

Active Blog
General

www.active-technologies.com
info@active-technologies.com

Hackers That Harm You Physically?

First, a brief discussion of the meaning of the word "hacker." Originally, it referred to anyone who was skilled at writing computer code, but today it has come to mean someone who breaks into computer systems or networks without permission. There are also distinctions between "black hat," "white hat" and "gray hat" hackers, depending on how they use their skills. In this discussion, we're referring to the modern common meaning, or "black hat" hackers.

Once upon a time, hacking into a computer was regarded as a minor crime most often committed by mischievous youngsters with too much technical knowledge and too much time on their hands. Many people didn't think of it as "real" criminal activity at all and hackers enjoyed admiration and respect from many in the IT community.

That's changed over the years, as the growing ubiquity of Internet access has exposed more businesses and individuals to attacks that can cost them time and money. A system taken down by a hacker can result in loss of business or even cause trouble in personal relationships when emails or IMs go unanswered. User-created data deleted by a hacker may be impossible to replicate exactly. Sensitive information accessed by a hacker can result in other crimes such as identity theft or can make businesses vulnerable to fines and other sanctions for violation of governmental or industry regulatory compliance requirements.

That's the reason hacking into other systems or networks is now a felony or high level misdemeanor in many states (usually referred to as "unauthorized access" or "breach of computer security"). In Texas, the offense classification depends on the amount of damage done (although it's still a crime if no damage at all is done). If enough damage is done, hacking can become a first degree felony - carrying the same penalty as murder.

Even though it's now recognized as a serious crime, hacking is still considered by most folks to pose primarily a financial risk. But we're beginning to see that it can be much more dangerous, actually putting people at risk for their lives. A few weeks back, we discussed how the way wi-fi networking is being implemented on some commercial airplanes could make it possible for hackers to access the plane's navigation and control systems. It's easy to imagine the dangers inherent in that, whether or not the hacker had malicious intent.

An interesting AP article that I ran across last week illustrates another way in which hacking can put your life in danger. It seems some modern implanted defibrillators communicate with monitoring devices over unencrypted transmissions that could be intercepted. It's worrisome enough that those transmissions sometime contain the patient's birth date, social security number and other personal information. But the article goes on to suggest that a particular talented - and particularly malevolent - hacker could reprogram the devices to prevent them from doing their job. And their job is to save the life of a person whose heartbeat becomes abnormal.

http://money.cnn.com/2008/03/12/news/companies/heart_device_hacking.ap/?postversion=2008031207

That's really not a big risk with the current devices, because you have to be physically very close to the patient to program them. However, newer technologies are expected to work at greater distances. Although makers of the devices say they will contain "stronger security," we all know that security measures don't always stop hackers.

Active Blog
General

www.active-technologies.com
info@active-technologies.com

This also gets you thinking about all the other ways in which medicine has become dependent on computers. In our recent article on robotics, we mentioned that some doctors are now performing "long distance" surgery (also known as telesurgery), using robotic arms at the surgical site that they control from hundreds or thousands of miles away. But how does the surgeon communicate with the robotic system? Over a high speed data link, of course.

According to Wikipedia, one surgeon in Canada performs many of these remote surgeries over a VPN connection using a "non-dedicated fiber optic connection that shares bandwidth with regular telecommunications data." A VPN (virtual private network) is designed to provide a secure connection through a non-secure network, but many VPN products have been found to have vulnerabilities that can be remotely exploited. Could a hacker interfere with the surgical process in a situation where a small slip of the scalpel is enough to kill the patient?

But there are much less dramatic ways a hacked connection might cause harm or death. Drug prescriptions and orders for treatments are now often stored on computers and accessed via portable Tablet style computers by nurses and doctors making rounds in the hospital. This means that information is transmitted over a wireless connection. It's conceivable that a hacker could intercept that data and make changes to it - increasing the drug dosage to a fatal amount, for example, or canceling a treatment that's essential to the patient's health.

And the possibilities for death by hacking extend far beyond the medical field. We've all seen the movies where traffic lights are computer-controlled from a central location. If a hacker can change the lights to display green in both directions, fatal accidents could ensue. And an attack that shuts down the electrical grid would pose potentially life-threatening problems both for patients on life support in hospitals and those who depend on powered oxygen machines at home.

Computers have made our world better in a lot of ways, but they have definitely opened up new dangers, as well. Personally, I'm glad that not everything is computerized yet. The first barn swallows of the season arrived at our house yesterday, a week earlier than last year. While it might be more convenient if their migration were controlled by computers so we could know exactly when they're coming, it makes me feel good to watch them dipping and soaring, completely oblivious to all our fancy machines.

If you require additional information or assistance with this item, please give us a call.