IN BRIEF

August 2016
Issue 129

OSB Professional Liability Fund

www.osbplf.org

Malpractice Prevention Education for Oregon Lawyers

Beware Ransomware: Data-Encrypting Software Continues to Extort

Imagine the stress of turning on your computer tomorrow to find a pop-up window stating that your personal files are encrypted and the date and time your private encryption key will be destroyed. To get your adrenaline pumping, the countdown-to-destruction timer is activated as soon as you open the computer: "Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server."

Beware: Cyber criminals continue to use data-encrypting ransomware to extort money. Ransomware is malicious software that sneaks onto your computer and holds your data hostage in an encrypted format until you pay the ransom to obtain the private encryption key to decrypt it. A few computer files or your entire computer may be held for ransom. The ransom payment is typically $100 to $500 or more paid in the untraceable form of Internet currency known as Bitcoin, delivered to an anonymous site.

Stories of ransomware are NOT the latest urban legend. Some of your colleagues here in Oregon have been victimized by this scary form of malware – short for "malevolent software" – which includes nasty computer viruses, Trojan horses, worms, spyware, and key loggers. (See accompanying Malware Glossary posted on the website under Practice Management>Publications>In Brief.)

Are You at Risk for Malware?

If your computer is connected to the Internet or is part of a computer network that is connected to the Internet, you are at risk. There are two chief ways that cyber criminals can get ransomware onto your computer: (1) by exploiting software vulnerabilities to install ransomware onto your computer or (2) by exploiting social engineering techniques, counting on your being too trusting of websites, pop-up windows, or emails (containing hyperlinks or attachments) that appear to come from someone you know. To protect against the first method, you need a good anti-virus, anti-malware protection program you keep up to date. You need to check for updates for all computer programs and install these updates as soon as possible. To protect against the second delivery method, you need to become savvier and less trusting, and train your staff to be the same!

Awareness and Training

Awareness and staff training are imperative. Ask yourself these questions:

1. Do you have current anti-virus, anti-malware protection on any computer connected to the Internet? Does your staff?
2. Do you perform regularly scheduled computer scans? Does your staff?
3. Do you check for current updates and install them as soon as possible? Does your staff?
4. Do you have a firewall installed on any computer connected to the Internet? Does your staff?
5. Do you avoid clicking pop-up windows when visiting various sites on the Internet? Does your staff?

6. Do you verify an email is legitimate before opening an attachment or clicking on a hyperlink? Does your staff?
7. Do you know how to spot a dangerous email? Does your staff?

Email Vulnerabilities

Unfortunately, it is too easy for your email address to get tied up in a malware scheme. Your address may be in several address books, and one of these books may be on an infected computer. The malware sends emails to all these contacts, hoping the recipient will see the familiar sender and open it. When the unsuspecting recipient opens the email and then opens the attachment or the hyperlink inside the email, malware is unleashed into your computer. If your computer is set up with a pathway to your server, the ransomware can also lock up your entire server.

How to Spot a Dangerous Email

Given that emails are one of the primary methods for effecting ransomware attacks, it is crucial to know what to look for. Beware of these red flags when reading emails:

1. Look at the sender's name and email address. The email message claims to be from one name, but if you click on the name, this name does not match the actual email address. For example, the email states it is from Sheila Blackford, but instead of seeing my expected email address sheilab@osbplf.org, you see it is from petrovich.bx1547@zoho.com.
2. Watch out when a pop-up window appears when you visit a website, for example, offers to claim a prize or get help from live customer service reps.
3. Watch out if you get an email from the IRS or from the U.S. Postal Service. They don't send emails.
4. Watch out if any email has a hyperlink for verifying personal identifying information, such as your Social Security number, driver's license number, or passport number. Move your mouse over the link to view the actual URL address.
5. Watch out if your bank requests your personal or account information, such as your account number, Social Security number, or PIN, via text or email – banks rarely do this.
6. Watch out for an email from a bank or credit card company, especially if you don't have an account there.
7. Before doing online banking, be sure your computer has been scanned for malware and your protection is up to date. The URL window should show a lock icon in front of the company name and a URL address that starts with "https," with the "s" indicating secure socket.
8. Don't panic if you get a message from the FBI or police that your computer has been locked due to being tracked by law enforcement for downloading pirated software, pirated music or movies, or child pornography. The cyber criminals are hoping you are sufficiently horrified at being accused of illegal activities and will pay to avoid further embarrassment and a ruined reputation! This ransomware has been so popular that it is known as a "cop trojan" or "police trojan."
9. Pay close attention to company logos to spot some detail amiss. An important word in the name that you normally would expect to see may be missing.
10. Pay attention to spelling errors or clumsy sentence structure that does not reflect the expected level of professionalism.

Prevention Practices

Prevention is the best way to protect yourself from a ransomware attack. Follow these steps to help thwart would-be cyber thieves:

1. Back up your computer daily. Disconnect your computer from the Internet before backing up data to a local server. Close your browser and disconnect your Ethernet cable from your router if you have a wired connection. If you have a wireless connection, disconnect according to the instructions from your owner's manual. You can also disable and enable your wireless connection through Windows.
2. Verify you have a clean backup copy of your data.
3. Store backups in locations inaccessible to your computer, such as on an external drive you unplug from your computer's USB port after you have backed up data to it. Disconnect anything that may be or may become infected, for example a USB backup or automatic uploads to DropBox. Ask your IT support services to help you if you are unsure how to implement any protective actions.
4. Encrypt your entire hard drive so confidential information cannot fall into the wrong hands.
5. Do not keep your decryption key on your computer so it will be safe from being discovered. See "Encryption Made Easy: The Basics of Keeping Your Data Secure," Sharon D. Nelson and John W. Simek, *OSB Bulletin* (April 2016).
6. Disconnect your computer from the Internet when you are not using it. Follow the steps in number 1. above.
7. Purchase intrusion detection software or anti-malware software or both. Intrusion detection software sends an alarm when intrusions are detected. Anti-malware software contains an alert or alarm feature to notify you something has been discovered.

8. Follow instructions provided by your anti-malware program. "You get what you pay for" applies to technology more times than not.
9. Contact IT support services who are knowledgeable about setting up safeguards to protect your computers and servers.

Sheila M. Blackford
PLF Practice Management Advisor

Resources – Cybersecurity

- Practice Aid: Information Security Checklist for Small Businesses, courtesy of Sunsei Enterprises, Inc. www.osbplf.org>Practice Management>Forms>Technology
- FYI Cyber Alert: www.osbplf.org>Practice Management>Publications>In Brief>August 2016
- Malware Glossary: Sheila Blackford: www.osbplf.org>Practice Management>Publications>In Brief>August 2016