



Ransomware Rescue

How to recognize and avoid a data hostage situation



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

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



Email



Internet



PDF

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

16.2 days: the average amount of downtime businesses experienced at the end of **2023** due to ransomware attacks¹



1 business every 11 seconds: the predicted frequency a business will fall victim to a ransomware attack by **2024**



\$20 billion: the predicted cost of damages due to ransomware by **2024**



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 their organization's reputation

PROTECT YOUR BUSINESS AND YOUR CUSTOMERS

Check emails carefully before opening them

Safety checklist

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



YOUR RANSOMWARE PREVENTION KIT



Patch every device to keep up with security updates



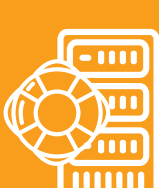
Ensure employees stick to trusted sites and watch out for scams (like "you're a winner!" banners)



Heed all warnings and act on alerts from your antivirus or endpoint detection and response solution



Advise employees to close popups asking them to update account information or install applications they didn't request



Back up all critical files often, preferably off-site—all on-site backups connected to the network are vulnerable



Ask employees to bookmark their favorite web pages to avoid visiting a fake site due to a misspelling (i.e., gogle.com)



Train employees to be wary of email attachments, like bogus shipping receipts

If you think your business has been infected, unplug their computer from the network before troubleshooting.

Fight Back Against Ransomware

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

We have the right solution for your business. Contact us to learn more. Contact sales@mindburnsolutions.com or call us @ 717.303.3309



<https://mindburn.solutions>