Cloud Destinations
Embrace Cloud Multiverse

Ransomware

What is Ransomware?

Ransomware is a type of malware (malicious software) that 'kidnaps' your business data and holds it hostage until you pay a ransom. Ransomware holds your data hostage by encrypting it and preventing access to it. If the ransom is paid, the decryption key is sent to you to decrypt and ideallyrecover your data. If the ransom is not paid, your data remains encrypted and unusable.

How Does Ransomware Get on Your System?

Ransomware typically enters your network through outdated software, or, more commonly, whenan employee responds to a phishing email by clicking on a link or opening an e-mail attachment containing malware.

Best Practices

Here are some ways you can help to defend against ransomware attacks.

- Recognize phishing emails. Don't open any attachments or click on any links in suspicious emails. Forward them to your IT department for verification. If you don't know how to recognize a phishing email – ask your IT department for help.
- If infected, IMMEDIATELY disconnect your computer from all networks and call your IT department.
- Always regularly back up business critical data and store backups disconnected from your network. You don't need to pay ransom if you have good backups!
- Keep all software on your computer up-to-date.