

Digital threats: Ransomware

Last Modified on 09/26/2025 12:32 am EDT

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

See also:

- [Digital threats: Doxxing](#)
- [Digital threats: Phishing and spam](#)
- [Information Security Education Program](#)

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.

Attention: Even if you do pay, **bad actors will often keep your data** and continue to request additional payments.



How it infects your device

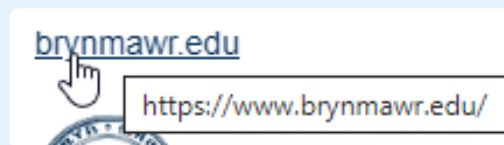
Infections most often occur when a victim downloads or opens a malicious file. The file can appear as an **attachment** to a [phishing email](#), a link in a **malicious text message**, or a download on a **fraudulent website**.

Preventing infections

Protect yourself with **healthy information security** habits!

1. Learn to identify [phishing and spam](#)
2. Only download files from senders and websites you know and trust
3. Install updated **antivirus software**
 - [College devices](#)
 - [Personal devices](#)
4. Stay up-to-date with our [Information Security Education Program](#)

Note: Even legitimate websites can redirect you to malicious ones. **Always check the URL** before clicking a link!



I think I'm compromised!

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

Attention: If you need help outside of Help Desk hours, **do not turn on your device**. Call the Help Desk when they open or email help@brynmawr.edu from a different device.

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 | [Service catalog](#) ☐

Location: Canaday Library 1st floor
