

Ransomware Rescue

How to recognize and avoid a data hostage situation

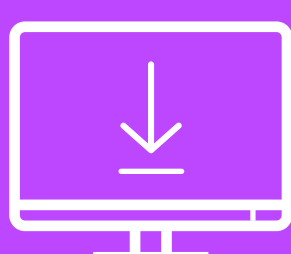
Stay alert to ransomware—malware designed by cyberthieves to hold your customer's computer or data hostage until they pay a ransom.



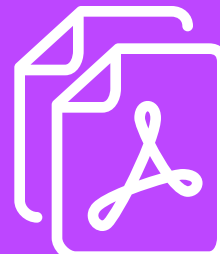
Threats seem innocent when they arrive from seemingly trusted sources via:



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 **2019** due to ransomware attacks¹



1 business every 11 seconds: the **predicted frequency a business will fall victim** to a ransomware attack by **2021**²



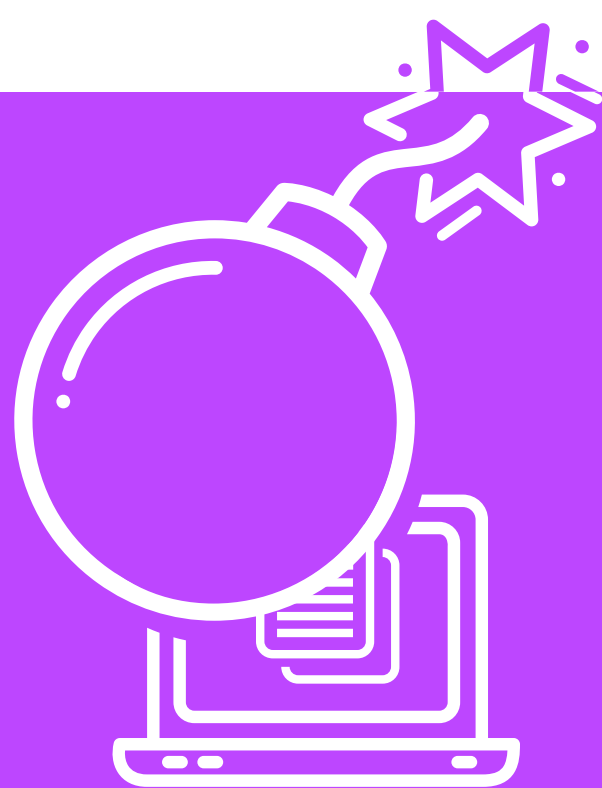
\$20 billion: the **predicted cost of damages** due to ransomware by **2021**³



1. "Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate," Coveware. <https://www.coveware.com/blog/2020/11/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate> (Accessed June 2020).

2. "Global Cybercrime Damages Predicted to Reach \$6 Trillion Annually By 2021," Cybercrime Magazine. <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/> (Accessed June 2020).

3. "Global Cybercrime Damages Predicted to Reach \$6 Trillion Annually By 2021," Cybercrime Magazine. <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/> (Accessed June 2020).



A ransomware infection means:

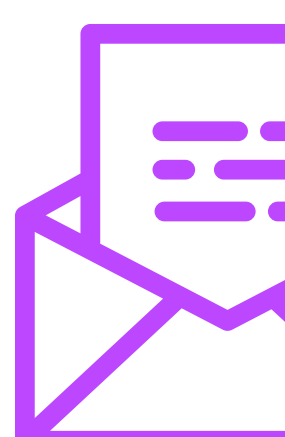
- ✓ Temporary or permanent data loss
- ✓ Little or no access to systems and applications
- ✓ Disruption to your regular operations
- ✓ Financial loss
- ✓ Harm to their organization's reputation

Protect yourself 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



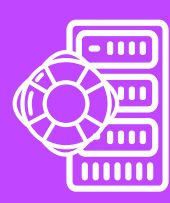
Train customers to be wary of email attachments, like bogus shipping receipts



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



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



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

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

Fight Back Against Ransomware

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

n-able.com/products

About N-able

N-able empowers managed services providers (MSPs) to help small and medium enterprises navigate the digital evolution. With a flexible technology platform and powerful integrations, we make it easy for MSPs to monitor, manage, and protect their end customer systems, data, and networks. Our growing portfolio of security, automation, and backup and recovery solutions is built for IT services management professionals. N-able simplifies complex ecosystems and enables customers to solve their most pressing challenges. We provide extensive, proactive support—through enriching partner programs, hands-on training, and growth resources—to help MSPs deliver exceptional value and achieve success at scale.

n-able.com

The N-able trademarks, service marks, and logos are the exclusive property of N-able Solutions ULC and N-able Technologies Ltd. All other trademarks are the property of their respective owners.

© 2021 N-able Solutions ULC and N-able Technologies Ltd. All rights reserved.