Recently, the IT project became aware of a report from the British Broadcasting Corporation of a virus on the Apple iPhone. This virus is a Java based script and accuses the user of viewing pornography or something similar and locks the browser. It requires the user to pay 100 pounds with an ITunes card (this is England) to unlock the browser; however, this virus is easy to get around by simply clearing your browser cache.

The latest updates to the iOS also close the hole that allowed the virus to come in and fix the error. Now, if this virus is easily fixed and is already patched, you may ask why this is significant.

To answer that question, we have to take a trip down memory lane. Seven or eight years ago, the first ransomware found on a PC was a browser hijack with the FBI logo that demanded a payment of 100 pounds sterling (equivalent of $150 to $200) via a card purchase from CVS. In the years since then, as we all have seen, ransomware has become increasingly invasive. We had computer lockers that would lock computers on boot and transform the executable to a random name so that it would be harder to find. This was followed by the crypto locker viruses that encrypt the files; we are all too familiar with this today. Some of them will now make copies of your files and threaten to distribute them if the ransom is not paid!

Now that we have looked at the past of ransomware, we can understand the significance of the fake browser locker on iPhones. Instead of looking at this as a minor exploit that has been patched and is no longer a problem, we need to look at this as a “proof of concept” that will lead to bigger and worse infections in the future.

The reason for this is simple. The desktop and laptop that we have been using for 30 years are not the future of computing. It could not even be called the present of computing; it is firmly the past of computing. Yes, the devices will remain

Continued On Page 3
Fee for Service (FFS) is now here and agencies are trying to figure out how to save money, but the "bad guys" don’t care. Cyberattacks are on a sharp rise and healthcare organizations are prime targets. Small to medium healthcare organizations are considered low-hanging fruit for easy attack. So, how do you protect your organization's IT systems, keep up with the latest technology and also comply with HIPAA? There is no choice: You have to put layers of protection with the newest technologies, which means additional expenses.

Over the past few years, the NJAMHAA IT Project has been focusing on cybersecurity. It has played a prominent role in our two most recent annual IT conferences. The annual IT conference is a great place to learn about what is happening and available solutions. The IT Project has also looked for cybersecurity solutions and is working with vendors to offer agencies discounts to make these solutions more affordable for the nonprofit community. Here are just a few of the solutions we suggest with brief descriptions. Over the next few weeks, I will be e-mailing our community with more information on the solutions and how to take advantage of these offers.

The IT Project is currently working with a vendor to offer a discounted agency risk analysis tool designed specifically for healthcare organizations. We are still working out the details, so watch for our big announcement.

Is your firewall more than three years old? If so, it probably is time to consider an upgrade or another solution. Having a firewall that simply blocks ports is not good enough. You need a firewall that inspects all Internet traffic and conducts deep packet inspection for a wide variety of threats. It should also include URL blocking and a variety of detailed reports on internet usage. The IT Project is working with Domain Computer Services, which allows you to design and schedule phishing tests, monitor results and then schedule training campaigns. If you don’t have time to manage another system, the IT Project can help implement this for you. KnowBe4 is offering 25% off one- and two-year contracts and an additional 20% off three-year contracts. I will be e-mailing much more information on this solution.

Finally, is your organization taking advantage of Microsoft's free Office 365 cloud for nonprofits? Microsoft spends millions of dollars on security and is on the leading edge to block cybersecurity risks. Your organization can have its e-mail system and file storage on the Microsoft cloud and take advantage of Microsoft's security. The IT Project has helped several organizations move to the Microsoft cloud and we can answer questions and help implement a plan to migrate to Office 365.

Paying attention to your organization's risks and security is a must or the cyber criminals will take your organization down.

Regards,

Ron Gordon
Director, IT Project
RGordon@njamhaa.org
Protect your Agency from Ransomware with KnowBe4 Training

Continued From Page 1

KnowBe4
Human error. Conquered.

for a while and there are some places where they will stay. However, we see the increasing use of handheld devices. That means the smart phone and tablet.

You can be sure that if we see this, the criminals also see this. Ransomware builders have shown us that they are nothing if they are not adaptable. They rely on their criminal activity to make money. They are more than ready to change their plans of attack as the face of computing changes.

