HIPAA Hints

Healthcare – Why Secure Your Mobile Device?

By Josh Black, Manager of IT Security Administration

What is a mobile device? Mobile devices include laptops, pagers, smartphones, tablets, flash drives, portable hard drives, CD/DVDs, and more. Due to their portable nature, mobile devices are wonderful at providing greater efficiency and productivity. However, if they are not secured properly they also present a greater threat due to their ease of being stolen, misplaced or surreptitiously compromised and used as an attack vector. The number one recommendation for securing mobile devices is encrypting the entire storage space on the device or, at a minimum, the confidential data on the device. For the purpose of this article, your smartphone will be the focus.

This year there were more than 11,000 iOS (iPhones/iPads) and 2,500 Androids reported as connecting to users' UAMS email accounts. Last year there were less than 9,000 iOS and Androids combined connecting to users' UAMS email. These numbers tell me that more and more people are using their smartphone or tablet for work purposes. Now imagine how likely it is for just one of those mobile devices to become compromised, with resultant individual or institutional harm. Loss of personal information or UAMS patient information are predictable outcomes, but that is merely the beginning. Compromise of the organization's control over its assets, information, or reputation are additional possible outcomes. It is vitally important that every person take ownership of securing their devices and safeguard not only their personal information but that of the organization as well. Let's look at a hypothetical scenario of what could happen in the event that an Android device was compromised. Though hypothetical, it is a scenario that is very likely to occur. The Android is chosen for this exercise simply because there are vastly more known exploits for them than for iOS at the time of this writing.

Jane Smith has an Android Galaxy S5 and she does everything from her phone. Since she has a full-time job working for UAMS and she has another full-time job at home as a mother and wife, she keeps a lot of information stored on her phone, which goes everywhere she does. On her phone she has all of the social security numbers and birthdates for herself and her family. She also keeps all of her passwords saved to each of her 20 different accounts, which include her two banking accounts, UAMS domain account, two personal email accounts, social networks, and more. Needless to say, if someone gains access to Jane's phone, they could do a LOT of damage.

Jane knows she has a lot of sensitive information on her phone, so she created a passcode to make it harder for someone to gain access. However, Jane needed something easy to remember so she used the numbers from her home address (2142 Dream Lane) as her passcode. Jane's busy and she didn't feel like taking the time to encrypt her phone, because to do so with her Android phone, which has 64 GB of storage space, could take up to two hours to encrypt. That's more time than Jane had to spare. She's not concerned though, because she has her passcode set and that makes her feel secure.

One night while Jane is sleeping she receives a carefully crafted text message from a hostile attacker who obtained her cell number from Facebook while investigating UAMS. This text message, when sent to an Android smartphone, exploits a software flaw and executes instructions specified by the attacker, who is able to hijack Jane's phone without her having to read or see the message. Unlike with computers and phishing emails where you generally have to open a file or click on a link, the text message hack is able to do its dirty work without the user doing anything.

HIPAA Hints Continued Next Page

HIPAA Hints

Continued from Page 6

Now that the malicious attacker has access to Jane's phone, he realizes it's unencrypted and starts snooping around. He deletes the message used to compromise the device, and walks around the file system. Before long, he has access to all of the social security numbers and account information Jane stored on her phone. While Jane is wondering why her battery life has dropped significantly, he is selling the SSNs on the black market and he uses the account information to start a bigger project.

Using her credentials, he collects thousands of patients' information from UAMS which he then sells to identity thieves and insurance scammers on the Dark Web. At this point, he pivots using Jane's UAMS account to email other UAMS employees a phishing email to collect their information and plant persistent malware. After a while he has access to several other UAMS accounts, including an administrative user who essentially owns the computer network. With information from the UAMS Online Checkbook site, he identifies a handful of monthly payroll employees whose salaries are significantly above average. As the end of the month approaches, he logs into the UAMS Employee Self Service portal using his vetted accounts and starts rerouting their pay check deposits to a bank account under his control – a little credit union Jane uses to operate the kids' sports team. Monthly payroll runs, and several hundred thousand dollars are wired automatically to that account. Using the bill pay service, he immediately forwards that money to a bank in Lagos, Nigeria. From there, it will be routed to a number of banks in Eastern Europe, where the money will be withdrawn by mules and handed over to the organization he works for.

This hacker was very careful in his work. For instance, once he hijacked Jane's phone, he was sure to clean up after himself so she never knew he was there. He was also very patient while collecting patient information and other UAMS employees' account information. He waited until just the right time to formulate his attack and reroute all of their paychecks to his stolen bank accounts, and, after he was done, he closed the accounts and cleaned up his tracks. Another big score was he sold all of the patient information on the black market. The banking system was unable to reverse most of the transfers, and the hacker, emboldened by his success in Arkansas, is setting his sights on another, much larger teaching hospital – this one on the West Coast.

Due to the breach that occurred, several employees had thousands of dollars stolen and UAMS now owes the Office for Civil Rights of the federal government $2M in fines and UAMS has lost the trust of its patients. After months of investigating, the forensics team at UAMS, along with the FBI, have narrowed the point of attack as Jane's Android phone. Jane now realizes what all she had on her phone and how much harm it caused not only UAMS, but her and her family as well.

How can smartphone users protect themselves from such attacks? They can start by encrypting their device. Secondly, it's important that when a security patch or update comes out that you apply it. A lot of the updates that are released for smartphones or tablets are to fix the vulnerabilities in the device. Lastly, never keep confidential information on your mobile device. This includes emails, notes or documents with personally identifiable information (such as dates of birth of your family members or your children's Social Security Numbers) or patients' PHI (Protected Health Information) in them, photos of patients, etc. Mobile devices are much easier to hijack or hack into, and they are often lost or stolen. Each person really needs to evaluate the risk they take by keeping confidential information on their device. In the end, you will hopefully realize that it's not worth it.

UAMS has several policies available that identify what needs to occur to secure your mobile device and to safeguard patient information or Protected Health Information. I have listed them here for your convenience:

a. **3.1.17 Mobile Device Safeguards**
   http://www.uams.edu/AdminGuide/PDFs/Section 3/3_1_17_Mobile_Device_Safeguards.pdf
b. **3.1.38 Safeguarding Protected Health Information**
   http://www.uams.edu/AdminGuide/PDFs/Section 3/3_1_38_Safeguarding_PHI.pdf
c. **3.1.44 Photographing Patients**
   http://www.uams.edu/AdminGuide/PDFs/Section 3/3_1_44_Patient_Photography_Audio_Recordings_Videography_and_Other_Imaging.pdf
d. **7.3.03 Computer Device Custodial Practices to Protect Confidential Information**
   http://www.uams.edu/AdminGuide/PDFs/Section 7/7_3_03_Computer_device_custodial_practices.pdf
e. **7.3.12 Enterprise Data Integrity & Encryption**
   http://www.uams.edu/AdminGuide/PDFs/Section 7/7_3_12_Enterprise_Data_Integrity_and_Encryption.pdf

Please contact the IT Technical Support Center at **(501) 686-8555** if you have questions or need assistance with securing your mobile devices. You can also submit your questions or requests on the Self Service page in ServiceNow located at **https://uams.service-now.com/navpage.do**.