Ransomware works

- **Who:** Ransomware is a threat vector that is rife for bad actors, both criminal enterprises and nation-states have made use of ransomware.
- **What:** Ransomware is a type of malware that encrypts the files on a user's device or a network's storage devices.
- **Where:** Top three targeted groups: (1) Municipalities, (2) schools, (3) hospitals. Clearly hitting the underrepresented/more vulnerable.
- **When:** Timing has seemed opportunistic, not strategic
- **Why:** Ransomware is a business model that works, victims are paying higher and higher ransoms. The willingness for victims and their insurers to pay out incentivize further use of ransomware.
- **How:** Ransomware-as-a-service kits mean nearly anyone can try their hand at a running a scam. Decades of lack of investment in IT, and a focus on systems operating more than system security, has left organizations across the country vulnerable to attack by ransomware actors.
Very Familiar Guidance

- Start with good cyber hygiene

**Prevent It**

Vulnerabilities: The Technical and The People

- Always be patching.
- Educate on phishing.
- Don’t rely on people, authenticate inbound email to prevent receipt of spoofed emails.
- Filter executable files from reaching end users

**Contain It**

- Segment your networks; make it hard for the bad guy to move around and infect multiple systems
- Limit access - Apply the principle of least privilege to all systems and services.
- Enforce access controls - Multi-factor
- Restricting user and third-party permissions to install and run software applications can help prevent malware from executing and spreading.

**Plan to Recover**

- Ask for help! Contact CISA, the FBI, or the Secret Service
- Work with an experienced advisor to help recover from a cyber attack
- Know your system’s baseline for recovery
- Review disaster recovery procedures and validate goals with executives
# CISA’s support

## Know your vulnerabilities
- Proactive Vulnerability Scanning
- Remote Penetration Testing

## Educate to protect your people
- Phishing Campaign Assessments
- CISA Trainings

## If it happens...
- Incident Response
- Technical Expertise

---

**No cost, just ask…**  
[CIOCC@CISA.dhs.gov](mailto:CIOCC@CISA.dhs.gov)  
(888)282-0870
Before Their Problem Becomes Yours

- Attackers looking to increase their likelihood of receiving payment want to spread to as many victims as possible.
- Managed Service Providers have been targeted to both exploit and propagate ransomware.
- Know who has access to your systems, and what actions they’re authorized to take.
- We’ve seen State and local governments enable MSPs to have persistent access and sweeping administrative privileges. If the MSP is hit with ransomware, there’s a high risk of their compromise.
Geoff Hale
Director, Election Security Initiative
Department of Homeland Security
Geoffrey.Hale@hq.dhs.gov