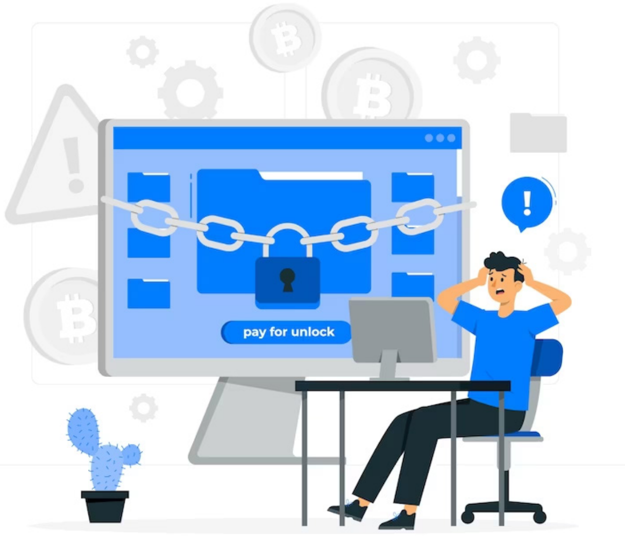

pay for unlock

What to do if you are hit by a **Ransomware Attack**

Ransomware attacks remain at a near-record high, and given the ever-increasing digital surface of businesses, it's harder than ever to stay protected. It doesn't help that the prevalence of tools like Ransomware as a Service (RaaS) has further emboldened and empowered hackers, allowing them to launch attacks on an unprecedented scale.

According to a report by Cybersecurity Ventures, businesses will fall victim to ransomware attacks every other second, up from 11 seconds in 2021 and 40 seconds in 2016. Ransomware attacks can be devastating to not just your bottom line but also to your reputation.

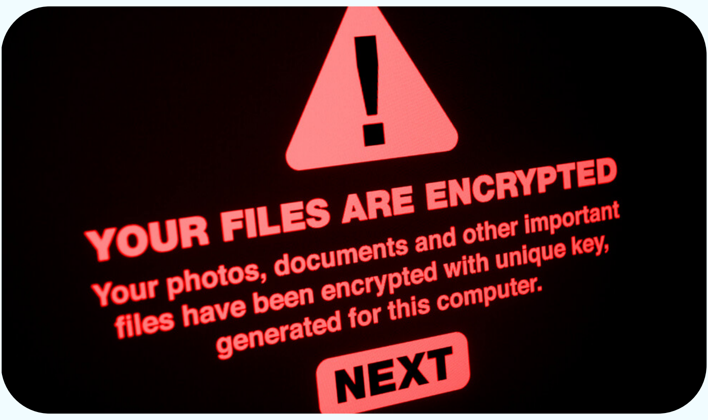
Here's what you should do if you get hit by a Ransomware Attack.

Identify the Infection

Try to identify the ransomware that affected your network infrastructure security. Take a picture of the ransomware note you received and use a site like "No More Ransom! Project" to help you with identification. This is an important first step in understanding how the infection propagates, what types of files it affects, and your available options for removal and quarantining.

In addition, you should also report the attack to the authorities. We understand it may not be a good look for your brand to inform others about the ransomware attack, but it's important to keep all stakeholders, including the authorities, in the loop about the cybersecurity event.

Documenting every attack allows the authorities to gain a clearer picture of the attack's origins and what can be done to stop them. You're doing your part to keep cybersecurity attacks at a minimum.


YOUR FILES ARE ENCRYPTED
Your photos, documents and other important files have been encrypted with unique key, generated for this computer.
NEXT

Isolate Your Systems

The ransomware attacks aim to spread to your entire network and infect as many systems as possible, giving you little time to react. This is why the first step is to isolate your infected computer from other endpoints on your network.

Disconnect the computer from the internet, and unplug the machine from the storage device, LAN, and anything else it may be connected to. Furthermore, disable Wi-Fi and Bluetooth. Doing so will contain the ransomware attack and also prevent the device from communicating with the attackers.

Do keep in mind that the ransomware may already have spread to other systems through multiple attack vectors. Learn more cyber security services for more information.

Plan Your Next Steps

The good news is that there are many decryption tools available that you can start using. This is why you should identify the ransomware strain to get an accurate tool. Websites like No More Ransom maintain a database of ransomware strains as well as how to go about decrypting them. Load the website and enter the name of the ransomware strain to see if you can find a decryption tool.

If you can't find a decryption tool, you may be left with very few options. You may be tempted to give in to the attackers' demands and pay up in exchange for your data. Hackers know that it is more convenient for businesses to pay up than to go about looking for damage control.

