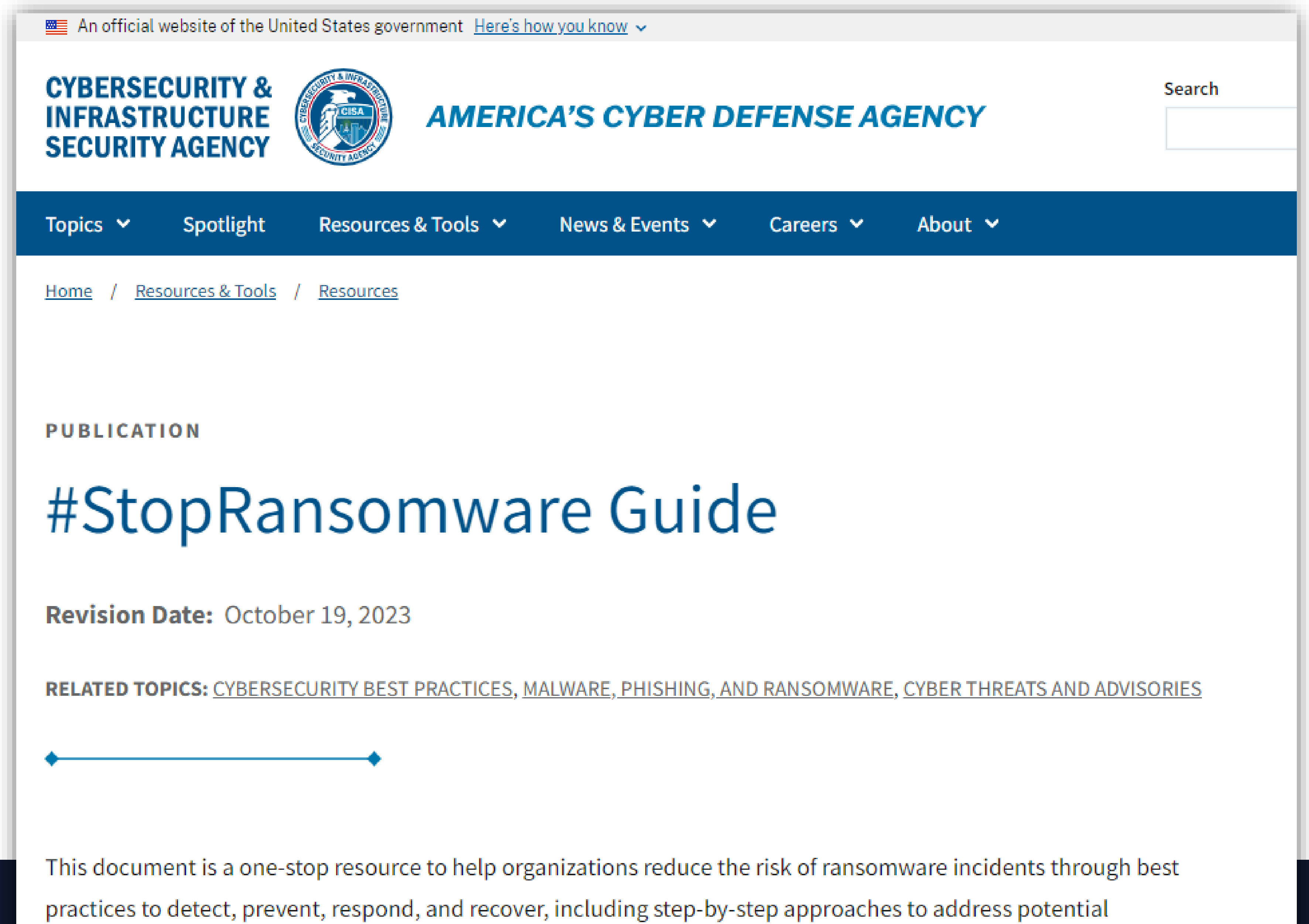
- Improving the security of **telework**, **remote access**, and **bring-your-own-device (BYOD)** technologies:
  Telework: Working Anytime, Anywhere
  Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security (SP 800-46 Rev. 2)

- **Patching software** to eliminate vulnerabilities:
  Guide to Enterprise Patch Management Technologies (SP 800-40 Rev. 3)
  Critical Cybersecurity Hygiene: Patching the Enterprise project

- **Using application control technology** to prevent ransomware execution:
  Guide to Application Whitelisting (SP 800-167)

- In-depth information on **detecting and responding** to ransomware attacks:
  Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events (SP 1800-26)

https://www.cisa.gov/resourcestools/resources/stopransomware-guide


An official website of the United States government Here's how you know
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
AMERICA'S CYBER DEFENSE AGENCY
Search
Topics
Spotlight
Resources & Tools
News & Events
Careers
About
Home / Resources & Tools / Resources

PUBLICATION

#StopRansomware Guide

Revision Date: October 19, 2023

RELATED TOPICS: CYBERSECURITY BEST PRACTICES, MALWARE, PHISHING, AND RANSOMWARE, CYBER THREATS AND ADVISORIES

This document is a one-stop resource to help organizations reduce the risk of ransomware incidents through best practices to detect, prevent, respond, and recover, including step-by-step approaches to address potential