RANSOMWARE IN THE TIME OF COVID-19

COVID-19 has accelerated cybercrime, particularly ransomware. Here's how things have changed and what you can do about it.

Ransomware, or malware that denies computer system access until the victim pays a ransom, is a serious problem. But the COVID-19 pandemic has made things worse.

RANSOMWARE IS NOT CHEAP

$4.62 million

The average total cost of a ransomware breach — **not including the ransom paid** or the financial damage caused when organizations are forced out of business.[1]

THE PROBLEM KEEPS GETTING WORSE

- Ransomware cost about **$20 billion globally in 2020,** compared with $11.5 billion in 2019[2]
- By 2031, **ransomware could cost $265 billion** annually
- The estimated average ransom paid in 2020 was $312,493, **up 171% from 2019**[3]
- **Approximately 205,000 U.S. organizations lost access to their files** due to ransomware in 2019[4]

COVID-19 ACCELERATED RANSOMWARE ATTACKS

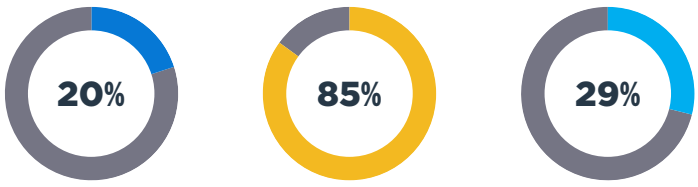
- **Workers at home** made networks more vulnerable
- Cybercriminals used **COVID-19-themed phishing and social engineering tactics** to infiltrate networks and install ransomware[5]
- Organizations with strong security may be **infiltrated through third-party suppliers' remote workers**

ANXIETY IS A FACTOR

Cybercriminals exploited employee fears about COVID-19

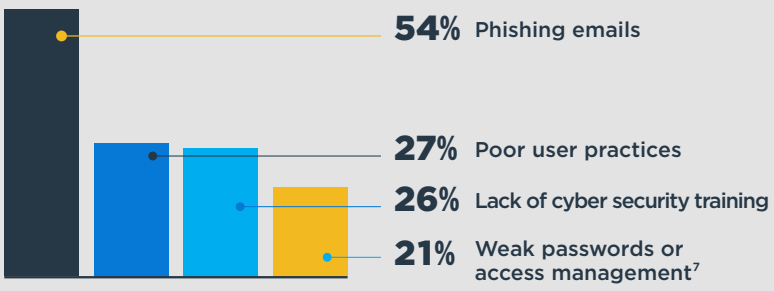
- Phishing attacks involving the **promise of government assistance** during business shutdowns
- Spoofing and email offering **information on vaccines, PPE and COVID-19 "cures"**
- **Free tech downloads for video conferencing** in the middle of the shutdown or **supposed critical updates to enterprise software**[6]

SMBs ARE NOT IMMUNE



- **20%** of ransomware victims are small and medium-sized businesses
- **85%** of managed service providers say ransomware is a common threat to SMBs
- **29%** of small businesses have reported experience with ransomware[4]

TOP CAUSES OF RANSOMWARE ATTACKS AT SMBs



WHAT YOU CAN DO

1 Audit security and backup everything

Audit your cyber security to ensure you have the latest patches and security protocols. Keep multiple backups at different locations, in real time if necessary.

2 Employee training

Employees are often the entry point for ransomware through email, website and phone scams. As hacker scams become more sophisticated, training and retraining employees is essential.

3 Prepare for the worst

Carry comprehensive cyber insurance, and have a detailed incident response plan in case of a ransomware attack — your broker can help formulate the right plan for your business.

Contact us today at hubinternational.com

[1] IBM, *Cost of a Data Breach Report 2021*, July 2021.
[2] Purplesec, "Cybersecurity Trends in 2021," accessed August 16, 2021.
[3] ZDNet, "The cost of ransomware attacks worldwide will go beyond $265 billion in the next decade," June 7, 2021.
[4] Purplesec, "The Growing Threat of Ransomware," accessed August 16, 2021.
[5] CBS News, "Cybercrime is thriving during the pandemic, driven by surge in phishing and ransomware," May 19, 2021.
[6] KPMG, "The rise of ransomware during COVID-19," accessed August 16, 2021.
[7] Datto, *Global State of the Channel Ransomware Report*, accessed August 13, 2021. Data is from 1,000 managed service providers' experience with small and medium-sized customers.

HUB

Risk & Insurance | Employee Benefits | Retirement & Private Wealth