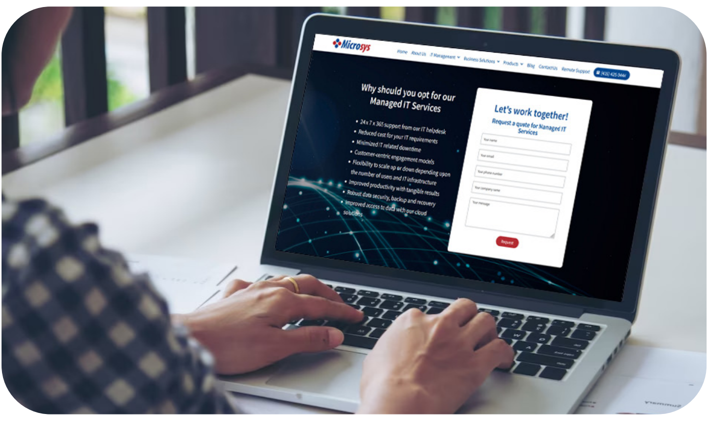
However, paying attackers only incentivizes them to attack other businesses like yours. Moreover, you may get penalized for giving in to their demands. Besides, it is possible that the hacker may never give you back your data - not out of spite, but because they themselves aren't always sure how to decrypt it.

NO MORE RANSOM
NEED HELP
unlocking your digital life without paying your attackers*?
YES
NO

Restore the Data from a Backup

We're big proponents of maintaining regular backups of your data. You can work with managed IT services providers to keep regular backups of your critical data and maintain copies of it in a safe environment.

In case you don't have a backup, you may have to start afresh - which is a better idea than just paying up.


Microsys
Home
About Us
IT Management
Business Solutions
Products
Blog
Contact Us
Remote Support
Why should you opt for our Managed IT Services
24 x 7 x 365 support from our IT helpdesk
Reduced cost for your IT requirements
Minimized IT related downtime
Customer-centric engagement models
Flexibility to scale up or down depending upon the number of users and IT infrastructure
Improved productivity with tangible results
Robust data security, backup and recovery
Improved access to data with our cloud solutions
Let's work together!
Request a quote for Managed IT Services
Request

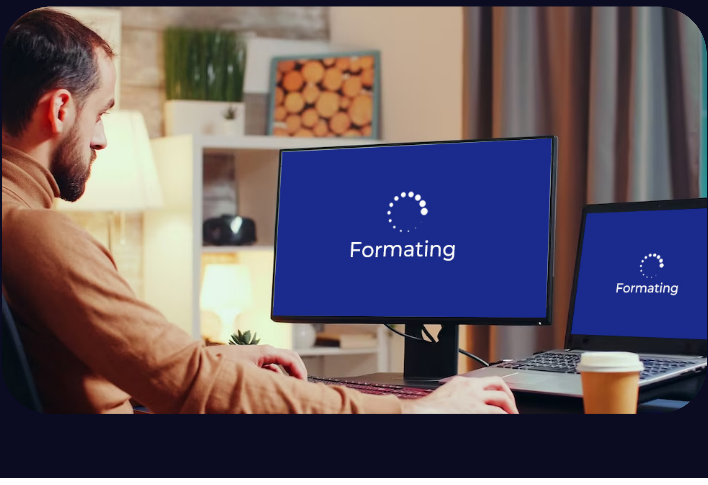
Start Over

The most effective way to deal with the ransomware attack if you can't find a decrypt tool is to start over. Do a complete wipe of all your hardware and reinstall all software from scratch. Format all storage devices to kill all remnants of the ransomware.

Create a backup strategy with both local and off-site backups. These backup copies should be isolated from your network, isolating them from future ransomware attacks. You can work with managed IT services providers to maintain healthy backup copies of your data.

It may be tempting to run a system restore to get your system back up and running; however, this is not the best solution for removing the ransomware. This is because the ransomware software may be sitting dormant within your system. In other words, the malicious code may have worked its way into your system restore. Also, the system restore doesn't save all copies of your data and is not a good replacement for ab backup.

You should always have a backup procedure in place to defeat ransomware attacks.


Formating
Formating

Change Passwords of all Accounts

Now that you've got all your systems up and running, it's time to change all account passwords. This is especially true for accounts that were connected with the infected system. Make sure to use a stronger password this time and enable multi-factor authentication (MFA).

Enter Your Password
••••
1 2 3
4 5 6
7 8 9
* 0 #

Preventing a Ransomware Attack

The best solution against ransomware attacks is to prevent them in the first place. Here are a few quick tips to avoid ransomware attacks:

- Apply security updates as soon as possible
- Be wary of social engineering attacks such as phishing emails
- Private cybersecurity training for your employees to help them distinguish threats
- Use MFA to add an extra layer of security, as it requires more than two pieces of evidence to access solutions
- Roll out daily backups to help you recover your data in the event of a ransomware attack
- Use anti-virus and anti-malware software as well as other security policies to block ransomware attacks
- Keep your security up to date by working with fully managed IT services providers who will deploy security software on various endpoints such as email servers and network systems

Although ransomware attacks are far from a pleasant experience, you can always make a recovery from the event. You don't have to pay ransomware or go out of business.

SECURED ACCESS
CONFIRM
click here for more information

For more information on how to effectively deal with ransomware attacks systematically, get in touch with experts at Microsys Inc, who can help.