Social Engineering

A Hacking Story

Typically when we think of hacking, we think of technical hacks. Some hooded, socially rejected fiend sitting in the dark corners of the world pumped up on way too much caffeine plotting the demise of your systems through some cleverly thought out computer virus. Although these types of hacks do occur, at a surprisingly high prevalence in the healthcare industry, the scarier type of hack is social engineering. This is a real threat that is often not addressed in staff training sessions or our operating procedures. And that is just how the social engineers of the world want it.

So what is social engineering, any way? Social engineering is the charming way of hacking into your data. Hackers rely on human interaction, often trickery, wit, and charm, to break into otherwise secure environments. Because it relies on the weakest link in any technical chain, the human element, it is one of the biggest threats in security. Let's look at an example of how a social engineer hacker may gain access to your systems:

Suzy, a clinic manager, has her place of employment listed on FaceBook. No biggie, right? She hasn't enabled all the security features on her personal FaceBook page, so her page is fully visible to the entire computing and wired world (meaning everyone with access to the internet). Again, this is Suzy's personal page, if she wants the world to her information, which has no bearing on the clinic's security, right?

George is a social engineer that is on the hunt for medical personally identifiable information, since he knows that it sells ten times the price than any other type of personally identifiable information, including credit card information George sees that Suzy's place of employment is at a medical clinic. He starts his attack.

George calls the clinic at a time Suzy has posted she will be out of the office on a vacation (Aruba does look nice this time of year). George calls and asks to speak to Suzy. Patti answers the phone and lets George know that Suzy isn't there, a fact he is already aware of. Patti asks George if he can be of any help. George laughs, acting like he forgot, and tells Patti how jealous he is that Suzy is in Aruba while they are stuck at work. Patti now believes that George is a trustworthy person, because he knows a fact that she believes would otherwise be unknown had he not been in communication with Suzy.

Now that George has Patti's trust, he tells her that he has been working with Suzy on quoting them a new server. Now he has no way of knowing if they have a sever, use an electronic medical record, or how technical the office is. But that doesn't really matter. If the office is not technical, he will spin a story about how Suzy is looking to get a server to support the adoption of an EMR or Practice Management System. Remember that social engineers are con artists, they will keep spinning until they either get what they need or they are road blocked enough that they move on to an easier target.

Patti confirms to George that they have a server in the office. He asks her to grab some information that he forgot to get from Suzy. Patti places him on hold and grabs all the information he needs to remotely access the server. George gained access to the server, thanks to Patti's trust in him. He infected their server with Ransomware (a type of computer virus that encrypts the entire hard drive and holds it hostage).

Think this couldn't happen in your clinic? Think again. Social engineering is a rampant problem, not only in the healthcare industry, but across the board. As technical security factors become more stringent, the hacker's reliance on social engineering techniques will continue to rise. The above story actually occurred in a health clinic not too long ago. Luckily, the clinic had a solid contingency plan in place and was able to recover all but one day's worth of data. This hack still resulted in thousands of dollars of lost work. The breach also had to be reported to the government and every patient was informed that their data was at risk due to the laxed security procedures.

Continued on pg 2…

Social Engineering continued from pg 2…

So how could this hack have been prevented? The first step is to ensure that all your employee's understand the risk their personal social media pages pose to your clinic's security. Train your staff on locking down their personal social media pages. Inform them of the dangers, not only to the clinic, but, also to their personal property and well being, of sharing too much information (like vacation schedules) on social media. Create and implement a hearty social media policy, which includes personal page posts or references to the clinic. Sending out periodic security reminders as part of your compliance training procedures will be necessary at first to reinforce the anti-phishing (this story is an example of non-technical phishing) procedures.

Patti could also have played an important part in preventing the hack. Patti should have asked for George's name and number and told him that Suzy would contact him when she returned. Or she could have confirmed with Suzy's supervisor (in this case the doctor) the right to share information with George.

The clinic did mitigate their risk slightly, by having a solid contingency plan in place that helped them to combat the ransomeware. However, they did incur the cost of the lost data – which included lost medical data that could cause patient harm due to lack of accessibility to access records. They had to bear the cost of a new server and restoration of data.

Don't let your clinic be the next victim of social engineering. Conduct a risk analysis to determine your areas of vulnerability, create and implement robust policies and procedures and train your staff thoroughly (not just a HIPAA 101).

Sarah Badahman
HIPAAtrek
www.HIPAAtrek.com