ENJOY SAFER TECHNOLOGY®

Protecting your organization from ransomware

Ransomware threats are increasing every year; get the facts and learn how to protect your business.

RANSOMWARE ON THE RISE

Ransomware damage costs will rise to $11.5 billion in 2019 and one business will fall victim to a ransomware attack every 14 seconds by that time.

—Cybersecurity Ventures Ransomware Damage Report, 2017

In a single year, the number of attacks on businesses nearly doubled, from 82,000 in 2016 to 159,000 in 2017.

—Online Trust Alliance (OTA)

More criminals are expected to shift to ransomware because they can now buy ready-made ransomware software from super hackers. These toolkits make it possible for anyone with basic computer skills to launch sophisticated attacks.

—NBCNews.com, 2017

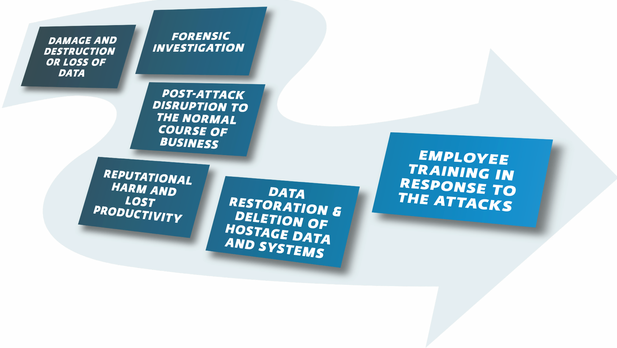
An IBM survey found that 70% of businesses infected with ransomware had paid a ransom to regain access to business data and systems. Half of those paid over $10,000 and 20 percent paid over $40,000.

—IBM Security, 2016

HOW RANSOMWARE COSTS ADD UP

Malware is often spread via email or by drive-by downloads from compromised websites or even via software updates. After it encrypts all your precious data, the ransomware generates a pop-up message asking you to pay.

HOW RANSOMWARE WORKS



⚠ WATCH OUT FOR PHISH

91% of cyberattacks start with a phishing email. The top reasons people are duped into opening these emails are curiosity (13.7%), fear (13.4%) and urgency (13.2%).

—PhishMe, 2016

PREVENTION IS KEY

UP TO 93% OF ALL BREACHES COULD HAVE BEEN AVOIDED WITH THESE SIMPLE STEPS:

1. *Implement a multilayered internet security solution.*
2. *Choose a security solution, such as ESET, that has ransomware protection built in. Many vendors charge extra for these features.*
3. *Choose endpoint security that includes Network Attack Protection, DNA Detections and Cloud Malware Protection, all of which work to block ransomware.*
4. *Update software regularly to keep it patched against vulnerabilities.*
5. *Make sure all your endpoints are protected, including laptops and smartphones.*
6. *Deploy an email security solution to block spam and phishing attacks, both of which can spread ransomware.*
7. *Back up all your data regularly; better yet, implement a backup and recovery system that will allow you to restore lost data.*
8. *Implement regular cybersecurity awareness training for all your employees.*

GET STARTED

Get your essential guide to preventing ransomware and protecting your organization.

DOWNLOAD NOW

ENJOY SAFER TECHNOLOGY®