Ransomware FAQ

by Sherri Davidoff, CEO, LMG Security

www.LMGsecurity.com

"Ransomware" has become an epidemic. Organizations of all are held hostage by ransomware, the malicious software that encrypts your data until you pay a hefty fee. All it takes is one person clicking on a link, and all of your shared files could be locked up for good.

How can you reduce your risk of a ransomware incident in today's complex environments, and how should you respond if you fall victim? Here is an FAQ that will help you understand how ransomware works, and how you can minimize your risk before—and after—a ransomware infection.

We will answer the following questions in this FAQ:

1. What does ransomware do, and how does it work?

"Ransomware" is malicious software that attackers use to encrypt the data on your computer. When you get infected with *ransomware*, all the data on your computer gets locked up (encrypted)—and only the attacker has the key. The ransomware may also encrypt files on any network shares your have attached. It can crawl through an entire organization, encrypting files. It can even encrypt files you have in the cloud, such as DropBox or OneDrive.

Typically, the attacker will demand payment. Once your files are encrypted, you'll see a ransom note--sometimes on your desktop, sometimes as a popup. The ransomware note will usually tell you that your files are encrypted, and you won't get the decryption key unless you pay up. The criminals hold you hostage. If you're lucky, when you pay the attacker, he or she will decrypt your data for you. Often, the attacker will only decrypt *some* of your precious data, and try to extort *more* money out of you to decrypt the rest.

2. What happens if I don’t pay the ransom?

That depends! Typically, one of three things will happen:

A) Your files won't get decrypted.

B) The ransom will go up over time.

C) Files will be deleted or destroyed over time.

3. What should I do if I think my computer is infected with ransomware?

Time is of the essence!

- ✓ Pull the network cable out, or if your computer is connected wirelessly, find some way to get it off the wireless network. Immediately disconnect any USB drives. Remember, the ransomware will crawl through your system encrypting files. You want to stop it from locking up files on any shared drives, or backup drives that you have attached to your system.
- ✓ Call IT. They may want you to pull your computer's plug out of the wall (or pull out the battery if it is a laptop). The not-so-nice shutdown is important. If you try to shut your computer down nicely by pressing a button, sometimes the ransomware can tell and it might not actually shut down.
- ✓ Figure out quickly what was encrypted, what the extent of the damage was. If you have backups for that data, GREAT! This really underscores the importance of taking regular backups, every single day, automatically.

  If you can't restore from backups, check to see if the ransomware you got is known to be broken. There are certain kinds of ransomware where we know how to break the encryption. For example, BitDefender, Emsisoft, and others frequently release updated decryption tools that work with many common ransomware variants. Don’t pay when a free decryption utility might be available.
- ✓ If all else fails, you may decide to pay the ransom.
- ✓ If there’s a chance you have sensitive or regulated data on any computer that was encrypted (such as personal information, Social Security Numbers, health care information, or other sensitive data), talk to legal counsel immediately for guidance on whether or not you are required to notify any parties involved.
- ✓ Consider reporting the ransomware attack to the FBI. They are tracking these cases. Either contact your local field office, or go to the Internet Crime Complaint Center at www.ic3.gov.
- ✓ Contact your insurer for support if you have coverage for cyber extortion or breach response.

4. How can I prevent ransomware from happening in my office?

An ounce of prevention is worth a pound of cure. To effectively prevent ransomware, use a combination of training and technical countermeasures.

- ✓ Educate staff about the dangers of phishing emails and scams on social media sites. Include phishing in annual training, and conduct regular phishing exercises to train your team not to click on links.
- ✓ Social media sites like Facebook and LinkedIn have also been used to spread ransomware, as well as other types of malicious software. Consider restricting access to social media sites on work computers, and instead encourage staff to use separate, personal devices for appropriate social media communications.
- ✓ If you have servers online that people use to connect remotely from home, make sure all of your account passwords are strong and changed regularly. Strongly consider using two-factor authentication for remote access whenever possible. There has been a recent spike of ransomware incidents where criminals broke into remote access servers using guessed or stolen passwords, and installed malware on corporate servers.
- ✓ Get effective spam-filtering software to block phishing emails consistently.
- ✓ Keep your organization's operating system and application patches up-to-date, so your workstations and servers are as resistant to infection as possible.
- ✓ Use reliable, commercial-grade antivirus software to reduce the risk of infections.
- ✓ Monitor your network (typically using a third-party service) so that suspicious activity is caught early.

