Secure Your Text Messages with Whatsapp or Signal

We've all been texting for the past 10 to 15 years. Back in the flip-phone days, texting was a sideshow. These days, most people text more than they call. Texting is easy, quick, and quiet. But, it has one big problem: it’s not really secure.

Regular Short Message Service (SMS) messaging does have its benefits. You can send an SMS from any phone to any other phone, even a dumb phone. However, since it’s not secure, it’s not an acceptable way to send private information. Apple’s iMessage (the blue bubble) is encrypted, but Apple has never had a third-party audit of its encryption.

There are two apps that can help solve this problem: Whatsapp and Signal. Whatsapp is the most popular messaging app in the world, with more than one billion users. Signal was designed by Moxie Marlinspike, one of the most knowledgeable security experts of our time. Both Whatsapp and Signal use end-to-end encryption. This means that messages are encrypted on the sending phone and can only be decrypted by the receiving phone. No one else, not even Whatsapp or Signal themselves, can read it. The Signal protocol is open and has been reviewed by third-party auditors to ensure its security.

Setting up either app is as easy as it gets. You download it from Google Play or the App Store, enter your phone number, receive a validation code, and that’s it. Both apps will scan your address book and see who in your contacts use Whatsapp and Signal. You’ll start appearing in their address books, too. That’s it: Open the app and you can start communicating securely.

The main difference is in the number of users (Whatsapp has many, many more, so your friends may already be using it) and what metadata is recorded. Metadata is essentially call records. If a court order was served on Whatsapp, they can supply the time and data of any calls or messages, even if they couldn’t provide the content of those messages. Signal only records the phone number you used to register and the last time you connected to the server. Since that’s all they record, that’s all they can provide. They keep no call metadata whatsoever.

It is also important to note that neither Whatsapp (owned by Facebook) nor Signal (owned by Open Whisper Systems) will sign Business Associate Agreements for HIPAA compliance. However, they are much better than regular SMS.

Also in This Issue

Pg. 3 How to Recognize a Suspicious E-mail
Pg. 6 Cryptomining Presents Network Threats
The IT Project has a lot of interesting projects in place that we hope members will take advantage of to benefit their organizations, staff and individuals they serve. Also, your input on what we can do, investigate or help to organize is always welcome. Please share your thoughts by writing to me at rgordon@njamhaa.org.

We are partnering with the New Jersey Innovation Institute (NJII) to help educate and onboard agencies to the New Jersey Health Information Network (NJHIN). We recently held a webinar to explain the program and qualifications and to sign up agencies to participate. The exciting part of this program is it is open to agencies that were not able to participate in Meaningful Use, as well as substance use agencies. A key advantage of joining an HIN is getting admission, discharge and transfer alerts.

Information about NJHIN can be found at http://njii.com/njhin-2/ and here is a brief explanation from their website:

“NJII’s New Jersey Health Information Network (NJHIN) Shared Services Platform is the New Jersey State-designated entity to build a collection of services that enable a statewide Master Person Index (MPI) and Health Provider Directory (HPD). These services support our primary-use case, which is achieving an automated Transitions of Care (TOC) program through which the NJHIN accurately and efficiently delivers Admission, Discharge and Transfer (ADT) notifications to connected New Jersey Health Information Exchange (HIE) participants, such as providers and long-term and post-acute care (LTPAC) organizations. Moreover, the NJHIN facilitates connected participants' queries to the New Jersey Immunization Registry. Additional NJHIN services include a Common Key Service (CKS) and the Active Care Relationship Service (ACRS) to help with patient matching and patient-provider attributions, respectively.”

Our second project is to help agencies conduct HIPAA required annual security risk assessments.

“The Security Management Process standard in the Security Rule requires organizations to ”(i) implement policies and procedures to prevent, detect, contain, and correct security violations.” (45 C.F.R. 164.308(a)(1)). Risk analysis is one of four required implementation specifications that provide instructions to implement the Security Management Process standard. Section 164.308(a)(1) (ii)(A) states:

“RISK ANALYSIS (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization].” [Visit https://tinyurl.com/y7nagrb9 to read Guidance on Risk Analysis.]

