

# Malware and spam: Ransomware

Last Modified on 08/04/2022 10:57 pm EDT

This article reviews **what ransomware is** and **how to protect yourself**.

## See also:

- [Malware & Spam: Email Phishing](#)

## What is ransomware?

Ransomware is a class of malicious software that holds your data hostage by blocking access and demanding payment. In some instances, the software may even threaten to leak your data unless you pay.

**Did you know?** Even if you do pay (which you should not), the bad actor will still keep your data and may continue to request additional payments.

## How can it infect your devices?

Commonly, infections come from successful phishing attempts in which the victim **downloads** or opens a **fraudulent attachment**. They can also occur when a victim **starts a download** from a fraudulent website.

## I think I'm compromised!

1. **Stop using** your device and **power it off** immediately
2. Contact the [Help Desk](#)


If you encounter this issue outside of Help Desk hours: do NOT turn on your device. Call the Help Desk when it opens or email [help@brynmawr.edu](mailto:help@brynmawr.edu) from a different device.

## How to prevent an infection

---

Links on **legitimate** websites can redirect you to a fraudulent website!**Always check the URL** before downloading.

Have **healthy information security** habits!

1. Be wary of fraudulent **emails**
2. **Only download** files from senders and websites you trust
  - Double-check the sender and URL
3. Run a **virus scan** every two weeks
4. Be adept at identifying and avoiding fraudulent emails and websites by completing your [Information Security Education program](#) 

## Questions?

If you have any additional questions or problems, don't hesitate to reach out to the **Help Desk!**

**Phone:** 610-526-7440 | [Library and Help Desk hours](#) 

**Email:** [help@brynmawr.edu](mailto:help@brynmawr.edu) | [Service catalog](#) 

**Location:** Canaday Library 1st floor

---