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

## BACKGROUND

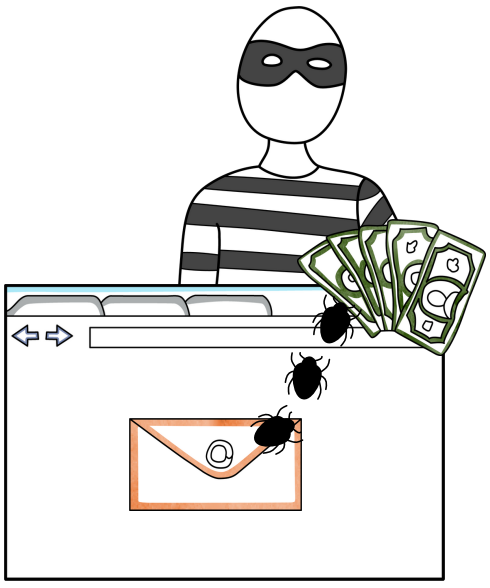
Malicious cyber-attacks dubbed "**WannaCry**" recently impacted businesses, hospitals, and public utilities worldwide. Heavy media coverage raised awareness about ransomware, a type of malware (malicious software) that cybercriminals use to infect computers, devices, and networks, and restrict access to data until a sum of money is paid.

WannaCry is a unique form of ransomware, as it integrates older threats into a new type of attack, combining the effectiveness of a phishing email with the capability of a **worm** so that it can spread automatically across a network.

While WannaCry is unusual in terms of its composition, geographical scope, and the widespread attention it garnered, methods for avoiding infection—for this form and for other forms of malware and ransomware—remain 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 frequently $300– $600 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.
- Make sure your operating system is 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.

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

- 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

## RESOURCES

Infographics: Phishing, Malware, and Ransomware

Microsoft Security Bulletin

National Cybersecurity Alliance Statement

Online Learning: Malware, Phishing, and Other Topics

Phishing Online Educational Resource

Risk Advisories and Best Practices for UW

The No More Ransom Project

"The Worm That Spreads WanaCrypt0r" A technical write-up of the threat

WannaCry Ransomware: What We Know Monday