6 tips to **protect your business** from ransomware

Ransomware attacks are on the rise, and your business could be next.

$5.3M

Average Ransom Demand in 2021

Ransomware is a type of malicious software that blocks access to a computer system until a ransom is paid. The number of data breaches caused by ransomware doubled in the last two years and is expected to pass phishing as the top cause for data compromise this year.[1]

As instances increase, so do the demands. In the first half of 2021, the average ransom demand was $5.3 million which is a 518% increase from the 2020 average of $847,000.[2] Companies are facing a "pay-or-else" situation that can destroy their entire business.

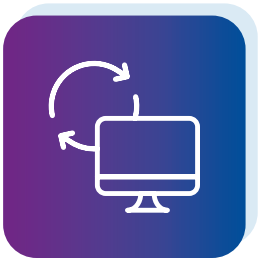
What We Know

At Experian, we've acquired the knowledge and developed the tools to combat these attacks. Over the last decade, we've observed that nearly 7 out of 10 breaches involved ransomware.

Ransomware events, in our experience with clients, take, on average, over 20% more time to begin than other attacks leading to more lost time and money.

With ransomware on the rise, it is time for all organizations, big or small, to take precautions against these cyberattacks. Don't panic, there are simple steps you can take right now to mitigate these threats.

Here are a 6 tips to help prevent and limit the impact of ransomware attacks



1 Update systems regularly

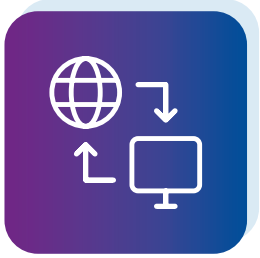
Up-to-date operating systems are often more secure than outdated ones because hackers have less time to find exploits. Always use the latest software version available so you don't fall victim to viruses or hacker attacks.

2 Back up your data

Local backups are essential to protect your files or other types of digital data stored on company servers (e.g., cloud storage services and web hosts).

3 Train your team

Organizations that provide employees with security awareness training are more likely to succeed in fighting ransomware attacks. Research shows that 88% of all data breaches are caused by employee error.[4] When team members know how to spot and avoid malicious emails, everyone can play a part in protecting the organization from these cyber threats.



4 Check your port settings

To protect against ransomware, carefully consider which ports your organization needs open. For example: Remote Desktop Protocol port 3389 and Server Message Block 445 are both targeted by malware that tries to take control of users' devices. You don't need any extra risk; you may want to close these connections if possible.

5 Practice and prepare

Consider implementing Experian's Reserved Response plan to enhance your preparedness for a data breach. This service includes crisis drill and simulation exercises with data breach experts. Our experts will guide you every step of the way and find any areas for improvement so you can be fully prepared when the time comes.

6 Make a plan

Create an incident response plan that includes defined roles and communications your team will use during attacks, as well as a contact list of companies who might need notification, like your partners and vendors. If you don't currently have one set up (or if it's outdated), consider creating a suspicious email policy so everyone knows what types of messages require immediate attention.

The only path forward is preparedness

The best way to minimize the impact of a ransomware attack is to create a preparedness plan that establishes negotiation and payment rules, defines external-breach communication strategies, and actively scans for threats from all angles. Breaches are our business at Experian. We know ransomware breaches have more complex FAQs, letter versions, and increased call center escalations.

To learn how Experian's Reserved Response solution can prepare your business for a data breach, click here.

You can learn more about other specific products by visiting us at our website **www.experian.com** and checkout more blogs from Experian on this topic **here.**

Or you can contact us **here.**

[1] ITRC Identity Theft Resource Center 2021 in review Data Breach Annual Report. Identity compromises: from the Era of Identity Theft to the Age of Identity Fraud. January 2022. https://notified.idtheftcenter.org/s/

[2] Palo Alto Networks. 2021. Extortion Payments Hit New Records as Ransomware Crisis Intensifies. https://www.paloaltonetworks.com/blog/2021/08/ransomware-crisis/#:~:text=As%20they've%20adopted%20these,the%202020%20average%20of%20%24847%2C000.

[3] Verizon. 2021. 2021 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/

[4] Influencive. 2021. HUMAN ERROR IS STILL THE NUMBER ONE CAUSE OF MOST DATA BREACHES IN 2021. https://www.influencive.com/human-error-is-still-the-number-one-cause-of-most-data-breaches-in-2021/