

How Ransomware Works

Ransomware is malware that holds your data and privacy hostage for money. Your small actions make a big difference in stopping ransomware attacks. Follow the steps to see how it works, and how your small actions can stop the attackers.

1

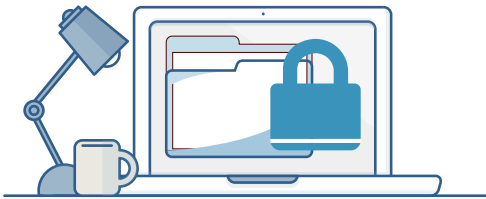


Cyber criminals send a phishing message with malware through a file attachment or link.

Click Wisely

When you receive an unexpected or out of the ordinary message, be suspicious. If the message came from someone you know, verify the message by calling or texting the sender to see if it's legit. If it's from a service or website, skip the link and go directly to the official page.

2

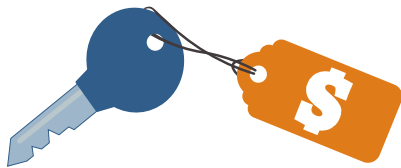


After clicking the link or opening the file, the malware uses security flaws in your computer to lock your data with a key you don't have.

Apply Updates

When you apply updates, your computer is not compatible with the cyber criminal's tool kits. The malware simply will not work.

3



Cyber criminals offer you the key to access your data in return for a ransom, paid in digital currency.

Know Your Data

When your data is backed up, you don't have to worry about paying a criminal for access to your pictures and files. A good backup protects you from all sources of data loss, from cyber attack and theft to everyday things like spilled coffee or a power surge.

No matter if you're at home or at Harvard, your small actions make a big difference to keeping yourself and the Harvard community secure.