We have seen this many times already. It used to be said that one of the best reasons to have a Mac was that there was no one creating viruses or exploits for them. In recent years, we have seen the creators of viruses start to focus on the Mac more and more. As we work on Macs, we have seen a proliferation of the MacKeeper “application”. This scareware app comes into the Mac through a download or an infected website and is packaged to install alongside another program. It may not be invasive, but again, as a first step to much worse, it is highly significant.

Since we now rely on phones and tablets so much and keep most of our lives on these devices, it would be extremely naive to believe that the segment of the population that uses these viruses for personal gain are not going to work hard to infect them. With that, we need to protect ourselves in this the same as we do with our PC’s and laptops.

Training Equals Protection

First and foremost is training. Your staff is the weakest link in your company and network and they are under attack by cybercriminals. How can you know if your employees will click on phishing e-mails or a ransomware attack occurs, causing a breach of data or encrypting all your network’s data? It happens every single day to someone at some organization. It can and will happen to yours.

No matter how many levels of security your agency may have in place - such as spam filters, firewalls, anti-virus software, anti-malware and more - cybercriminals figure out how to get e-mails that are phishing for information, possibly even HIPAA protected information, to your staff. Ransomware e-mails steal and encrypt computers and network data, causing havoc and downtime. And if you don’t have a good backup strategy, you may just need to say “bye-bye” to your data, or pay a ransom.

Staff need to be aware of the signs of what an illegitimate e-mail looks like. One of the major things to be careful of is links in every e-mail. If by viewing the link, you can see that it goes to a different spot than it says, the e-mail is most likely malicious. Other things to look out for are attachments and sender e-mail addresses.

Under the HIPAA/HITECH regulations, you are required to perform a risk assessment and test your network to see how vulnerable it is. And we have the perfect solution that serves not only this requirement, but your training needs, as well.

KnowBe4 and the IT Project Offer Cost-Effective Solutions

KnowBe4 provides targeted training and periodic assessments through different forms of attack vectors. They will send an e-mail to users and test if they click on the links or open the documents attached to them. This is the most effective way of curbing this type of attack.

The KnowBe4 system also has a large library of on-demand, interactive trainings available in several languages. You can roll out trainings and then throughout the year, send out phishing tests to make sure your staff are not clicking on illegitimate links anymore. The system comes with extensive reports to show results of tests, and track training campaigns and identify who still needs more training.

KnowBe4 is a subscription service with one- to three-year contracts and four levels of service and features. IT Project and NJAMHAA members will receive a 25% discount on each contract and an additional 20% off if you sign up for a three-year contract. The full service includes the phishing and training service. If you would like just the phishing system or just the training system, you can contract for either of those and pricing will be 50% off the full service fee.

If you are interested in this offer, need more information or links to the training library to review full videos, would like to set up a webinar to learn more and/or view the management console and receive pricing information, please contact Ron Gordon, Director of the IT Project, at RGordon@njamhaa.org or 609-838-5488 x 215.

If your agency does not have the time or staff to roll out this type of project, the IT Project can help implement, administrate and run this for you!

Contact Ron Gordon for more information about this service. We would be happy to take this much needed task off your plate! Give us a call today to learn more about this necessary solution or e-mail Ron at rgordon@njamhaa.org.

To learn more about KnowBe4 and take advantage of their free tools, go to www.knowbe4.com.
KRACK: it is as Serious as it Sounds
By Art Powis, Tech Specialist I, NJAMHAAN

Recently, the IT project has been made aware of a serious threat to wireless networks. The threat known as KRACK, which stands for Key Renegotiation Attack, can be used to read any data that is passed on wireless networks. This is a serious threat, so it is important to know about it.

Before we discuss the attack, it is important to know a little about how a wireless network works. Wireless networks are by their very nature less secure than wired networks because the information is broadcast over the air in exactly the same way that a TV or radio channel is broadcast. This means that anyone between the transmitter (your phone, tablet or laptop) and receiver (the wireless access point) can monitor or intercept the signal. Also, all wireless cards are not directional; the radio broadcast goes out in all directions. This means that the signal from the transmitting station can be seen from anywhere in the pattern. It is a relatively simple matter to read these signals as they pass from transmitter to receiver.

