



8 Steps: Never Get Held to Ransom How to Protect Yourself from Ransomware Attacks

YOU ARE AT RISK. 40% of businesses fell victim to Ransomware attacks in 2016, in 2017 that number is already rising. Protect your data from Ransomware.

Ransomware is a sophisticated, malicious type of malware that blocks access to your files or computer until a Ransom is paid. **The best way to protect yourself is by being prepared.**


1. Be Cognisant of Unsolicited Email

-  **DON'T** open an attachment in an email that seems suspicious. To effectively safeguard yourself, don't open any attachments or click links in emails from unknown sources.
-  **DO** Go into your settings and unhide or 'Show Extensions' so that you can monitor the file types of all sent email attachments. Be very cautious of the attachments you choose to open.


Examples of Common Email Ransomware Carriers:

- Any unsolicited email that asks you to enable a Microsoft Office feature called macros
- An email from an unknown person or company with an invoice attached.
- Any email with details regarding an unexpected payment into your bank account
- An email from your bank requesting that you enter your details, enter their website, or any page, from a link contained in that email.
- An email from a tax association regarding either a payment into your account or a payment due that requests you download any file or directly click on a link.



2. Think Before You Click

-  **DON'T** click on suspect adverts or links, even if they are hosted on trusted websites.

Malvertising is on the rise so avoid suspicious links, ads and websites.


-  **DO** Google Search the product or service if you are interested in finding out more.

3. Don't Talk to Strangers

-  **DON'T** open unsolicited messages in any messaging service (including Skype, Facebook, Twitter etc) without thinking twice. The old adage of not talking to strangers applies, if you don't know the person sending it, rather don't click on it or open it. It might be a virus.
-  **DO** make sure your privacy settings on all of your social media and messaging accounts are up to date and secure.

4. Always Have a Backup

Most importantly, and the only bulletproof protection from being held Ransom, is making sure you have a recent backup of all your files. This means you are never at risk of losing your data and having to pay a Ransom to get it back.


-  **DO** speak to your IT Department about Cibecs, the best endpoint data backup and complete data protection solution for businesses.


Ransomware variant,
WannaCry infected
200 000 computers
globally in 2 days!

8 Steps: Never Get Held to Ransom


How to Protect Yourself from Ransomware Attacks


5. Keep with the times

 **DON'T** delay or disable your OS and AV updates and never expect your users to perform updates on their own.


 **DO** ensure you have prompt software update policies which can be centrally managed and enforced to all devices on the network.


6. I hear you Snowden!

 **DON'T** think that simple, more convenient passwords are more sensible in terms of productivity, through reasoning such as “you trust the people you work with” or “I’m simply not hiding anything or it’s not important enough”. Ransomware tools are designed to exploit any vulnerable device, regardless of who you are and they ransom your data and they will use your device to spread further.


 **DO** ensure you have strong password policies enforced to avoid exploits through remote protocols such as SMB or RDP.

7. Sharing isn't always caring

 **DON'T** hesitate in switching off or disconnecting your infected device immediately. The longer the device is online the higher the risk of it scanning and sharing its nasty self.

 **DO** switch off the device or disconnect any wifi or lan connection and keep any removable media such as USB drives and flashdisks connected to the device away from other devices.

8. Don't bring a knife to a gun fight

 **DON'T** rely on sync or backup tools which utilize SMB shares, even in cases where the SMB exploits are patched a share may be legitimately available to the devices, where it may spread itself and infect other devices sharing from the same server.

 **DO** use the right backup solution, such as Cibecs which offer:

- Centrally managed and automated backups, your users must not be expected to do anything!
- Secure backup protocols, such as SSL.
- Encrypted data at rest, meaning data backed up is isolated and contained so even infected files will not spread to other user's backups
- Point in time recoveries, allowing you to recover all files or even a single file as it was at a point before infection. Sync tools typically only offer this on a file by file basis meaning I.T. can spend hours possibly even days trying to recover a single users data.

About Cibecs

Cibecs is the best endpoint backup & data protection solution for business, it's built locally and trusted by thousands of companies worldwide. Cibecs is easy to deploy and manage and equips IT with a single solution for complete end-user data protection. With Cibecs you'll have total visibility with impressive and intuitive reporting that enables Corporate Governance Compliance.