U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

We lead the National effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent threats and hazards

seconds | days | weeks

GOAL 2

SECURE TOMORROW

Strengthen critical infrastructure and address long-term risks

months | years | decades

Shields Up - cisa.gov/shields-up

- Russia's invasion of Ukraine could impact organizations both within and beyond the region, to include malicious cyber activity against the U.S. homeland, including as a response to the unprecedented economic costs imposed on Russia by the U.S. and our allies and partners.
- Evolving intelligence indicates that the Russian Government is exploring options for potential cyberattacks.
- Every organization—large and small—must be prepared to respond to disruptive cyber incidents.

Shields Up - cisa.gov/shields-up

- As the nation's cyber defense agency, CISA stands ready to help organizations prepare for, respond to, and mitigate the impact of cyberattacks.
- When cyber incidents are reported quickly, we can use this information to render assistance and as warning to prevent other organizations and entities from falling victim to a similar attack.
- Organizations should report anomalous cyber activity and/or cyber incidents 24/7 to report@cisa.gov or (888) 282-0870.

Shields Up - cisa.gov/shields-up

- CISA recommends all organizations—regardless of size—adopt a heightened posture when it comes to cybersecurity and protecting their most critical assets.
- **Shields Up Guidance for All Organizations**
  - Reduce the likelihood of a damaging cyber intrusion
  - Take steps to quickly detect a potential intrusion
  - Ensure that the organization is prepared to respond if an intrusion occurs
  - Maximize the organization's resilience to a destructive cyber incident

Shields Up - cisa.gov/shields-up

- Corporate leaders have an important role to play in ensuring that their organization adopts a heightened security posture.
- **Recommendations for Corporate Leaders and CEOs**
  - Empower Chief Information Security Officers (CISO)
  - Lower Reporting Thresholds
  - Participate in a Test of Response Plans
  - Focus on Continuity
  - Plan for the Worst

Shields Up - cisa.gov/shields-up

- **Ransomware Response**
  - Determine which systems were impacted, and immediately isolate them.
  - Only in the event you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection.
  - Triage impacted systems.
  - Develop and document an initial understanding.
  - Engage your internal and external teams.
  - Take a system image and memory capture of a sample of affected devices.
  - Consult federal law enforcement regarding possible decryptors.

Shields Up - cisa.gov/shields-up

- **Steps You Can Take To Protect Yourself & Your Family**
  - Implement multi-factor authentication on your accounts.
  - Update your software. In fact, turn on automatic updates.
  - Think before you click.
  - Use strong passwords, and ideally a password manager to generate and store unique passwords.

Shields Up - cisa.gov/shields-up

- **Additional Resources**
  - Free Cybersecurity Services and Tools
  - Known Exploited Vulnerabilities Catalog
  - Cybersecurity Advisories
  - Cyber Essentials Toolkits
  - Cyber Hygiene and Web Scanning Services
  - Mis-, Dis-, and Malinformation Resources
  - Emergency Communications Resources

For more information:
www.cisa.gov
www.cisa.gov/shields-up

Questions?
CISARegion5@hq.dhs.gov


CYBERSECURITY & INFRASTRUCTURE
SECURITY AGENCY
CISA