Ransomware Tip Sheet

What is Ransomware?

Ransomware is a relatively new way that cybercriminals are infecting PCs and mobile devices. Ransomware uses encryption to lock a victim’s files and hold them hostage until they pay the attackers demand—usually in bitcoin, a digital currency.

One of the most common attack methods is phishing emails that have malicious attachments or links in the email. When the user opens the attachment in the phishing email, it installs a malware on the computer that allows the attacker to encrypt or lock the files. The computer screen freezes with a pop-up message—often from the FBI or another federal agency—saying that because you violated some sort of federal law your computer will remain locked until you pay a fine. The email typically warns the user that the files have been encrypted and the files will be unencrypted when a ransom is paid.

Cyber Attacks are on the Rise in Healthcare

In 2014, the FBI signaled an alarm to the healthcare industry, calling it “a rich new environment for cybercriminals to exploit.” Only in recent years has the healthcare industry begun the process of transitioning from paper to electronic systems. The rush to adopt the technology has left some healthcare organizations more focused on the clinical and workflow aspects of the electronic systems and less focused on data security. Meanwhile, cybercriminals have discovered new opportunities for
financial gain from the virtual “treasure trove” of information contained in a medical record and medical devices.

What You Can Do to Prevent a Ransomware Attack

- Back up your operating system and all its contents to an external hard drive every single day
  - It is less likely that you could be held hostage if you have copies of important data
  - Data can be recovered from back-up files
- Be careful what you click on
  - Do not open attachments included in unsolicited emails. A suspicious email may tell the user that they should immediately review an overdue invoice or a similar tactic to entice the user to open the attachment
- Use a reputable anti-virus and firewall. Make sure your software is up-to-date
- Keep current with patching to minimize exploits and vulnerabilities
- Be cautious when clicking any link containing free software or other offers
- Business users should allow their IT departments to perform upgrades
  - Many ransomware attacks come in the form of fake ads for upgrades to products such as Windows, Java, and Adobe
- Enable the pop-up blocker on your browser to prevent suspicious ads
- Use virtual browsing sessions whenever possible, so everything is deleted—including malware—when the session is closed
- Avoid clicking on links to suspicious websites
  - A common technique attackers use to distribute ransomware is through fake websites they have created. Attackers entice victims to visit the infected website
and then run their malware once the victim downloads infected software from the website

- Use secure sites when sharing confidential information (understand the difference between HTTP and HTTPS)
  - Anytime you need to share confidential information, such as a social security number or your credit/bank account number (to make online payments), you should always make sure that the site is HTTPS. This will protect your information from being taken by hackers and used to steal your identity. If you want to make a purchase online and you notice that the site is not HTTPS, you should either phone in your order or physically go to the store.

- Be extremely wary of all shortened URLs
  - Shortened URLs, produced by services like bit.ly and goo.gl, can be brute-forced. (a trial-and-error method to obtain information such as a password or a personal identifier)
  - Searching a shortened URLs yields all sorts of secret documents - many of them can be edited, and can be infected with malware
  - The destination of a malicious link may be confusing
  - Some shortened link services have a better reputation than others
  - Services exist to reveal the destination of shortened URLs, for example X-Ray. (These will reveal the destination domain underneath the apparently harmless short URL)

- Limit access to business critical data and shared drives

- Use strong passwords
Immediately notify your IT department, the FBI, and MagMutual if you believe you are a victim of a ransomware attack. Disconnect from the Internet if you receive a ransomware note so your personal data isn’t transmitted back to the criminals. You may be able to mitigate risks by acting quickly.

The content and information presented here is intended to be used for general information and is not legal advice. It does not create an attorney client relationship. Consult a licensed attorney to assist with specific situations that require legal advice or counseling.

05/06/2016

---