Ransomware Data Recovery

Trust DriveSavers to Recover Your Data from Ransomware

DriveSavers engineers have the in-depth knowledge and technical expertise that comes from over thirty years of data recovery experience, allowing us to achieve the highest success rate in the industry.

Using proprietary tools, techniques and knowhow, DriveSavers data recovery experts can circumvent ransomware or find data that has escaped full encryption.

We can ensure that no additional damage or malware access to your device will occur. We guarantee receipt of your data or no payment is due.

- No data, no charge
- Encryption experts
- Highest success rate in the industry
- No hidden fees
- Free evaluation
- Free shipping

Certified Secure

DriveSavers upholds the highest standards of privacy and security for protected information. Our strict security protocols satisfy the stringent requirements of the data loss prevention, security and privacy protocols mandated by:

- SOC 2 Type II
- HIPAA
- FERPA
- GLBA
- SOX
- NIST SP 800-34 Rev. 1

Restoring Data and Peace of Mind Since 1985

We know how devastating it is to lose personal or business data. DriveSavers is dedicated to doing all we can to help retrieve irreplaceable data.

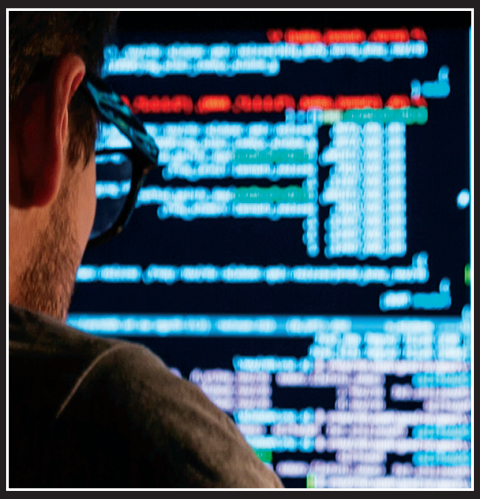
- 24/7 Customer Service
- Live U.S.-based advisors
- Toll-free Skype

We can save it!®

800.440.1904 · www.drivesavers.com

Call DriveSavers

800.440.1904



Ransomware Tips

Regularly Update Security Software

Hackers are always exploring computer security measures to find weaknesses and develop ways in. In reaction, security software manufacturers are constantly developing patches and software updates to eliminate threats as they are discovered.

- Keep up with software and operating system updates. Otherwise, known weaknesses remain like open doors inviting criminals into your computer.
- Identify what firewalls, anti-spam, antivirus, anti-malware and anti-spyware software you have installed and, always install updates as they are made available.

Prevention Tips

- Disable Remote Desktop or Terminal Services completely when not in use.
- Use IP address based restrictions to allow access to devices from trusted networks only.
- Watch out for malicious emails and phishing links. Don't open email from strangers. Be suspicious of any links or attachments from unknown sources.

Ransomware Recovery Tips

If you are a victim of ransomware, your first step is to take some time and look for backups, even those located on the affected drives. It's possible that they were not encrypted.

- DO NOT attach unaffected devices to a computer or other device that has been infected with ransomware, as the malicious program may spread and cause even bigger problems. Instead, use a different computer to look for your files on external drives, thumb drives and other devices that were not previously attached to your infected computer and may hold some of your irreplaceable files.
- DO NOT delete any files from a device infected with ransomware, whether the files are encrypted or not. The key to getting your data back could be anywhere.
- DO NOT reload your operating system. This may permanently delete all of your irreplaceable data, including photos, financial files and more.

Call DriveSavers—800.440.1904

- Free shipping
- Free evaluation
- No data, no charge