Ransomware is Creepy

By Angela Spinks

This article is penned for the benefit of any practice owner or manager who has not read the recently published horror story in CDA Oasis. **A dental office was down for 3 days after an employee opened an innocent-looking email.**

The email contained Ransomware that immediately infected and encrypted all files – despite the significant backup and anti-virus precautions that the practice had in place. The fraudsters demanded cash to hand over the decryption key.

The stress, expense and loss of revenue are one thing. Pile on patient safety, potential breach exposure, government fines, tarnished reputations and collegial reprimands… the risk is immense. Yet often avoidable!

Here's the link if you want to read about the Dentist's [horror story](). In today's limited space, I'd prefer to focus on prevention.

What can you do to avoid such a nasty trick?

1. Use a reputable email service provider with both anti-virus and anti-malware security built in. A good email product has layers of filtering to block, quarantine or eliminate bad files from ever reaching the desktop

2. Secure a personalized domain for your practice (name@PracticeName.com)

3. Train yourself and your staff to recognize the warning signs of non-legitimate emails:

   - the sender name is not recognized
   - there are obvious spelling, grammar and language mistakes
   - a legitimate company logo is mimicked – it appears warped, blurred, stretched or otherwise off
   - a different url appears when you hover your mouse over the address or link
   - the subject does not make sense in the context of your business/practice

4. Don't follow unknown or suspicious links

5. Don't open attachments from an unknown sender, or if any aspect of the email seems strange. Examine zip files carefully; do not open .exe files. When in doubt, verify with the sender

6. Be wary about websites visited – ensure all users stay on legitimate business sites and not be lured by ads, sponsored banners and pop-ups

7. Have at least 2 backups. Rotate daily and weekly backup files. One must go offsite so that you are protected from fire, theft, or flood. They MUST be [encrypted]() and you MUST safeguard the encryption key (password to decrypt)

8. Have the backup data verified quarterly. This is like simulating a disaster; restoring your data from the backup to make sure that it works!

Note: Simply checking the backup notification is NOT DATA VERIFICATION.

We all take this issue very seriously; it's alarming that in the first quarter of 2015, the security company McAfee reported a 165% increase in ransomware attacks.

Scary. Even when you are diligent and think you're protected, malware can strike. One of our clients relates his experience:

"We had been backing up our servers locally to external drives using a service that wasn't very reliable when needed. Just 2 days after switching to ABEL's online backup service, one of our servers was compromised by ransomware that encrypted and deleted all our vital data. The local backup drive had also been erased and encrypted. The ransomware demanded $3000 to restore the data.

We contacted ABEL for assistance and, once we were able to get the server running, they logged in, restored our ABEL data and configured the software. Within less than 24 hours, we were back up and running. Had it not been for ABEL's amazing support and their reliable backup service, we would have lost over 3 months' worth of data."

If you haven't already, please talk to us about protection, backup, data verification and recovery. Malware is everywhere and does not limit its ghoulish behavior to one day in October.

Thanks to our friend Anne Genge, CIPP/C at Healthcare Compliance Network, for her insights on this topic.