RANSOMEWARE GUIDE

BU Information Services & Technology

BU Information Services & Technology

What is Ransomware

Ransomware is a type of malicious software (or malware) that encrypts all the files that someone has access to, making them unreadable. Once encrypted, the malware demands a payment (ransom) to release the files. Sometimes scammers threaten to release files to the public until that sum of money is paid. Ransomware is commonly introduced into a network through phishing, malicious attachments, or malicious downloads.

2020

30%

of U.S.-based cyberattacks were ransomware according to Verizon research

Ransomware targets individuals as well as organizations of all sizes. Ransomware attacks are becoming more common in the United States. They accounted for 30% of all U.S.-based cyberattacks reported to and confirmed by Verizon data breach researchers in 2020, more than double the rate for the world.

Why is it important for the BU community to be familiar with ransomware

Since higher education institutions store vast amounts data, including personal, financial, health, and research data, and have sizable budgets, they make ideal targets for ransomware attacks.

According to Microsoft Security Intelligence, higher education accounted for 62.8 percent of almost 9.4 million malware encounters reported during just the month of November in 2020.

What can we do to protect ourselves & our community from ransomware?

STARTS WITH YOU

There are several resources at Boston University to help reduce our risk. The first is you. Simply understanding what ransomware/malware is, is the first step toward protecting our data.

STARTS WITH PHISHING

Since we know that ransomware attacks can begin as phishing scams, such as software downloads through an attachment or via hyperlinks, it is essential to stop and think before opening an attachment or clicking on a link.

CROWDSTRIKE

The chances of infection can be significantly reduced by using antivirus or end point protection software such as Crowdstrike. Additionally, visit the BU Phishing Guide for a quick tutorial on how to spot a scam or the BU Phish Bowl to see some of the most reported phish circulating on our network and compare a phishy email you may have received.

Here are some tips to keep you safe from ransomware:

KEEP UP-TO-DATE

Keep all software up to date, including operating systems and applications. Set them to update automatically.

DOWNLOAD CROWDSTRIKE

To help protect yourself from ransomware, download Crowdstrike, it's free of charge for all students, faculty, and staff for their personal laptop or desktop computers. Note: If you're using a BU managed device, we're already protecting you!

USE MULTIFACTOR

Add multifactor authentication to your online accounts whenever possible.

REPORT IT

Contact the IT Help Center (or your college or department's local IT support) before taking any action if you find yourself victim to a ransomware scam: ithelp@bu.edu.

DON'T OPEN OR CLICK

Don't open unknown attachments or click on links before verifying them.

BACK UP YOUR DATA

Make it a point to back up you data on a regular basis to prevent data loss in the event of a ransomware attack.

BU Resources

Crowdstrike End Point Protection:
https://www.bu.edu/tech/services/cccs/desktop/device-security/endpoint-protection/

BU Phish Bowl:
https://www.bu.edu/tech/support/information-security/bus-phish-bowl/

Terrier Cybersecurity Checkup:
https://cybercheckup.bu.edu/

BU Phishing Guide:
https://www.bu.edu/tech/support/information-security/security-for-everyone/phishing/

Report Phishing to: abuse@bu.edu
Contact the IT Help Center:
617) 353-4357 ithelp@bu.edu

BU Information Services & Technology