When Hacking is More Than a Cough

By
Jeffrey Pearson, D.O., F.A.O.A.S.M.

"Hacking doesn't affect me at all. I'm small potatoes – hackers only go after the big guys."

Guess what? Hacking affects ALL of us (and not just medical practices). I recently entered the cybersecurity world and had my eyes opened – I mean *really* opened – by an internet security friend who was working with me to secure my practice.

I was concerned because so many of us are regularly engaging in telemedicine and related technologies as we deal with the pandemic. I learned that some of the popular software that we use is susceptible to malware and other programs. "Ransomware," for example, has been in the news recently because a few very large hospital systems were held hostage by unknown hackers and had to pay out large sums of money to save all of their data from being erased or lifesaving equipment remotely shut down.

Per the Oxford English Dictionary, a hacker is someone who uses computers to gain unauthorized access to data, usually for malicious purposes. Some of them have been nicknamed "Black hats." On the flip side, "white hats" access to data is authorized in order to protect us from the "black hats" (just like in the old wild west). [This is a gross oversimplification; It bears noting that some "white hats" started out life as "black hats." Other color terms used, as well.] What follows is what I learned from my "white hat."

We are ALL vulnerable. I repeat: WE ARE ALL VULNERABLE!

It is ridiculously easy to compromise any machine connected to the internet and for that compromise to extend exponentially *world*wide. All it takes is one bad guy with a USB flash drive to insert into the computer of an unsuspecting victim. Nanoseconds are all it takes for the malicious code (hence the term 'malware') to insert itself into the computer, not just on the data hard drive, but even places where one would least expect it such as the battery running the hardware. From there, it rapidly reproduces and travels along electrical connections to find new hosts both near and far (just like a human virus).

Once released into the internet, these bits of 'malware' can hide across multiple machines across multiple continents. Some break themselves up and only perform malicious tasks when instructed to combine with other destructive code pieces. Once this occurs, it's very difficult to detect and neutralize their effects.

The scary thing is that one doesn't even require physical insertion of code into a machine in order to bring down entire systems. My white hat was able to access my office network's files in less than a minute without physically touching any of the equipment – he simply used his

When Hacking is More Than a Cough

By
Jeffrey Pearson, D.O., F.A.O.A.S.M.

smartphone! He proceeded to reveal all of the attempted intrusions into our office's computers (on the order of several per day) seeking private/protected information.

Our system was relatively unscathed, but a nearby doctor's office computer system was chock full of security breaches. Fortunately, these were mitigated using relatively easy measures. Still, the damage was done; hackers had already electronically scoured his system searching for cybergoodies, i.e. anything they could ultimately monetize (patient's identities, credit cards, etc).

We turned to examine my practice' web site, which I've had running for more than 20 years: it turns out that my internet hosting company was compromised on more than one occasion and remained so. He went on to show me how he could easily tamper with the price of gasoline at a filling station in Tennessee - if he wanted to– because they did not enact effective computer safety measures.

I could go on, but you most likely get the picture. Now, let's discuss what we, as physicians, can do to protect our patients' data and our own personal information. [You're no doubt aware that our work computers often contain some personal information in addition to practice management. Hackers can use even the smallest bits of information they obtain from a machine to learn specific aspects of your life and use it to access other parts.]

It will never be possible to prevent a determined hacker from intruding into some part of your digital life. However, **here are some tips that can help to make you less vulnerable:**

Rule #1: Be diligent. Understand how computer technology works and how equipment communicates with one another. Many YouTube videos explain the basics: the internet (LAN/WAN), WiFi, keeping hardware and software updated, etc. Watch them. Frequently.

Rule #2: Passwords. The more complex, the better. Include a combination of capital and small letters, numbers, and some characters (such as #,!, or &). Do not incorporate your name (or those of family members, pets) or your company into your password. Fortunately, we're nearing the point where passwords are becoming meaningless as systems can be keyed to individual biometrics such as facial recognition and fingerprints. Two-factor authentication is now in use, as well.

Rule #3: E-Mails: NEVER OPEN A MESSAGE FROM A SENDER THAT YOU DO NOT RECOGNIZE AND TRUST. Learn about "spoofing" and "phishing." Many an organization (including our government) have had their systems compromised because an employee opened a supposedly innocent e-mail. For example, one might receive an email informing you that there was a problem with a recent order, the problem being that you never ordered the item(s) in the first place and as soon as you respond to correct the sender, you're compromised. Ransomware often compromises institutions in this manner.

When Hacking is More Than a Cough

By

Jeffrey Pearson, D.O., F.A.O.A.S.M.

Rule #4: Set up a firewall. A firewall is a piece of hardware used to filter all communications between your computers and the outside world. Don't just purchase one and hook it up. It's essential to take the time to configure it appropriately for it to do what it has to do. *I use a brand called Firewalla that allows me to organize my home and office networks efficiently and alerts me to any unwanted/unexpected intrusions from potentially malicious entities. Because of its cloaking, any cyber-entity that attempts to look into my network sees absolutely nothing. [That's a good thing.]* Also, all of your cyber components should be secure. There are known brands of routers, for example, that covertly send data to unfriendly countries without your knowledge (or consent). Consult with an expert, if necessary.

Rule #5: Choose your hardware and software carefully. Some brands, such as Apple, take their responsibility for privacy more seriously than others. Because Apple controls every aspect of their machines (hardware and software) from start to finish, they create machines that are more resistant to hacking than other brands, which are often a mishmash of programs designed by separate companies

Rule #6: Choose a reputable hosting service for your website, if you have one. Be aware that this can be difficult as outside adversaries have compromised many hosting companies. When we looked up some reputable corporate web sites, we found that they were diverting personal data to offshore agents. This begs the question "how does one find a reputable service?" Unfortunately, in light of recent cyber events, it's difficult. All one can do is follow the common sense that you'd use when you're looking to find a good physician. Do your homework, ask around, read reviews, and use critical thinking skills to parse the Information that you've gathered.

Rule #7: Hire a reputable internet cybersecurity specialist and listen to them. *And act upon their recommendations*. I was lucky to have stumbled upon my white hat. You'll have to make some calls - find out if any of your colleagues has been through this process and can recommend someone to you. Alternatively, look to see who large companies in your area are trusting for their security.

Finally, be aware that fixing your security problems might require a small capital investment but be mindful that it pales compared to the costs associated with getting hacked. Be aware that companies that have attempted to hide their compromised systems were fined extraordinary amounts for violating the public's trust.

Cybersecurity problems are not going to go away. The only choice is to remain vigilant and follow best practices. There are many excellent online reference sites on this topic. Read them and learn. Repeat often.

Dr. Pearson is founder of Medicine-in-Motion, a family and sports medicine practice in Carlsbad, California. He is a former member of the Medical Economics Board of Editors.