

Major Keys to Ransomware Protection

Don't get locked out by ransomware.

Protect yourself with these quick tips so you don't pay!



Back-Up Your Files

Ransomware will look for files to encrypt or delete. Ensure all files are backed up to a secondary location like a secure cloud storage service or another storage media. This protection can make files inaccessible to edits or deletion by cybercriminals.



Keep Security Software Up to Date

Security software that is not up to date is an easy target for cybercriminals that try to infiltrate systems. Updates for these types of software are generally done to protect against new cyber threats.



Never Pay the Ransom!

Cybercriminals are always trying to deceive and take advantage of people. If you suspect you have fallen victim to a ransomware attack, make sure to disconnect any devices from your network and contact your organization's IT team immediately.



Only Use Secure Networks

Cybercriminals look for persons connected to unsecured Wi-Fi networks to track their internet usage. Using a verified and secure network will assist in adding a layer of protection.