To combat these issues, over the years, the IEEE (Institute of Electrical and Electronics Engineers) have come up with various forms of encryption. The first was WEP, followed by WPA and finally WPA2. All of these are supposed to use some form of a randomly generated code to keep someone in-between from being able to access the data. It is precisely this code on WPA2 that has been cracked. WPA2 uses a four-part handshake to connect the wireless device with the access point at the third step of the handshake. The KRACK method takes advantage of a flaw that the randomness is not as random as it is supposed to be and can use this to access the data that is passed.

Since it is a flaw in the WPA2 code itself, it is device independent. This means that any WiFi using WPA2 is at risk. Android and Linux devices are at a higher risk than Windows and Mac devices because of another flaw in the code that lets the encryption key be reset to all zeros. Researchers have cracked every device that is using WPA2 encryption and as they get better at it, they find better and faster ways to hack into the data being sent. All they really need to do is it is a copy of some known data that is sent clear and a similar packet that is sent encrypted. And with these two small pieces of information, they can read all the data sent among stations on wireless networks.

What Is Not Affected?
Since this hack is only for data transmitted on the wireless network, hackers cannot use this to read data stored on drives. If the websites you use are secured with HTTPS; they add another layer of encryption, so these websites are safe for the most part. Also, VPN traffic is not affected since it is also secured with a unique key. The only caveat to this is that older forms of web encryption (SSL 1.0, 2.0, TLS 1.1..) are in themselves vulnerable to being accessed and traffic from them can be read. And if your VPN has a weaker encryption key, it could be penetrated. The good thing about this is that all the electronic health record sites use the latest TLS encryption, which has not yet been cracked.

What Is Vulnerable?
Attackers can use this method to access any information that is sent in clear text. This includes, but is not limited to, usernames, passwords, credit card numbers and protected health information. Worse yet, since this type of attack is at the physical level of the OSI model, it can be used to inject malicious code into computers, sending ransomware and other viruses to encrypt or steal your data.

What Can You Do about It?
At the moment, this is a rare instance that currently does not have a solution. The first recommendation is to, wherever possible, use a physical connection to the network. With a physical connection, the data cannot be intercepted by a device that is listening outside of your network. Microsoft and Apple are working on updates to combat this issue, but at the moment, there is not one for either device. So, another recommendation is to keep checking for updates to your devices. You should also check your wireless access points for updates and implement these updates as they become available. Some manufacturers have already patched the issue, but they do not have an automatic update like Windows, so you will need to perform the updates manually. If you have older devices that are not updated any longer, it would be a good idea to replace them with newer devices that will be updated. This would also give you a speed advantage on your network since these older devices will be much slower.

It is also a good idea to periodically check to see if your signal is going outside of your building. If it is, you should relocate the devices so that the signal covers the inside of your building, but does not go beyond the walls. It will be much harder for hackers to use this kind of attack since you have to be in radio range if the signal does not leave the building; the attacker would have to be inside to accomplish it.

So, at the moment, the best advice on this is to keep patching your network devices, phones, tablets and PC’s as they become available and to check on your physical security to know where your signal goes. Some manufacturers already have patches to fix this issue, so you should check the websites for your access points and routers to see if updates are available.

Knowing the threats are out there in the wild will enable you to know what to look for to keep your network secure.

Use the URL below to read an article with a list of companies that have released patches and updates to firmware, published by ZDNet.

tinyurl.com/y79z9d6h
Another Threat to Look Out For: New Ransomware Tech Support Scam

A new type of ransomware scam has been detected. It uses a seemingly innocent tech support approach to convince users to spend money to resolve issues. It may come in the form of a fake software update or through an ad. Instead of maliciously encrypting your files, the malware, once installed, will run at every startup.

Appearing to look like a legitimate Windows warning message to persuade users that it’s authentic, it displays a false warning with a phone number to call for tech support. The contacted representative may then attempt to establish a screen sharing session to resolve the issue and request you pay to complete the process.

To attract new co-conspirators to the world of cybercrime, the originators of the code used to infect its victims are offering involvement with no cost (and an even split of the profits) to wannabe criminals. This development opens the door for expanding the growth of phishing-related malicious attacks on individuals and businesses.

According to an article published by KnowBe4 and as reported by ZDNet, the victims are infected with Dot ransomware by opening email used to carry the payloads to the recipients. While large-scale proliferation has not yet been seen, it may only be a matter of time before the publicity generates an increased interest from the general public.

