8 tips for preventing ransomware

nakedsecurity.sophos.com/2016/03/24/8-tips-for-preventing-ransomware/

John Zorabedian
by John Zorabedian

- 0Share on Facebook
- Share on Twitter
- Share on Google+
- Share on LinkedIn
- Share on Reddit

Chances are you know someone, or some organization, who has suffered a ransomware attack – it could be your local police department, a small business, big hospital, or someone in your family.

If you haven't been hit by ransomware personally, you're either very lucky, or you've taken some proactive steps to protect your computers and files.

If you do get infected with ransomware, unless you've got back-ups, or the crooks made some kind of cryptographic mistake, you're left with either paying or losing your locked up files forever.

Prevention is far better than a cure. So here are 8 tips to protect yourself against ransomware.

1. Back up your files regularly and keep a recent backup off-site.

The only backup you'll ever regret is one you left for "another day." Backups can protect your data against more than just ransomware: theft, fire, flood or accidental deletion all have the same effect. Make sure you encrypt the backed up data so only you can restore it.

2. Don't enable macros.

A lot of ransomware is distributed in Office documents that trick users into enabling macros. Microsoft has just released a new tool in Office 2016 that can limit the functionality of macros by preventing you from enabling them on documents downloaded from the internet.

3. Consider installing Microsoft Office viewers.

They allow you to see what a Word or Excel document looks like without macros. The viewers don't support macros so you can't enable them by mistake, either.

4. Be very careful about opening unsolicited attachments.

Most Windows ransomware in recent months has been embedded in documents distributed as email attachments.

5. Don't give yourself more login power than necessary.

Don't stay logged in as an administrator any longer than necessary. Avoid browsing, opening documents or other regular work activities while logged in as administrator.

6. Patch, patch, patch.

Malware that doesn't come in via document macros often relies on bugs in software and applications. When you apply security patches, you give the cybercriminals fewer options for infecting you with ransomware.

7. Train and retrain employees in your business.

Your users can be your weakest link if you don't train them how to avoid booby-trapped documents and malicious emails.

8. Segment the company network.

Separate functional areas with a firewall, e.g., the client and server networks, so systems and services can only be accessed if really necessary.

Further reading

Experts from Sophos have put together a comprehensive, free guide on **how to stay protected against ransomware**, including practical advice you can follow to secure yourself and your business in both the short term and down the road.

Follow @JohnZorabedian
Follow @NakedSecurity

Image of businessman with umbrella courtesy of Shutterstock.com.