How to defend against ransomware

November 10, 2016
by Ben Rossen
Attorney, Division of Privacy and Identity Protection, FTC

In September, the FTC hosted a workshop on ransomware, one of the most serious online threats facing people and businesses today — and the most profitable form of malware criminals use. How does ransomware work? Hackers hold your files "hostage"— often encrypting them — then demand payment, typically in bitcoins, for you to get them back.

Missed the workshop? Check out our videos featuring conversations with security researchers, technologists, law enforcers, and business leaders. Want some bite-sized takeaways? Here are some tips to protect your devices from ransomware, and what to do if you're a victim.

How can I defend against ransomware?

- **Update your software.** Use anti-virus software and keep it up-to-date. And set your operating system, web browser, and security software to update automatically on your computer. On mobile devices, you may have to do it manually. If your software is out-of-date, it's easier for criminals to sneak bad stuff onto your device.

- **Think twice before clicking on links or downloading attachments and apps.** According to one panelist, 91% of ransomware is downloaded through phishing emails. You also can get ransomware from visiting a compromised site or through malicious online ads.

- **Back up your important files.** From tax forms to family photos, make it part of your routine to back up files on your computers and mobile devices often. When you’re done, log out of the cloud and unplug external hard drives so hackers can’t encrypt and lock your back-ups, too.

What if I'm a victim of ransomware?

- **Contain the attack.** Disconnect infected devices from your network to keep ransomware from spreading.

- **Restore your computer.** If you've backed up your files, and removed any malware, you may be able to restore your computer. Follow the instructions from your operating system to re-boot your computer, if possible.

- **Contact law enforcement.** Report ransomware attacks to the Internet Crime Complaint Center or an FBI field office. Include any contact information (like the
criminals' email address) or payment information (like a Bitcoin wallet number). This may help with investigations.

Should I pay the ransom?
Law enforcement doesn't recommend paying the ransom, although it's up to you to determine whether the risks and costs of paying are worth the possibility of getting your files back. If you pay the ransom, there's no guarantee you'll get your files back. In fact, agreeing to pay signals to criminals that you haven't backed up your files. Knowing this, they may increase the ransom price — and may delete or deny access to your files anyway. Even if you do get your files back, they may be corrupted. And you might be a target for other scams.

Worried about ransomware affecting your business? Check out our Business Blog for specific tips.

Blog Topics: Privacy, Identity & Online Security
Ransomware – A closer look

Share This Page

Ben Rossen
Nov 10, 2016


Ransomware has emerged as one of the most serious online threats facing businesses. The FTC examined this issue at a September 7th workshop kicking off the Fall Technology Series, the first of three events looking at new and evolving technologies that raise critical consumer protection issues. Panelists – including security researchers, technologists, law enforcers, and business leaders – discussed the nature of the ransomware threat, how to defend against it, and essential steps to take if your business becomes a victim.

What is ransomware?
Ransomware is a form of malicious software that infiltrates computer systems or networks and uses tools like encryption to deny access or hold data “hostage” until the victim pays a ransom, frequently demanding payment in Bitcoin. In the typical case, the criminals demand between $500 to $1,000, but some have demanded as much as $30,000. Panelists described a wide variety of ransomware variants. For instance, some hackers will delete the victim’s files if payment isn’t made within a specified period of time, and many newer variants use highly advanced methods of encryption. Ransomware can be incredibly profitable to criminals, many of whom now have the resources to hire professional developers to build increasingly sophisticated malware.

Ransomware incidents have skyrocketed in the past year, and several high-profile attacks on health care organizations highlight the challenges that ransomware poses. In February, an attack on a hospital in Southern California knocked out its network for more than a week, leaving staff without access to email and some patient data. The hospital ultimately paid a $17,000 ransom to restore access. Another attack crippled the networks of ten Washington, DC area hospitals for nearly two weeks. But ransomware isn’t just a health care problem. It affects businesses across the economy. Panelists agreed that incidents of ransomware will continue to increase across the board – and nobody is immune.

The risks associated with ransomware
If your business holds consumers’ sensitive information, you should be concerned about the threat of ransomware. It can impose serious economic costs on businesses because it can disrupt operations or even shut down a business entirely. In addition, a business’ failure to secure its networks from ransomware can cause significant harm to the consumers (and employees) whose personal data is hacked. And in some cases, a business’ inability to maintain its day-to-day operations during a ransomware attack could deny people critical access to services like health care in the event of an emergency. Thus, a company’s failure to update its systems and patch vulnerabilities known to be exploited by ransomware could violate Section 5 of the FTC Act. Also, this principle is illustrated in several recent FTC actions that highlight the importance of defending against malware, such as cases against Asus and Wyndham.

**How is ransomware delivered?**

Criminals deliver ransomware in a variety of ways. According to one panelist, 91% of all ransomware arrives through email phishing campaigns. These typically require the user to take some kind of action such as clicking on a link or downloading a malicious attachment. Other campaigns use drive-by downloads, where a user visits a malicious website or a site that has been compromised, and the act of loading the site causes the ransomware to automatically download onto the user’s computer.

Other delivery methods are even more sinister. Several panelists described the rise of “malvertising” campaigns, where malicious code is hidden in an online ad that infects the user’s computer. These attacks are particularly nefarious because they can occur even on trusted websites through third-party ad networks that redirect the user to an infected server. More recently, attackers have exploited server-side vulnerabilities to deliver ransomware payloads by searching for networks that had failed to patch known vulnerabilities.

**How to defend against ransomware**

So what can you do to defend against the threat of ransomware? Panelists urged businesses to invest in prevention and recommended:

- **Training and education.** Implement education and awareness programs to train employees to exercise caution online and avoid phishing attacks.

- **Cyber hygiene.** Practice good security by implementing basic cyber hygiene principles:
  - Assess the computers and devices connected to networks to proactively identify the scope of potential exposure to malware.
  - Identify technical measures that can mitigate risk, including endpoint security products, email authentication, intrusion prevention software, and web browser protection.
  - Implement procedures to keep security current. Update and patch third-party software to eliminate known vulnerabilities.

- **Backups.** Back up your data early and often.
  - Identify business-critical data in advance and establish regular and routine backups.
  - Keep backups disconnected from your network so that you can rely on them in the event of an attack.

- **Plan.** Prepare for an attack. Develop and test incident response and business continuity plans.

**How to respond if you’re a victim**

If ransomware strikes, panelists urged organizations to consider these steps:
- **Implement your continuity plan.** To be ready if an attack occurs, have a tested incident response and business continuity plan in place. Well-prepared organizations with reliable backups may be able to restore systems from those backups with minimal data loss or business interruption.

- **Contact law enforcement.** Panelists recommended immediately contacting law enforcement, such as a local FBI field office, if you discover an attack.

- **Contain the attack.** Keep ransomware from spreading to networked drives by quickly disconnecting any infected computer from the network.

What should organizations do if there are no backups available? Does it ever make sense to pay the ransom? Most panelists, including law enforcement, don’t condone paying the ransom. If you pay, that doesn’t guarantee your encrypted data will be returned. In some cases the attackers simply increase their demands once a victim expresses a willingness to pay. Despite the serious risks to consider before paying a ransom, panelists also recognized that businesses may need to evaluate all possible options in the event of a crippling ransomware attack that limits the organization’s ability to function.

The Fall Technology Series continued last month with a workshop on **Drones** and will conclude with a workshop on **Smart TVs** on December 7th. Looking for advice on addressing the ransomware risk? Watch this video.

---

ftc.gov