Physicians: Protect Your Data from Hackers in 5 Steps

By Martin Merritt

Doctors have a lot of valuable personal and professional data on their laptops and other devices. Here are five simple ways to keep that data secure.

Source: Physicians Practice

According to a recent CNBC report, hackers may have stolen personnel data and Social Security numbers for every single federal employee last December. If true, the cyberattack on federal employee data is far worse than the Obama administration has acknowledged.

J. David Cox, president of the American Federal of Government Employees Union, believes "hackers stole military records and veterans' status information, address, birth date, job and pay history, health insurance, life insurance, and pension information; [as well as] age, gender, race data," according to the report. This would be all that is needed for cybercriminals to steal identities of the employees, divert funds from one account to another, submit fake healthcare claims, and create fake accounts for everything from credit cards to in-store credit card purchases.

Although physicians maintain personal and professional data which is especially valuable to thieves, you are not the federal government. Make it hard enough on cybercriminals, and they will move on for lower-hanging fruit. Readers Digest offers good advice in five simple steps in its article, "Internet Security, How not to Get Hacked":

1. Be aware of what you share.
On Facebook, Twitter, or social media, avoid posting birth dates, graduation years, or your mother's maiden name — info often used to answer security questions to access your accounts online or over the phone.

2. Pick a strong password.
Hackers guess passwords using a computer. The longer your password and the more nonsensical characters it contains, the longer it takes the computer. The idea here is that longer, more complicated passwords could take a computer 1,000 years to guess. Give 'em a challenge.

3. Use a two-step password if offered.
Facebook and Gmail have an optional security feature that, once activated, requires you to enter two passwords: your normal password plus a code that the companies text to your phone to access your account. "The added step is a slight inconvenience that's worth the trouble when the alternative can be getting hacked," CNET tech writer Matt Elliot told Readers Digest. To set up the verification on Gmail, click on Account, then Security. On Facebook, log in, click on the down icon next to Home, and then click on Account Setting, Security, and finally Login Approvals.

4. Use Wi-Fi hot spots sparingly.
By now, you probably know that Internet cafés and free hotspots are not secure. You shouldn't be doing your online banking from these spots. However, the little button that turns off your laptops Wi-Fi so that your laptop cannot be accessed remotely is also handy. In Windows, right click on the wireless icon in the taskbar to turn it off. On a Mac, click the Wi-Fi icon in the menu bar to turn off Wi-Fi.

5. Back up your data.
Hackers can delete years' worth of e-mails, photos, documents, and music from your computer in minutes. Protect your digital files by using a simple and free backup system available on websites such as Crashplan and Dropbox.

Take this basic instruction and build on it yourself. Google, for example offers advice expanding on the concept of "strong passwords." The worst thing you can do is use "dictionary words," the word "password," and sequential keystrokes, such as "1234" or "qwerty," because the hacker's computers will try these first. For e-mail, pick a phrase, such as "[m]y friends Tom and Jasmine send me a funny e-mail once a day" and then use numbers and letters to recreate it as a cryptic password. "MFT&Jsmafe1ad."