Office of the Chief Information Security Officer
Risk Advisory: Malware and Ransomware

Ransomware is a type of malware (malicious software) that cybercriminals use to infect computers, devices, and networks, and restrict access to data until a sum of money is paid. Ransomware attacks have impacted businesses, hospitals, and public utilities worldwide.

In Sophos' 2021 State of Ransomware Report, it was reported that the average ransomware recovery costs for businesses more than doubled, rising from $761,106 in 2020 to $1.85 million in 2021. Besides the ransom payment, calculated costs include downtime, salaries, device and network costs, lost opportunity, and other associated financial loss.

Methods for avoiding ransomware attacks are consistent with best practices typically recommended for securing and protecting personal and UW institutional data.

How does a ransomware infection occur?

Ransomware is typically spread via phishing emails that contain links to malicious web pages or attachments. Infection can also occur through "drive-by" downloading, which occurs when a user visits an infected website, and malware is downloaded and installed without the user's knowledge.

If the ransomware is successful, files are locked through a process known as "encryption," which generates a "key," and an on-screen ransom note offers the decryption key in exchange for payment. Ransom varies greatly but is and typically must be paid in virtual currency, such as bitcoins.

In some cases, decryption tools are developed and made available online, but there is no guarantee for their efficacy for unlocking any of the many strains of ransomware.

How does it spread and what is the impact?

Infections on one machine may migrate to network drives; additionally, vulnerable web servers may be exploited directly by cybercriminals to deliver ransomware and other forms of malware to multiple users in an organization. The potential consequences of infection in computers, systems, and on the University network may include:

- Inaccessibility of personal or UW data, either permanently or temporarily,
- Disruption of business or organizational operations, and any associated financial loss,
- Lost money and/or time needed to restore systems and files, and
- Reputational harm to the unit, department, or the University.

The decryption key is not always delivered, so victims could lose data, money, and time if the ransom is paid. Cybercriminals may receive the victim's money, and in some cases, their banking information, but there is no guarantee that the key will be delivered and data restored. Additionally, restored files might contain other forms of malware, and victims who pay ransom once could be vulnerable to repeated attacks

What to do

- Make sure you have the latest anti-virus updates on your machine.
- Keep your operating system updated and patched.
- Back up your data regularly, making sure you have at least one backup that is not attached to your computer.
- Don't click on links in email.
- Don't download unexpected email attachments, and scan any attachments you absolutely must open with anti-virus software.

- Use strong passwords, and don’t reuse your UW NetID password on other accounts.
- Sophos anti-virus software for home use can be accessed here: https://itconnect.uw.edu/wares/uware/sophos-anti-virus-software/

This list is not exhaustive. For additional information, consult your department IT support person.

Resources

Ransomware Recovery Cost Reaches Nearly $2 Million, More Than Doubling in a Year, Sophos Survey Shows

CISO online training: Ransomware

Phishing Online Educational Resources for UW
https://ciso.uw.edu/education/#phishing

Infographics: Phishing, Malware, and Ransomware
https://ciso.uw.edu/education/infographics/

Online Learning: Malware, Phishing, and Other Topics:
https://ciso.uw.edu/education/online-training/

Risk Advisories and Best Practices for UW
https://ciso.uw.edu/resources/risk-advisories/

The No More Ransom Project
An initiative between police and IT security companies to disrupt ransomware-related cybercrime
https://www.nomoreransom.org/

CISA Ransomware page
https://www.us-cert.gov/Ransomware