Keeping your Website Safe from Hackers

Most of us think, “It won’t happen to me”—unfortunately in the world of online security that’s rarely the case. A hacker’s cyber attack can spread yours and your patients’ data throughout the web. They can even get you blacklisted by Google and others when they infect your site with malicious content that can be spread throughout the web—getting un-blacklisted usually involves creating a new website; which is what I had to do when I was hacked.

Most personal and small websites are “Pre-Scripted Templates”. They are public and the most vulnerable on the Internet—they’re easy for hackers to attack. “Custom Scripted Systems” have far less of a chance of being hacked. Most of today’s website security systems are more of a chain-link fence than a firewall, and only repel the obvious, clumsy attacks (about 97% of cyber attacks). An effective cyber-defense must also include a plan to account for the other 3%. When attacked, your server provider will lock you out of your website and you may need to rebuild part or all of it, if the problem cannot be resolved—this can be very expensive and disruptive. **Your best defense** is to make sure that your website provider has a sound “Web-site Maintenance Plan” that: (1) keeps regular backups of your website and its data, (2) moni-tors for cyber attacks, and, (3) quickly fixes or restores your website when attacked. Check with your website provider to make sure that you have this kind of support.

Hackers can attack your website in many ways:

- Insert seemingly credible files that contain hidden commands that expose your hidden data
- Hijack and control or even destroy your website
- Divert your users from your website to theirs for whatever nefarious reason
- Block you and your patients out of your own website
- Insert information into your files that can crash your system or ruin your reputation
- Shift money from your website accounts to theirs if your website handles money

The 97% common website attacks can be resolved by inexpensive, effective techniques such as a “Website Maintenance Plan” and trained employees who can *spot breaches*—simply; *your website just isn’t working as it should*.

Unfortunately, there is always the possibility that the other 3% of hackers will get through. Hackers are savvy and not all “auto-detect” anti-hacker systems can keep them out, although, some do a better job than others. To *fully* repel that 3%, you need external proactive human monitoring to detect and quickly fix issues before they blow up in your face. There has to be some human monitoring to help spot a hack and deal with it appropriately and quickly before any damage is done. My “TheBioEngineeringCo.com” website has a very effective Mainte-nance Plan to keep out the 97% and an *auto-detect* anti-hacker system to make us aware of when the other 3% attacks. It also has human monitoring that has kept *all* hackers out since its inception, repelling over 100,000 attacks.

If interested, other than using an effective Website Maintenance Plan, you can also employ an effective, inexpensive auto-detect anti-hacking system that can be found at the following link: http://shop.heavenknows.biz/hacker/malware-control-services.html, where you can also obtain human monitoring support if desired.