Vice President's Perspective

Is Your Data Safe?

WannaCry. Crypto. Ransomware. Malware. Viruses. Are you familiar with these things? Unfortunately, the risk associated with data attacks and data hostage schemes just keeps growing. You need your data to be secure. What can you do to minimize your risk?

One thing you might consider, if you haven't already done so, is to outsource your data storage and backup responsibility. In 2010, Ortho2 released Edge – a truly optimized cloud solution. Edge data is stored in a private building with 12-inch reinforced pre-cast concrete walls and 24/7/365 video monitoring. It is compliant with PCI-DSS v3.0 and HIPAA/HITECH guidelines. Or, in a word: SECURE. The Edge data that resides in this facility is also backed up to other locations for the ultimate in redundancy. Keeping your data secure is VERY important to us. It should be for you, too.

And while your data in Edge is safe, ViewPoint data, or even personal data on your computer may not be. Here are a few tips to help you make sure your computers don't fall prey to hackers and viruses:

- Logins and Passwords – Longer is better, even up to 12 digits, and always include lowercase and uppercase letters, numbers, and symbols if permitted.
- Updates – Software providers regularly provide updates to address evolving threats. This includes Windows and the programs you use like Edge and ViewPoint. But to be fully protected, you must regularly install the updates. Which brings me to the next item:
- Antivirus Software – Make for sure you use it, and keep it current.
- Firewalls – Whether you use a hardware or a software firewall, having something in place to protect your practice is important. Talk to our Network Engineering Team to discuss the best option for you.

- Retire Windows XP – Its support ended on April 8, 2014. Since then, security updates have not been regularly provided. Yet XP is still the fourth most-used version of Windows. If you have Windows XP in your office, please update the computer or, at a minimum, the operating system.
- Be cautious with email links and attachments, and instruct staff to do the same! Opening attachments or clicking links from unknown sources is never a good idea. And unfortunately, hackers can also spoof (masquerade) or hack (steal) email addresses from people you know. These days, regardless of the source, you simply MUST be wary of links and attachments that are unexpected or seem odd.
- Backups – Even if your practice data is securely stored and backed up at our Edge data center, you will want to make regular backup copies of locally stored data like QuickBooks, presentations you've prepared, or pictures you upload to your computer. For help confirming or implementing local backups, contact our Network Engineering Team.

We periodically hear from customers that have been infected with a virus, or have lost data and don't have a recent backup. In almost every case, these are preventable issues. And if it happens to you, it will be unpleasant at best… and potentially devastating.

And unfortunately, this threat is growing year by year. We are doing what we can to protect you, but we can't do it all. Please take care!

Amy Schmidt

Amy Schmidt, Ortho2 President

Reprinted from
The Newsletter for Members and Friends of Ortho2
July 2017 - Volume 35 Issue 3