The IT project has teamed up with ComplyAssistant to offer a modified version of its complete assessment tool. The tool being offered is a web-based portal that conducts interviews regarding HIPAA security requirements. Your answers are then reviewed and commented on by staff at ComplyAssistant. Upon completion, ComplyAssistant will give the agency a certification that a compliant security assessment has been completed. We have negotiated a healthy discount for an initial group of agencies who will sign up for the service. For more detailed information on this initiative, contact June Noto, Vice President, IT, Human Resources and Administrative Services, at JNoto@njamhaa.org or me at Rgordon@njamhaa.org.

Finally, we have our free educational workshop series. Each year, we offer trainings on IT issues that we think our members would find valuable. In past years, we have had billing trainings for clinical and billing staff, power Excel, introductory HIPAA, HIPAA updates, mobile device management, HIPAA and social media, what to look for in a firewall and many more.

This year, I have a few ideas of trainings for us to conduct, but I would really like to hear from you as to what trainings you would like to see and would attend. Send me an e-mail at Rgordon@njamhaa.org or call me at 609-838-5488 x 215.

To see a listing of trainings we will be holding, go to http://www.njamhaa.org/free-trainings.

On October 18th, we held a webinar on Defining Agency Value through Discovery Data Mining. Value-based payments are here - but how do you define value? The NJAMHAA IT Project and TenEleven Group demonstrated how members can leverage data analytics tools to perform Discovery Data Mining exercises that will help discover and articulate an agency’s value proposition. In early November, we held a workshop on cyber liability insurance. Other workshops I am putting together are how to work more efficiently with Outlook, SharePoint® document management for users, Medicare billing update, HIN HIE Meaningful Use update and Power Business Intelligence (PowerBI).

Let me know what you would like to see.

Ron Gordon
IT Project Director
A cross the world, 269 billion e-mails are sent every day. It’s estimated that the average business user will receive 96 e-mails per day by 2019 (source: Radicati).

Given our reliance on the medium, it’s no surprise that e-mail is one of cybercriminals’ favorite methods of attack. According to the National Cyber Security Alliance, 85 percent of U.S. organizations have experienced phishing attacks and 30 percent of people have opened phishing e-mails.

There are simple steps you can take to ensure that you don’t become a victim of a cyberattack. Somewhat like a poker tell, suspicious e-mails contain hints that the senders aren’t who they claim to be.

Visit https://tinyurl.com/ycj9wo9z to watch a video to learn how to spot e-mail scams.

The Facts about E-mail Scams
- Suspicious e-mails engage in “spoofing”, a type of scam in which an attacker impersonates a trustworthy entity to make it more likely that the recipient will open and act on the e-mails.
  - Spoofed e-mails typically employ one of two tactics:
    - Phishing, the attempt to obtain sensitive information such as usernames, passwords and credit card details (and, indirectly, money) for malicious reasons.
    - Spreading malware by getting users to open malicious e-mail attachments or click on malicious links.

This article was based on information published by TechSoup in accordance with Creative Commons Attribution-NonCommercial-NoDerivs 4.0 International License.

Practical Tips for Spotting Suspicious E-mails

- Look carefully at the e-mail and ask yourself the following questions:
  - Do you know or recognize the “from” address or contact’s name?
  - Does the message contain incorrect grammar or misspelled words?
  - Does the message ask you to take action on something you didn’t request, such as “Click on this link to pick the new phone you requested”?

- If the answer to the first is “no”, or the answer to the second or third above is “yes”:
  - Don’t click on links. Instead, hover your cursor over each link to determine if the address is unknown, suspicious, or misleading. Don’t open any attachments the e-mail contains.
  - If you suspect a work e-mail is a phishing attack, immediately report it to your IT administrator so he can alert your fellow coworkers of the attempted attack. If it’s a personal e-mail, most e-mail service providers provide a mechanism to report that. Visit https://tinyurl.com/ygc7vok2b for an explanation from Google about recognizing and avoiding phishing e-mails.
One of the best things about SharePoint® is the ability to collaborate on a document without having multiple copies going back and forth. By sending a link instead of the document, you will always know which one is the latest. With versioning turned on, you can easily go back to an earlier version of the document and track changes that have been made. This is very simple to do within your organization, but what if you need to work with an outside vendor or someone in another organization? In that case, usually you end up e-mailing the document. This can be complicated by the settings on the receiving server. It may block that file extension or the file may be too large. In any case, you have lost complete control of the document. Another option is to use external sharing on your Office 365 SharePoint site.

