pmm
practice management
and marketing news

LCP Dental Team Coaching (the new name for Julie Weir & Associates) is recognized as the premier consulting firm specializing in pediatric dentistry since 1996.

The Growing Threat of Ransomware: Is Your Practice at Risk?

Ransomware is a cryptovirus that holds patient information hostage and shuts down your practice. The ransomware encrypts patient files stored on practice devices/computers, preventing access unless a ransom is paid. These attacks on dental practices are increasing due to inadequate virus protection and information back up protocols. Since access to patient files is essential to patient treatment, doctors are motivated to pay the ransom to be able to get back to business as usual. Practices across the country can lose hundreds of thousands of dollars due to weeks of lost production because of the time it takes to negotiate with the thieves to hopefully get the decryption key to restore patients' files. Education, prevention, and having the right advisors are crucial to reducing the risk of a ransomware infection.

IMPACT OF RANSOMWARE INFECTION

- The recovery process is very stressful due to loss of production, employee wages and the large amount of time and effort it takes to recover the files.
- Paying a ransom does not ensure patient files will be restored. Experts disagree on the odds of recovery if a ransom is paid; however, there is a fair chance a decryption key is never received or that a decryption key is received but does not work. In some instances, paying the ransom encourages attackers to ask for more money for full recovery or results in the company being retargeted because of their willingness to pay.
- In the event the practice closes, doctors may be unable to accommodate emergencies or urgent treatment needs. This can lead to negative feedback in the community and patients may leave the practice to seek treatment elsewhere.
- During ransomware attacks, there may be a data breach of sensitive and protected patient health information.

STEPS TO PREVENT INFECTION

Understanding how cryptoviruses access practice devices and ways to deter them are the keys to preventing a ransomware infection. It is the doctor's responsibility to understand current cyber attack issues so they can make sure the practice is protected with the best preventive measures. Do not leave the responsibility to others as this can cause a gap in protection.

- A cryptovirus typically enters devices through seemingly harmless emails and email links. These emails look very similar to known email addresses; however, they contain subtle differences that trick a user into thinking it is a real person. Your IT service company can be a good resource to help educate the team on how to recognize these email scams.
- Hire an IT service company to properly install HIPAA-compliant firewalls and set up automatic updates and backups. **Be sure the IT company has adequate insurance to pay a ransom if they are attacked and can explain how backup programs are protected.**
- Consider hiring a cybersecurity company in addition to an IT service company to double the protection and reduce risk even further. Whereas IT service companies specialize in general computer systems, networking, and hardware and software applications, cybersecurity companies focus on the prevention of cyberattacks and aid in risk management. Have a cybersecurity plan in place so all team members understand its importance and know what to do if an attack does occur.
- Purchase a cyber insurance policy through a current business, audit, or malpractice insurance company to help reduce costs if the practice gets attacked. Some companies offer to combine these policies to lower monthly premiums. In the case of an attack, a cyber insurance policy may cover expenses related to the investigation of the attack, monetary losses due to business interruption, data loss recovery, data breach notifications and credit monitoring for customers, and legal expenses associated with settlements and fines. In some cases, a cyber insurance company may pay the ransom to ensure files are restored. Although cyber insurance charges a monthly premium for coverage, it will defray the cost in a ransomware attack.
- Always use an encrypted email to send and receive protected information. An IT service company can ensure emails are properly configured for HIPAA compliance which will add extra protection for the practice and its information.

