



# How to beat ransomware: prevent, don't react

Posted March 11, 2016 by Wendy Zamora

Picture this: You've spent the last few weeks working on a tribute video for a friend's 30th wedding anniversary. You collected photos and video clips and edited them together, laying over a soundtrack of their favorite songs. It was a real labor of love.

When you finally finish the project, you go to copy the file onto a DVD and—what the?—a strange message pops up.

“Unfortunately, the files on this computer have been encrypted. You have 96 hours to submit payment to receive the encryption key, otherwise your files will be permanently destroyed.”

You've been hit with ransomware.

You didn't back up the anniversary video. In fact, you haven't backed up any of your files in months. What do you do?

Unfortunately, when it comes to ransomware, once your files are encrypted, there's not much you *cando*—besides cut your losses or pay up. And even if you do pay up, there's a chance you won't get your files back, so you're out the files and your cash.

That's why it's so important to prevent ransomware attacks from happening in the first place.

### **Types of ransomware**

The first step in ransomware prevention is to recognize the different types of ransomware you can be hit with. Ransomware can range in seriousness from mildly off-putting to Cuban Missile Crisis severe.

### **Scareware**

Okay, yes, it's called scareware, but in comparison to other types of ransomware—not so scary. Scareware includes rogue security software and tech support scams. You might receive a pop-up message claiming that bajillion pieces of malware were discovered and the only way to get rid of them is to pay up. If you do nothing, you'll likely continue to be bombarded with pop-ups, but your files are essentially safe. A quick scan from your security software should be able to clear out these suckers.

*Pro tip: A legitimate antivirus or anti-malware program would not solicit customers in this way.*

### **Screen lockers**

Upgrade to terror alert orange for these guys. When lock-screen ransomware gets on your computer, it means you're frozen out of your PC entirely. Upon starting up your computer, a full-size window will appear, often accompanied by an official-looking FBI or U.S. Department of Justice seal saying illegal activity has been detected on your computer and you must pay a fine.

In order to reclaim control of your PC, a full system restore might be in order. If that doesn't work, you can try running a scan from a bootable CD or USB drive.

*Pro tip: The FBI would not freeze you out of your computer or demand payment for illegal activity. If they suspected you of piracy, child pornography, or other cybercrimes, they would go through the appropriate legal channels.*

### **Encrypting ransomware**

This is the truly nasty stuff. These are the guys who snatch up your files and encrypt them, demanding payment in order to decrypt and redeliver. The reason why this type of ransomware is so dangerous is because once cybercriminals get ahold of your files, no security software or system restore can return them to you. Unless you pay the ransom—they're gone. And even if you do, there's no guarantee you can get those files back.

*Pro tip: While the FBI often recommends people just pay the ransom, cybersecurity professionals advise otherwise. Complying with ransomware criminals just opens the door up for future attacks.*

So what should you do about this kind of ransomware? Get out in front of it. "If any attack in the history of malware proves that you need protection in place before an attack happens, encrypting ransomware is it," says Adam Kujawa, Head of Intelligence at Malwarebytes. "It's too late once you get infected. Game over."

### **Ransomware prevention**

The first step in ransomware prevention is to invest in awesome cybersecurity. Start with an antivirus with active monitoring and layer on other applications that are specifically designed to thwart advanced malware attacks such as ransomware. These include anti-malware and anti-ransomware programs.

Next, as much as it may pain you, you need to create secure backups of your data on a regular basis. You can purchase USBs or an external hard drive where you can save new or updated files—just be sure to physically disconnect the devices from your computer after backing up, otherwise they can become infected with ransomware, too. Cloud storage is another option, but we recommend using a server with high-level encryption and multiple-factor authentication.

Finally, stay informed. One of the most common ways that computers are infected with ransomware is through social engineering. Educate yourself on how to detect phishing campaigns, suspicious websites, and other scams. And above all else, exercise common sense. If it seems suspect, it probably is.