RM Matters
May 2015

The Dentists Insurance Company
1201 K Street, 17th Floor, Sacramento, CA 95814
800.733.0634 thedentists.com

Actions to Help Avoid Ransomware Nightmare

By TDIC Risk Management Staff

Dental practices are among the victims falling prey to ransomware, a type of malware that infects and disables computers and demands payment from victims to restore computer access.

The Dentists Insurance Company warns dentists that ransomware can bring a practice to a standstill. One California dentist reported that her computer system was infected by ransomware, which encrypted all electronic patient information, scheduling software and digital X-rays. Via an onscreen prompt, the hackers demanded $500 to restore the files.

The dentist said the malware essentially shut down her practice for several days while she determined the next steps. The immobilizing extent of the malware surfaced when the dentist's cloud backup and hard-drive backup were unusable as well. The problem in this case was that the dentist left the hard-drive backup plugged into the computer system, and the ransomware accessed the backup when encrypting the system. Ultimately, the dentist's IT consultant built a new server for the office to remedy the problem.

TDIC reports calls to its Advice Line about ransomware are increasing, and while only a few dental practices have related a specific problem with the malware, NBC News recently noted that ransomware has targeted at least 1 million victims nationwide, including individuals, small businesses and even a Tennessee sheriff's office.

With names like CryptoWall and CryptoLocker, ransomware continues to be a threat as rogue authors improve file-encrypting programs and infection methods, according to PC World, which categorizes ransomware into three varieties: scareware, lock-screen viruses and the really nasty stuff.

Scareware is described as the simplest and consists of fake antivirus or clean-up tools that claim to detect issues and demand payment to fix them. Lock-screen viruses make computers unusable and display a window, often with an FBI or Department of Justice logo, stating that you violated the law and must pay a fine. According to Microsoft, these claims are a "scare tactic designed to make you pay the money without telling anyone who might be able to restore your PC." Encrypting malware such as CryptoLocker is labeled the most serious because it encrypts and locks personal files.

In its online Malware Protection Center, Microsoft lists various types of ransomware and states all of them prevent owners from using their PCs normally and extort a ransom, often demanded in Bitcoin online currency. Ransomware can also include a "countdown clock," giving victims 24 or 72 hours to make payment. Working in different ways, ransomware can encrypt files, prevent access to Windows or stop certain apps, like a Web browser, from running.

Cybersecurity experts and Homeland Security advise victims to avoid paying the ransom and say there is no guarantee that computer access will be returned. In the case of the California dentist, she chose not to pay the ransom and risk more trouble. The dentist was directed by local police to contact the FBI about the incident. The only upside of the situation was that the dentist had encrypted the patient information on her system, so she was not required to send out breach of patient information notices.

Paying the ransom can also make victims a target for more malware, according to Microsoft's website. Other experts note that payment perpetuates the ransomware threat by funding cybercriminals. While there are accounts of some businesses and organizations succumbing to the extortion, making payments and regaining computer access, the recommendation from Homeland Security is to not pay.

Paying ransom does not guarantee the encrypted files will be released; it only guarantees that the malicious attackers receive the victim's money, and in some cases, his or her banking information. Additionally, according to Homeland Security's website, decrypting files does not mean the malware infection itself is removed.

Ransomware can infect computers through a malicious website or a website that has been hacked. "Drive-by" download attacks are launched from compromised websites or through malicious ads and usually exploit weaknesses in browser plug-ins like Flash Player, Java, Adobe Reader or Silverlight, according to recent information from PC World. IT professionals say even popular software download sites and freeware sites can offer software bundled with malware. Spam emails and infected removable drives are other ways ransomware gets on computers.

In one case documented by NPR, an employee at a small business opened an email that appeared to be from PayPal. The email said, "Somebody paid you money," but when the employee clicked the link, a red alert dominated the computer screen with a written demand for ransom. The company's database was encrypted by the malware, and the business lost everything it had built up over 14 years.

To help avoid the threat of ransomware and other malware, IT professionals at the California Dental Association say practice owners must exercise diligence in protecting their data, often through multiple layers of protection or by utilizing strict process methodologies. In addition to antivirus programs, malware detection software such as Malwarebytes or Spybot Search and Destroy is recommended. Experts also say these applications are not impenetrable and do not guarantee protection, especially if they are not updated on a regular basis.

TDIC recommends the following precautions issued by IT professionals, Microsoft and other sources:

- Always run an up-to-date antivirus program.
- Complement an antivirus program with malware detection software.
- Keep software and browser-related components updated.
- Turn on computer firewalls.
- Keep your browser clean to prevent adware invasions.
- Be wary of email attachments, even if they appear familiar.
- Regularly back up important files.
- Unplug all backups and store them in a separate location.
- Download software only from official vendor websites.
- Understand what you are installing on your computer.
- Limit user privileges through user account controls.
- Curtail Internet use on office computers.
- Allow Internet use for work-related business only.
- Alert employees of ransomware risks.

TDIC offers data compromise as an addition to property coverage. The data compromise policy has $50,000, $100,000 and $250,000 limits, and can pay for mailing notifications letters to patients, providing affected individuals with credit monitoring and more.

TDIC's Risk Management Advice Line can be reached at 800.733.0634.

For use by the California Dental Association components, the Arizona, Hawaii, Nevada, New Jersey, North Dakota and Pennsylvania dental associations, the Alaska Dental Society and the Illinois State Dental Society. **If you reprint this article, please identify TDIC as the source.**

TDIC requires this article be used in its entirety. If you need to edit, expand or reduce this article, please call Jaime Welcher beforehand at 800.733.0634, ext. 5359 or fax your suggested changes or additions to 877.423.6798.