

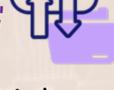
18 Tips To Prevent Ransomware Attacks

Globally, cyberattacks are likely to cause USD 6 Tn business losses by 2021, 30 percent of them linked to 'ransomware'.



Remain Secure With 18 Tips!

1 Take Regular Backups



Take regular backups, save multiple copies and monitor integrity of your backups.



2 Personalize Anti-spam Settings

2

Effective way is to configure webmail servers to block malicious emails.

3 Beware of Suspicious Emails



Emails are often eye-catching and appealing in the disguise of useful information.



4 Beware of Link Clicks

4

Beware of malicious requests seeking link-clicks, which may result in a security compromise.

5 File Extensions



File extension is another means for threat actors; malicious files can have multiple extensions.



6 Patches and Updates

6

Ensure your software, browser, OS, and other apps are updated with security patches.

7 Shut Internet Connection



Command prompt, control server are less vulnerable; internet shutdown can help during attacks.



8 Disable vssvc.exe

8

Disable this at the event of a compromise to prevent ransomware from erasing shadow volume snapshots.

9 Firewall



Keep Windows Firewall on and properly configured; security suites can offer additional firewall protection.



10 Archived Files

10

Scan compressed or archived files with the help of security software.

11 Windows Script Host and PowerShell



Disable these two functions to prevent ransomware; Enable PowerShell only if necessary.



12 Microsoft Components

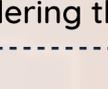
12

Secure Microsoft components like MS office tools, especially the macros and ActiveX.

13 Block Pop-ups



Add extensions to browser to block pop-ups, considering their vulnerability to trojan attacks.

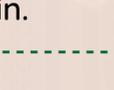


14 Disable Auto-play

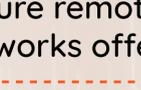
14

Doing this blocks immediate threat entry through USB devices upon plug-in.

15 Remote Services



Secure remote services, which involve diverse networks offering scope for intrusions.

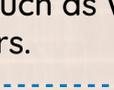


16 Unused Connections

16

Disable all unused connections such as Wi-Fi, Bluetooth, IR ports, among others.

17 Software Restriction Policy



This restricts .exe files from running in vulnerable locations such as ProgramData, AppData, and Temp.



18 Block Tor Gateway

18

Tor gateway is a major source for ransomware, blocking that delays the threat entry.

Secure with StealthLabs

Make the best out of available security options to remain safe. StealthLabs can help You!



Contact Us