Ransomware

What it is & How to prevent it

What is Ransomware?

Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or when users unknowingly visit an infected website.

Ransomware can be devastating to an individual or an organization. Anyone with important data stored on their computer or network is at risk, including universities, government, law enforcement agencies, healthcare systems, or other critical infrastructure entities. Recovery can be a difficult process that may require the services of a reputable data recovery specialist, and some victims pay to recover their files. Paying ransoms is not recommended, and there is no guarantee that individuals will recover their files if they pay the ransom.

The best way to prevent an infection is to not rely on only one solution, but to use multiple, layered solutions for the best possible protection:

- Update software and operating systems with the latest patches. Outdated applications and operating systems are the target of most attacks.
- Use a top-notch, up-to-date antivirus software, or more advanced endpoint protection.
- Never click on links or open attachments in unsolicited emails.
- Backup data regularly. Keep them on a separate device and store them offline. Regularly test the recovery function of your backup/restore procedure.
- Follow safe practices when browsing the Internet. Read Good Security Habits for additional details.

We also recommend employing the following best practices:

- Implement effective security awareness training to educate users on what to watch for to prevent ransomware applications from being downloaded/executed.
- Restrict users' permissions to install and run software applications, and apply the principle of least privilege (POLP) to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through a network.
- Use application whitelisting to allow only approved programs to run on a network.

- Ensure everyone in your organization is using top-notch, up-to-date antivirus software, or more advanced endpoint protection products like whitelisting and/or real-time executable blocking.
- Configure firewalls to block access to known malicious IP addresses.

For more information, review the following ransomware prevention resources:

- Ransomware Security Publication
- How to Protect Your Networks from Ransomware
- https://security.ucsb.edu
- Social media: #ransomUCinfosec

Adapted from Department of Homeland Security - CISA