5. How can I limit the damage caused by ransomware if someone does get infected?

A ransomware infection doesn't have to be a major crisis—but it often is, if you're not prepared. There are three things you can do to limit damage in the event that ransomware does worm its way into your network.

- ✓ Take regular backups of everything important-- and test your backups. Karen Sprenger, COO for LMG Security advises, "Test the backups and the restore process regularly. If you aren't testing, then you don't really have backups."
- ✓ Make sure everyone knows who to call, and what to do if they get infected with ransomware. Set up an easy-to-remember hotline that anyone can call to report ransomware, at any hour. You don't want to wait until the ransomware spreads throughout your whole network before IT figures out the problem. Everyone in your organization needs to recognize the signs and know that time is of the essence, pull that network cable, and call for help quickly.
- ✓ ONLY give people access to folders they really need. One of the reasons that ransomware is SO damaging is because we trust each other. Within your organization, you give people access to lots of files on the network shares. The Ponemon Institute did a survey and found that 71% of people have access to files that they really don't need to do their jobs.[1] We used to think that's convenient. Now it's a huge risk.

  Remember, when one person gets infected with ransomware, it will encrypt every file you have access to on your network. Now is the time to go through your organization's file permissions and lock them down, so if one person clicks a link they can't accidently encrypt everything.

[1] Ponemon Institute. "Corporate Data: A Protected Asset or a Ticking Time Bomb?" Ponemon Institute, Dec. 2014. https://info.varonis.com/hs-fs/hub/142972/file-2194864500-pdf/ponemon-data-breach-study.pdf. Retrieved 9 Aug. 2016.

6. How do I recognize whether an email might contain ransomware or other malware?

It can be hard to tell if an email is legitimate, especially if you typically get email from a wide variety of people, such as clients.

Phishing emails are designed to convince you to click on a link or open an attachment. The sender wants you to click right away, without thinking or checking to make sure it's legitimate. To accomplish this, they often appeal to your sense of fear or excitement, hoping to instill a sense of urgency that will trigger you to click without thinking.

Common characteristics of phishing emails include:

- ✓ A "lure," such as a free gift card or a tax refund;
- ✓ A scare tactic, such as an expiration or a threat that a service will be shut down unless you take action;
- ✓ A deadline or other urgent reason that you should take action immediately.

At LMG Security, we like to say, "Think Before You Click" (a phrase coined by my colleague Mike Wright, who managed cybersecurity for a community bank).

When you receive an email that prompts you to take an action, always take time to think. Ask yourself:

1. Do I even know this person?
2. If so, did I expect to receive this message from this person? [Remember, their email account could have been hacked]
3. Do I really NEED to click on this link? Let's say it looks like it comes from your bank. It's much better to go to your bank's web site and find the link from there, than to click on it in an email.

You can always hover your mouse over a link without clicking on it to see where it really goes. This can be a quick way to verify that an email is suspicious.

If you are not sure if an email is legitimate, as for help from your IT security staff or your organization's point of contact. When in doubt, don't click.

7. Ransomware Decryption Safety Tips

You never know what you're going to get when a criminal sends you a tool and tells you to run it. More and more often, victims of ransomware pay to receive a ransomware decryption tool— **only to find that it installs even more malware. When you do receive a ransomware decryption tool, remember these important safety tips:**

- **Don't trust tools given to you by criminals!** (This may seem obvious, but when you're being held for ransom, it's tempting to quickly run whatever tools they send you. Don't.)
- **Always run ransomware decryption tools in a malware laboratory first**, to check for malicious behavior.
- **Decrypt your files in a non-networked environment** whenever possible.
- **Scan any files you recover using multiple antivirus vendors** before putting them back into production. Criminals can leave additional malware behind for you to discover later.
- **After you've recovered, monitor your network carefully** for any signs of lingering compromise.

Call a professional if you need help. For more information, see:

"Ransomware Decryption is Like a Box of Chocolates"

https://LMGsecurity.com/ransomware-decryption-is-like-a-box-of-chocolates/

Questions?

Sherri Davidoff

Web: www.LMGsecurity.com

Phone: 855-LMG-8855

Email: info@LMGsecurity.com