THEVISIONCOUNCIL

PREVENTING DAMAGE FROM RANSOMWARE

Dan Bailey is a well-known marketing expert with numerous highly-regarded optical lab clients. Members of The Vision Council's Lab Division have exclusive access to Dan's marketing and communications consulting services tailored specifically to optical labs, and have access to his products and services available at a discounted rate.

As an additional offering to members, Dan will be writing a series of articles on topics of tremendous importance to labs, and we begin this month with a conversation about the daunting topic of "Ransomware". The Vision Council encourages labs to take the precautions to avoid this potentially disastrous situation, and reminds you of your access to Dan's services to protect and promote your organization.

We usually talk about things you can do to market and grow your business, with a focus on taking advantage of today's technology to make your marketing more cost-effective. In this article I would like to talk a little bit about a facet of technology that can hurt rather than help your business: Ransomware.

In September, one of my non-optical clients got infected with ransomware. Most of you have probably heard a little about this particularly heinous form of cyber extortion. And, most of you have probably thought to yourself, "Gee, I hope that never happens to me!" and then thought nothing further about it.

The most typical way your network gets infected with Ransomware is when someone receives an email with an attachment, usually a .zip file and, when the person clicks on this file it opens up a program that then searches the user's hard drive, and any hard drive it can find on the network, for any data file such as those created by Word®, Excel®, database programs or similar, and then encrypts the file so that you no longer have access to the files unless you pay the "Ransom" demanded by the person who initiated the attack.

As the ransomware is running it places a file on the infected computer's desktop with instructions on how to pay the ransom and restore access to your data. Ransom is usually paid by using an untraceable digital Bitcoin sent to an untraceable address on the web. Ransom's can range from just a few hundred dollars to tens of thousands of dollars, with the criminal hoping you will pay the ransom rather than spend the money on the complicated process of recovering your data through other means.

Most small businesses budget their IT operations at bare minimums and quite often will not have adequate protections, data backups or professional assistance to deal with a major data loss event, whether intentional or accidental. Just like you practice preventive maintenance for your critical lab equipment, you must also practice prevention when it comes to your technology assets. Here are a few points to consider

1. Install, and keep current, protective programs such as anti-virus, anti-malware and firewalls on your servers and individual computers
2. Maintain regular backups of your data, including off-site and off-network copies of the data
3. You, and a trusted few, should be familiarized with your network equipment and know how to shut down and/or disconnect server and storage devices should the need arise
4. Work with your IT professional to develop a contingency plan for such events
5. Familiarize all employees with the common ways malicious code is introduced to your network and the need to be diligent to prevent it

As with any quality control effort, proper education of personnel, along with regular refreshers, is the best way to protect your company and your people from this ever present threat to your and their well-being.

Dan Bailey | Lab Division Marketing Partner | dan@danbailey.com | 770-973-3683