How to Avoid **Ransomware Attacks**

It's official – cybercriminals are now using automation to scale the ferocity and volume of ransomware attacks. To make matters worse, Ransomware as a Service (RaaS) groups are crawling out of the woodworks and arming the average cybercriminal with powerful tools that can devastate networks and systems.

It's a matter of when, and not if, businesses would run into a ransomware attack.

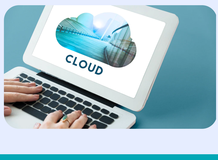
The onus is now on businesses to beef up their security systems with the help of intelligent solutions and smart cybersecurity practices. This guide provides the reader with 6 tips to keep ransomware attacks at bay.

Backup Your Data

We know this strategy has been discussed a million times already – but it needs reiteration.

C-level executives should prioritize data backups across multiple locations – both remote and physical. Store your data on external hard drives and keep them isolated from the internet, making sure to sync up with your network at least once per day. Cloud servers are the go-to solution for businesses because syncing data is as effortless as connecting to the internet.

We strongly recommend creating multiple copies of your backup data. Bonus points if the storage server utilizes immutable (cannot be altered) and indelible (cannot be deleted) technology. This way, even if your data gets encrypted by malicious software, you will always have backup copies to rely on.



Utilize Browser Isolation Solutions

Browser isolation solutions are a popular – but frowned upon – strategy to stop users from visiting malicious websites and downloading dangerous files. Isolation technologies can be used to block malicious code that can spread ransomware, including trojan horse viruses that are often disguised as legitimate software.

Note that browser isolation filters should be constantly configured to keep blocking threats and stop employees from visiting unknown domains. Isolation can be one of the most effective ways of completely eliminating the threat of ransomware downloads and securing company resources.

Regularly Update Your Systems

Discussing this security tip is like beating a dead horse – most readers are probably tired of being told the same thing over and over again. But some security tips simply cannot be underestimated and the more you discuss them, the better. Regularly updating your systems and software to the latest version is right up there with the best security strategy you can ever use.

We know it can be a nuisance for employees to deal with pop-up notifications to update their software – but it is a necessary nuisance. If you don't update your software, you leave your systems vulnerable to attacks that can cripple your whole infrastructure.

New variants of ransomware are emerging everyday to bypass your security features. Outdated software and systems are easier to break by leveraging well-known vulnerabilities.

Larger businesses, in particular, are a major target of cybercriminals because they rely on legacy systems that haven't been updated for far too long. The WannaCry wave of ransomware attacks that broke into Windows operating systems is a bone-chilling reminder of what happens when you keep using legacy systems.

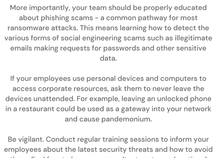
WannaCry brought Taiwan Semiconductor Manufacturing Co, Telefonica, and hospitals to their knees. And all they needed to prevent the attack was upgrading to the latest software. Doing so would have temporarily disrupted service – but could have ultimately saved these institutions from the public embarrassment and losses due to WannaCry.

Far too many businesses rely on the 'if it ain't broke, don't fix it' mantra. It's 2022 and the ability to constantly evolve and use cutting-edge technology is the need of the hour.

Train Employees about the Principles of Ransomware Attacks

Most ransomware attacks can be attributed to employee negligence and lack of awareness. In fact, social engineering provides cyber criminals with the path of least resistance and the greatest value for their time.

At this point, the vast majority of security breaches can be prevented by educating your employees. Educate your employees to be vigilant about protecting corporate data and setting up firewalls.



More importantly, your team should be properly educated about phishing scams – a common pathway for most ransomware attacks. This means learning how to detect the various forms of social engineering scams such as illegitimate emails making requests for passwords and other sensitive data.

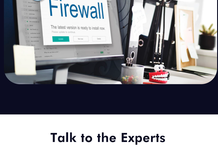
If your employees use personal devices and computers to access corporate resources, ask them to never leave the devices unattended. For example, leaving an unlocked phone in a restaurant could be used as a gateway into your network and cause pandemonium.

Be vigilant. Conduct regular training sessions to inform your employees about the latest security threats and how to avoid them. Feel free to have our consultants set up educational seminars that inform, inspire, and empower your employees.

Install Antivirus and Antispyware Software on Your Computer

Your network and computer are only as safe as the tools used to protect them. This is where antivirus and anti-spyware tools come in. They are constantly working behind the scenes to avert the latest attacks. Just make sure to update these tools because they can be rendered useless if not routinely updated.

Make sure the antivirus solution includes strong end-point security for all your devices. End-point is particularly useful for remote employees who use their personal devices to interact with company resources. These antivirus solutions block malware from infecting your systems. They also allow admins to detect when a device has been breached – and stop it from spreading into your networks.



Talk to the Experts

Implementing the above cybersecurity strategies can mitigate your enterprise's risk of a ransomware attack. Are you ready to take advantage of smart and intelligent security solutions? Talk to our security consultants to create a customized solution for your organization to succeed, grow, and ward off ransomware attacks.

Talk to our security consultants