topsOrtho™

Three Steps to Avoid the Dark Overlords of Ransomware

It starts when an innocent looking email contains a link or attachment. If you click on this link or attachment, you get a message on your screen that your data has now been locked and the only way to get it back is by paying a ransom.

The most recent ransomware in the news has a chillingly appropriate name: WannaCry. In fact, this specific ransomware—also known as WannaCrypt, WanaCrypt0r 2.0, Wanna Decryptor—has attacked various versions of Microsoft's Windows operating system.

No Apple macOS or Mac computers in an office network have been affected. It's one reason we built topsOrtho™ software for the Apple macOS. It was designed to be super secure—requiring 2 factor authentication and will not accept simple passwords. Another benefit for developing topsOrtho for Mac is Mac's unmatched speed and reliability.

Here are easy steps to ensure you never succumb to ransomware.

1 Ransomware hackers often use an email to trick you into installing the ransomware software. Train yourself never to click on a link or attachment in an email, even if the email is from a friend.

2 If you do get an email from a friend with a link or attachment, contact the friend if you weren't expecting the email. If you get an email from a business you work with, rather than clicking on the link in the email, open your browser and go on the business's website by manually entering the website name. Then, navigate to the section mentioned in the email. This prevents your browser from opening a page made to look like the site of the business, while it is really the site of the hackers.

3 If you do end up mistakingly clicking a ransomware link or attachment in a rogue email, you'll be asked to enter the admin password to your computer. It's critical that you never enter that admin password after clicking any website link or attachment within an email.

Your computer admin password should only be entered if you are knowingly installing a legitimate piece of software or when deliberately changing your computer's configuration. If you are ever asked on-screen for an admin password and the request is a surprise, click "Cancel".

WannaCry attacks your practice network via email, tricking you to install once, then spreads to the rest of your network without your help. Once WannaCry is installed on a Windows computer, WannaCry uses a "worm" to scan other Windows computers on the local network in your practice. Exploiting a Windows vulnerability, WannaCry can then install itself on those other Windows computers without the need for a human entering an admin password.

In addition to the above precautions, using Apple computers for running Apple's robust macOS operating system drastically reduces your exposure to ransomware. WannaCry did not effect any topsOrtho practices, nor any Macs running macOS.

A major reason topsOrtho is designed and built as a 100% Real Mac app—not as a Windows app or browser app—is for the renown security of the Unix-based macOS. There are other significant design reasons we built topsOrtho as a 100% Real Mac app and the net result is a smooth system that's fast, easy and reliable.

We hope this information makes you practice immune to ransomware because nobody likes to be held hostage—ever!