Ransomware Rescue

How to recognize and avoid a data hostage situation

Stay alert to ransomware—malware designed by cyberthieves to hold your computer or your data hostage until you pay a ransom.

Threats seem innocent when they arrive from seemingly trusted sources via:

Email

Internet downloads

PDFs

But one click can let an infection into your entire network.

Ransomware attacks:

63% of attacks required more than a business **day to fix**[1]

90% increase in ransomware detections among businesses in 2017[2]

11.5 billion USD is the estimated global cost of ransomware by 2019[3]

1. "International Study Finds Nearly 40 Percent of Enterprises Hit by Ransomware in the Last Year," Business Wire. https://www.businesswire.com/news/home/20160803005545/en/International-Study-Finds-40-Percent-Enterprises-Hit (accessed June 2018).
2. "Cybercrime Tactics and Techniques: 2017 State of Malware," Malwarebytes Labs. https://www.malwarebytes.com/pdf/white-papers/CTNT-Q4-17.pdf (accessed June 2018).
3. "Global Ransomware Damage Costs Predicted to Hit $11.5 Billion by 2019," Cyber Security Ventures. https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/ (accessed June 2018).

A ransomware infection means:

- Temporary or permanent data loss
- Little or no access to systems and applications
- Disruption to your regular operations
- Financial loss
- Harm to your organization's reputation

PROTECT YOURSELF AND YOUR COMPANY

Check emails carefully before opening

Safety checklist

- I know the sender of this email
- It makes sense that this was sent to me
- I can verify that the link or attached file is safe
- The email doesn't threaten to close my accounts or cancel my cards if I don't provide information
- When I hover over a link, the URL matches where I expect to go

YOUR RANSOMWARE PREVENTION KIT

Patch every device to keep up with antivirus and software updates.

Stick to trusted sites and watch out for scams (like "you're a winner!" banners). Also, be wary of email attachments, like bogus shipping receipts.

Back up all critical files often, preferably off-site. All onsite backups connected to your network are vulnerable.

Heed all warnings from your AV and report all alerts to your support team.

Close popups asking you to update account information or install applications you didn't request.

Bookmark your favorite web pages to avoid visiting a fake site due to a misspelling (gogle.com, for example).

If you think you've been infected, unplug your computer from the network and call your IT service provider immediately.

Fight Back Against Ransomware

SolarWinds MSP can arm you with the tools to help you tackle ransomware threats, including patch management, antivirus, mail protection, backup, and more.

solarwindsmsp.com/products