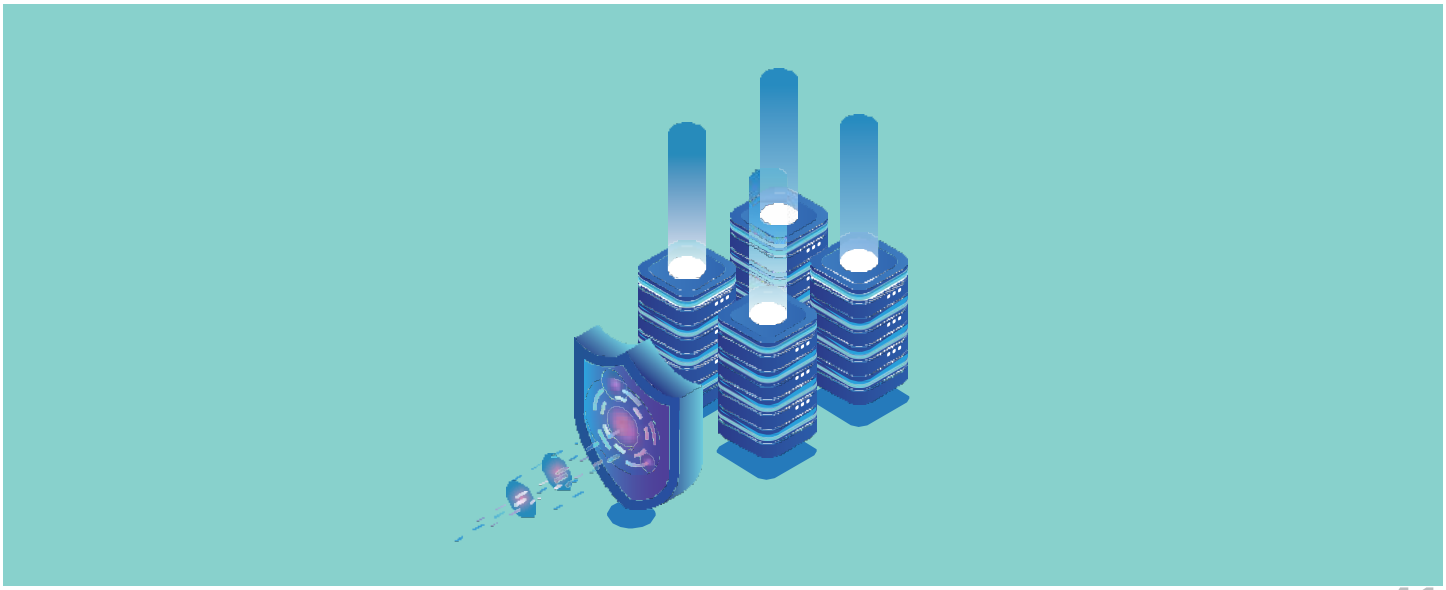
- Have a professional email connected to your URL domain, such as manager@awesomedental.com. A practice email should not be hosted by a site such as Gmail or Yahoo.
- Avoid accessing practice devices from home. This is an easy access point for a cryptovirus to infect practice files. If the remote desktop protocol is not secured or set up properly, it leaves an entry point for attackers to hack into practice devices. Experts are finding that in addition to a vulnerable remote desktop protocol, an attack due to weak login credentials happens far more often. If remote access is necessary, be sure that a 2-step authentication process is set up and working properly. This ensures each time remote access is requested, an authorized user is behind the request.
- Use resources, such as **Infragard,** to stay educated on current cyber events affecting the healthcare sector.
    - **Infragard** is a partnership between the Federal Bureau of Investigation (FBI) and members of the private sector for the protection of U.S. Critical Infrastructure.
    - Infragard provides an online communication forum for education, information sharing, networking, and workshops on emerging technologies and threats.
    - Through this partnership, both the FBI and private sector gain an improved understanding of the threatscape and share valuable intelligence.

HAVE A "BACKUP" PLAN

- Perform daily virtual and external hard drive backups of the practice management software, patient files, and financials. Running hard drive backups daily can help a practice recover quickly from a ransomware virus attack.
- ***Virtual BackUp:*** A virtual backup is a copy of the practice's files that are currently stored on the device's hard drive. The copy of the files is transferred to a virtual drive within the computer that is often installed by your IT servicer.
    - Be sure that all essential information is saved to the shared drive on the server, as virtual backups only copy files saved to the network and not on individual devices.
    - The cloud is one example of a virtual backup option; however, there are other virtual backup options that may be recommended by your IT servicer. Ransomware viruses can also access and encrypt data stored on the cloud so an external hard-drive backup should be utilized in addition to a virtual backup.
- ***External BackUp:*** An external backup is a copy of the device's files that are saved to an external hard drive. At the end of each day, the doctor should take the external hard drive to another location for safekeeping.
    - This also protects the information in case the office and its devices are damaged from an unexpected disaster, such as fires or floods. Leave external hard drives unplugged unless files are being backed up. A cryptovirus can access your practice information if the external hard drive is plugged into a device.
    - Some computer viruses do not go active right away and infect the device unknowingly at a later date. To ensure a clean backup is always available, it is recommended to have 2-3 external backups that are rotated. For example, if Backup A is used on Monday, Backup B would be used on Tuesday and Backup C would be used on Wednesday. This way, the worst that could happen is losing one day's worth of data.

MAINTAINING HIPAA COMPLIANCE

- HIPAA compliance ensures that patient information is protected and safeguarded against unauthorized individuals.
- Practices that are not HIPAA compliant may be more susceptible to cryptovirus attacks. When a practice is attacked, a patient's sensitive personal and health information is at risk of exposure and could be vulnerable to becoming victims of fraud.
- To ensure the practice maintains HIPAA compliance, schedule annual HIPAA training for the entire team and designate a team member to be the HIPAA privacy officer who oversees that compliance is maintained.



As you can now understand, a ransomware cryptovirus can cause serious harm to a practice. Doctors must be proactive in taking preventive measures to protect their businesses, employees, and patients that depend on them. While many offices resume business after an attack, the lost production, patients, and employee wages have lasting effects. Ensure the proper fail-safes are in place through expert advisors, HIPAA compliance training, daily backups, and continuing education on recommended protocols and systems for the prevention of a ransomware attack.

We would like to thank Colin Macdonald from QeH2 and PCMag for all the insight provided on this topic.

"By failing to prepare, you are preparing to fail."

Benjamin Franklin

Published four times a year, Practice Management and Marketing News is a featured column in Pediatric Dentistry Today.