To begin, there are two ways to share documents on SharePoint. You can share anonymously or with an authenticated external user. Both ways have their advantages, disadvantages and security concerns. By default, both of these settings are turned on and available for use. This article will tell you how external sharing works and how to configure the SharePoint site to enhance the security of your data.

Anonymous Sharing
As the name implies, anonymous sharing means that anyone can access the document. This is done with a link that can be passed to anyone. The person choosing to do this can decide to make the link either editable or view only. It is very important to note that since anyone with the link that is created can access the document, you will not know who has viewed or edited (in the case where the link is editable) the document. When using anonymous sharing, you must be careful that you do not expose personal health information or any other data that is valuable to your organization. These links can be set up so that they expire after a period of time or are available indefinitely. You can only share documents and folders with this method. Some of the places where you may use this form of access is perhaps for forms such as employment applications, press releases and other announcements.

Authenticated External Access
This method of access provides more control of the information. To begin with, you are sending a link to a particular person or group of people. When they access the link, a guest user is created in your active directory and you can track the activity of that user just as you would any other user in your organization. Using this method allows you to share whole sites, not just files and folders, within your SharePoint organization. As with anonymous sharing, you can limit the access that is shared with outside people.

Configuration and Security
These features are configured on the admin console of your Office 365 site. To configure it, log in with your admin ID and navigate to Admin, Admin centers, SharePoint. On that page, you will see a tab for sharing. Entering this, you will find the settings that you can modify to enhance the security of your site. As previously stated, it is set up with a default to allow all forms of sharing. In some cases, administrators have thought that this is too big of a risk and have simply turned it off. This does make the site’s security better, but you are limiting the functionality and people will find ways to share the information they need to share and it will be out of your control.

So, if you leave it on and modify the settings for better security, you can use this feature to help your organization. For example, you can set it to allow or disallow anonymous access and, you can white list or black list domains to which invitations can be sent. You can also specify default settings for whether the document can be editable or not. You can also specify a default expiration period for the link. One other thing: You can set who can share the documents. This can be limited to users or groups of users.

External sharing in Office 365 can be a great tool for your organization. But, if it is not set up correctly, it can also cause issues.

You can find free documentation of this at sharegate.com
Does your agency issue cell phones to employees? Many do. But, once you’ve handed over those shiny new Androids or iPhones to your employees, you need to still have control over them. Many business cell phone plans do not have unlimited data, and you simply can’t afford to have employees installing music and movie apps, burning through data and money.

There’s also the problem of employees leaving and returning phones that are locked because they didn’t provide the phones’ PINs or passwords. Yes, they’ve returned their phones, but they cannot be reissued to other employees if you can’t get into them. If the employees have used personal Apple IDs on the phones, you have no way to get back into them.

This is where Mobile Device Management (MDM) can help. MDM involves a software package. Maas360 is one provider; Microsoft’s Intune is another. MDM gives you administrative control over the phones, much like Active Directory gives your IT staff administrative control over agency PC’s. With MDM, if a phone is returned and you don’t have the PIN, you simply wipe the phone from the MDM console. You can disallow apps or even permit only a few whitelisted apps. You can lock out functions from the phones that aren’t necessary for your work, if you like.

It’s even possible to use MDM with employees’ personally owned phones if your agency uses bring-your-own-device policies. MDM can sandbox agency data such as e-mail, so that it is protected from disclosure. You can keep employees from saving e-mail attachments, photos and the like to the phones. If any employees leave on bad terms, you have the safety and peace of mind of knowing you can wipe agency data from their phones.

