Ransomware Prevention Guide

1802 Wright Street
Madison, WI 53704
forensics@gillware.com

***Ransomware** is malware that denies access to files on your computer, mobile device, or network by encrypting them or making them otherwise inaccessible, and demands that payment be made in order to regain access.*

The ransomware "industry" rakes in millions of dollars a year from its victims, although concrete figures are hard to come by (many victims are hesitant to admit they paid to regain access to their data). Ransomware has proliferated with shocking speed, thanks in part to the spread of untraceable "cryptocurrency" such as Bitcoins and the proliferation of ransomware "kits" on the dark web, which allow anybody, even "script kiddies" with no programming skills, to put together and reap the financial rewards of ransomware attacks.

Chief targets by ransomware hackers include organizations in the financial and healthcare industries. These organizations often have thousands or even tens of thousands of gigabytes of customer/patient data they cannot afford to lose—which makes them all the more willing to pay handsomely to get their data back at any cost. However, any business or organization can fall victim to a ransomware attack.

Here are some actions you can take which will be helpful preventing a ransomware attack, or easily recovering from one if it occurs:

Back Up Your Files.

The one sure way to defeat a successful ransomware attack without having to pay the ransom is to have the ability to recover your files from a recent or real-time back up. Before restoring your backup data, be sure that the computer system or network you are restoring is safe, and that all malware threats have been cleaned up and unauthorized remote access has been blocked.

Backing up files to a reputable cloud-based backup service or creating regular

backups to an external drive that is not constantly connected to your computer or network can allow you to easily recover in the event that you fall victim to ransomware intrusion.

It's good policy, not just in case of ransomware but in general, to have a strong, secure, and automated backup system in place. For a backup system protected against ransomware encryption, the backups you keep of your data should be stored off-network and regularly audited. Auditing your backups will ensure that nothing goes missing and nothing goes wrong in the event that you do come under attack and have to restore data from these backups.

Be Informed and Aware of the Threats and Risks.

Ransomware infections are usually the result of risky end-user behavior. Phishing emails with malicious attachments or links that are opened by an end user can result in the installation of ransomware and other malware. Educating end users to avoid risky behavior can prevent infection in the first place.

Train your employees to recognize email spam and phishing techniques. Bad actors almost always worm their way into their targets' networks by exploiting human psychology, and bad actors will often claim to be from an end user's bank, their IT department, UPS or USPS, or even the FBI to coerce their victims into clicking a fishy link and allowing dangerous software into their network.

Of course, spam and phishing tends to look extremely… fishy. However, their senders use a wide range of tricks to try and bypass the part of our brains that says, "Hey, hold on, this doesn't make any sense."

To keep your organization safe from these threats, your employees should be trained to recognize these kinds of hacking and phishing attempts on sight, and react accordingly.

Keep your Systems and Software Up to Date.

Like other malware, ransomware relies upon vulnerabilities in your computer, mobile device or network's operating system and installed software. Enabling automatic updates of your devices, operating system, and software and keeping your systems and software up to date and patched reduces vulnerabilities and can prevent infection.

It can be a pain to make sure everything from your computers' operating systems and antivirus software to your domain is up-to-date. But these updates make your computers, your networks, and your entire organization safer. Bad actors are constantly working to exploit any weaknesses they can.

Software designers and systems engineers are caught in an arms race with malware developers. As hackers find vulnerabilities, the engineers plug them up. Failing to keep your systems up-to-date can leave massive holes in your security systems.

Recognize the Usefulness and Limits of Antivirus Software.

No computer or mobile device you use should be without a good antivirus system. Installing and running up to date antivirus software from a reputable company can help to detect and stop malware, including ransomware. At the same time, you also need to be aware of the limitations of antivirus software.

Antivirus software is far from a panacea for digital ills. Malware developers are constantly updating and changing their software. Like any vaccine, your antivirus software can only protect you from the viruses listed in its database of virus definitions. Zero-day viruses—malware that has appeared so recently that antivirus software providers haven't yet had time to enter it into their database—can easily sneak by. In addition, some ransomware intrusions don't use viruses at all.

As necessary as antivirus software is, it is not the be-all, end-all of computer security. Conscientious computer usage and thoughtful security measures are an absolute must to protect your organization from ransomware.

Make Strong Passwords.

Viruses aren't the only ways bad actors can slip ransomware into your system. If your passwords are weak enough, a hacker can slip right into your network and deliver a ransomware payload—no email phishing necessary.

It's easy to see the appeal of easy-to-remember passwords—but the problem is that "easy to remember" is also "easy to guess". Lots of people like to work in things like their birth date (or a family member's birth date), the street they grew up on, their pets' names, etc. into their passwords. If a dedicated hacker can dredge this kind of information up on the internet (by, for example, taking a look

at the target's presence on social media platforms like Facebook or genealogy websites), it makes their job of cracking that password much easier.

A secure, randomly-generated password works much better. Good password generators create random passwords with high levels of "information entropy". The more "entropy" a password has, the harder it is for a hacker to brute-force their way in. Humans tend to be quite bad at coming up with high-entropy passwords on their own. Computers, however, can come up with passwords that can take billions of years to crack.

Use Multi-Factor Authentication.

A strong password is a good first step toward a more secure and ransomware-resistant network. A good next step is multi-factor authentication. Multi-factor authentication is especially critical if you have employees who frequently or even just occasionally work from home.

No matter how strong your passwords are, there are still ways a dedicated hacker might get around that and gain access to your network or your organization's social media accounts (Facebook, Twitter, LinkedIn, etc.). To prevent intrusions, two-factor authentication adds another layer of defense to your security systems.

Now it doesn't just take a password to log on—you need new login credentials provided by a hardware or software token as well. Even if a hacker can get around not knowing your password, they can't get around not having the token.

Limit User Account Access.

Setting up systems where users have limited privileges rather than Administrator or root level access can provide protection by preventing malware from being able to install itself if the account is compromised. Use of strong and unique passwords that are changed regularly can also assist in making computer systems more secure.

Ask yourself: Should all of my employees have the privileges to install new software on their workstations? Do all of my employees need write permissions for every share folder on our server? Should all of my employees be able to send emails with attachments to other employees? If so—why?

Maybe your answers to these questions are “Yes.” Maybe your answers are “No.” And maybe your answers are “Sometimes.” It all depends on what you do and what you need to have done. The most important thing is ensuring that the policies in place correspond appropriately to both your answers and your security needs.

If there’s a discrepancy—you’re letting employees install new software willy-nilly and you really don’t need to be, for example—that’s a hole in your network security you really should fill.

Do your employees need new restrictions? If so, implement them. Do your employees need less restrictions? If so, make sure they are well-trained not to abuse their freedoms.

Keep Your Eyes Peeled.

Constant vigilance and thoughtful, prudent, proactive security measures will keep your organization safe not just from ransomware attacks, but all cyberattacks. Businesses and organizations owe it to themselves, their employees, and their clients and customers to keep their fingers on the pulse of cyber security and look for new exploits and threats to be aware of.

Gillware™
Digital Forensics

1802 Wright Street
Madison, WI 53704
forensics@gillware.com