if you SEE SAY SOMETHING® SOMETHING CYBER

NEW YORK STATE | Counter Terrorism | Cyber Incident Response Team

Kathy Hochul
Governor

Ransomware

Ransomware is a type of malware that prevents users from accessing their system or personal files and demands a ransom payment in order to regain access.

Ransomware is most commonly delivered through phishing emails. Phishing emails often appear as though they have been sent from a legitimate organization or someone known to the victim and entice the user to click on a malicious link or open a malicious attachment.

Most common types of ransomware:

- **Scareware -** This is often disguised as a security software or tech support scam. You might receive a pop-up message claiming that malware was discovered and the only way to remove it is to download their software or to pay the ransom. A legitimate cybersecurity software program would not solicit customers in this manner.
- **Screen Locker -** This ransomware revokes the access to use your computer entirely. A screen will typically appear and display an official-looking law enforcement or authoritative agency logo or seal stating that illegal activity has been detected on your computer and you must pay a fine.
- **Encrypting Ransomware -** Cybercriminals use encryption algorithms that prohibit you from accessing your files. They demand a payment in order to decrypt your files or give you the decryption key.

Tips on avoiding and recovering from ransomware attacks:

- Use strong passwords that are easy to remember but hard to guess
- Keep all software up-to-date
- Frequently run security scans
- Think twice before clicking on unusual links
- Refrain from opening attachments that look suspicious
- Regularly back up your data to a device that is disconnected from computers and networks when not in use

If you find yourself infected with ransomware, NEVER pay the ransom. Paying the ransom doesn't guarantee that you will get your data back, but it does encourage cybercriminals to launch additional attacks in the future.

If you suspect a cyber incident, immediately contact:

CIRT is an initiative of the New York State Division of Homeland Security and Emergency Services.
For additional information, visit dhses.ny.gov/cyber-incident-response-team