Smartphones have changed our lives since they first came out. Make sure your IT plan includes MDM.
There is a growing threat to networks and individual PC’s called cryptomining. Cryptomining is the acquisition of crypto currency. It is acquired by performing a complex algorithm search that returns the code for the cryptocurrency that is being searched. This process requires a large amount of resources to be completed. So, criminal organizations have taken to using ransomware style attacks to infect PC’s so they can do the searches and acquire the currencies. This is increasingly becoming a preferred activity for criminal organizations because the risk is low since most people will not report it, and the rewards are greater. It is said that 10 of 100 users will pay a ransom, but 100 of 100 computers do the searches for the currencies.

As in your traditional ransomware malware, the malicious code is delivered in two ways. It can be delivered as a link within an e-mail or website that will install the code on the infected machine or it can come from a hacked website or pop-up ad that then runs the Java code for the cryptominer.

It must be noted that these programs do not steal any data or encrypt the PC’s; this would be counterproductive to what they are trying to do. The reason why this is dangerous on our networks is the lost time due to system slowness and also the wasted time for helpdesk personnel while troubleshooting this as a hardware problem. It also takes a significant amount of bandwidth, which slows down the entire network.

One of the locations that has been known to use this type of exploit is Github, which is a completely legitimate source for shared code that provides applications and scripts for computers. However, these criminals will download the code and inject their own code into it and then place the code back on the site. When the unsuspecting users download and install the package, it infects the computers.

One of the more dangerous versions of this software is called Winstarnssmminer. This miner will actually cause your PC to crash if you try to disable it. Here is how it works: When it is run, it starts two svchost processes. The first one looks for antivirus software and if it finds tougher software, it does nothing. If it finds weaker AV, it will disable it and start a second process that will do the mining. It then marks this as a critical process, which will cause the PC to crash if it is not stopped. This software has been confirmed to have mined more than 133 monero, which equates to $28,000.
Website Infection
The other way that cryptomining is done is through the use of a hacked website or an ad put on a website. This works by injecting the code into an ad or a website that when visited, runs the code and takes over your processor to do the mining operation. This is the more popular way of doing this. For every 10 installed miners, there are 90 miners running on a website. This is because the more computers doing the mining means more profits for the miners.

These miners are only in operation when the websites are open. This means that no code is stored on the victims’ PC’s. However, they are very difficult to find, since closing the page makes them go away. Cryptomining is becoming so prevalent that some of the miners seek and destroy other miners on the infected PC’s.

What Can I Do About It?
Knowledge is key! Now that we know how these work, we can use that to help limit the infections. The first and most important thing is to train your staff to not click on unknown links in e-mails and to not install software off the web. These two steps will eliminate most of the installed infections.

Having a modern antivirus such as Symantec Endpoint Security or Malwarebytes that can scan the websites that are opened will also block these apps. There are also extensions available for Google Chrome called Minerblock.

Another important thing to have is some form of a webfilter, which will allow you to block websites that have exploits on them. You can also blacklist sites that may not fail, but are known to have the infected content. Barracuda and Sonicwall make particularly good webfilters, but there are many other ones available.

Conclusion
Cryptomining may not pose the threat to your data that ransomware causes. But, it is still a serious threat that could cause problems on your networks, lost man hours, and possibly purchasing of parts that were not needed.
Although the terms EMR and EHR have become somewhat interchangeable, that has not always been the case and there are those who believe the distinction between the two should be understood by those who use them. The Office of the National Coordinator for Health Information Technology (ONC) has put forth distinctively different definitions of these terms summarized as follows:

Electronic Medical Records are the digital versions of patient data, including notes and information, used in offices, clinics and hospitals for diagnosis and treatment.

Electronic Health Records may be used to provide a larger view of a patient’s care as they collect information from all clinicians involved in administering care to a patient.

Another term described by the ONC is Personal Health Records (PHR) that contains the same types of information as EHRs but is managed by the patient. It may also contain information from a wider range of sources such as personal devices and the patient themselves.

For more detailed information, please see the following article: bit.ly/2xASfYk

---

**EMR vs EHR**

- Provides more in-depth data tracking over time
- Gives reminders for patient screenings and checkups
- Improves patient care from the individual provider

- Simplifies sharing up-to-date, real time information
- Access to tools for clinical decision support (CDS)
- Full medical history, from x-rays and labs to patient allergies