For more details on this subject and others from the world of cybercrime, please use the following link: bit.ly/2sNTG12

Call Rob Molinaro for all your data and telecommunication needs.
Tell him that the IT Project referred you!
215-922-1862
rmolinaro@choruscommunications.com

Gene Landino
gene@huntertechnologies.com
732.542.9292

Sandra Rocha
Client Development Executive
908.347.1317
Microsoft Planner, Free for Non-Profits, Worth a Look

Many agencies have moved to Microsoft’s Office 365 platform for e-mail. Office 365 offers much more than just an e-mail host or even all the benefits of Exchange. SharePoint and OneDrive are the best known, other than e-mail. However, Microsoft is adding new apps to Office 365 all the time. One of the new additions is Planner.

Planner can be seen at tasks.office.com and is available to nonprofits using the free E1 plan. It is a task planner for groups. You create groups of Office 365 users and assign tasks to them. Then, they can either update these tasks as ‘In Progress’ or complete them. It’s also possible to make notes on tasks.

The nice thing about Planner is that it’s very easy to use. The UI is simple and does not get in the way. It’s all about task management and that’s all it does.

An agency with a small IT department could use Planner as a simple helpdesk ticketing system. Users could enter their own technical problems into Planner; IT staff would record their responses and close out tasks, and even closed tasks would be documented. Supervisory staff could see at a glance who had done what and what tasks remain outstanding. There’s no hardware or software to buy. You just need a web browser and an Office 365 login.

That is not all Planner can do. Because it’s a very simple app, it’s easy to adapt to just about any situation. Any time you have a team that needs to divide up and manage tasks, Planner can come into play.

Microsoft is currently developing a Planner app for iOS and Android. Unfortunately, it is not yet released. It is possible to access the mobile site on your phone’s browser. Microsoft has been aggressively developing for both platforms and the app will not be far away.

Planner’s simplicity, ease of use, and inclusion with Office 365 make it well worth a look.

Web-Based PowerPoint Alternative Microsoft Sway May Be What You Need

Presentations for meetings go hand in hand with PowerPoint. It hasn’t changed in years. If you’re making a presentation, you use PowerPoint. Now, Microsoft offers a new alternative called Sway. Sway is part of the Office 365 package, so if your agency is using Office 365, you already have access to Sway.

Sway is not a complete replacement for PowerPoint. It won’t make charts for you, but it can handle text and graphics quite easily. Since Sway is web-based, your presentation exists on Microsoft servers and can be accessed through a web browser. No worries about incompatible software versions or losing the flash drive your presentation is on – just log on from anywhere.

Sway can also add content from OneDrive, Facebook, and YouTube as easily as content stored on your computer. Doing so is very easy and doesn’t take up space in your presentation.

Since Sway is web-based, you don’t need to worry about storage space. You can keep your presentation on Microsoft’s servers as long as you like. If you need to review it again, it is just a login away.

If you’re going to be doing a presentation and aren’t happy with PowerPoint, Sway may be the answer for you.
Enhance Windows 10 Performance with These Tips

Now that Microsoft’s Windows 10 has been available for a little while, users may be looking for some useful helpful hints, tips and tricks to maintain or improve its performance. One such source of information was recently written by Ed Bott and published by ZDNet.com online.

It contains a variety of performance and maintenance subjects with details on how to use the tools available to better control your Windows 10 experience. Information is provided to guide users through areas such as finding ways to reduce battery drain, hard drive maintenance and system recovery techniques. Battery maintenance control can be found in the Settings section. Hard drive maintenance can be found by typing “defrag” in the search box area, selecting “Defragment and Optimize Drives” and observing the status displayed. Information regarding system recovery options may be found by typing “Create a recovery drive” in the search box. More advanced topics include controlling UEFI firmware settings, troubleshooting mode, safe mode and other advanced startup settings.

In a similar approach to Windows system control, maintenance and troubleshooting, an article written by Chris Hoffman and published at the How-To Geek website provides more helpful information. His article covers various system utilities available in Windows such as memory diagnostics, resource monitor, performance monitor and computer management and administrative tools. Memory diagnostics can be used to determine the status of your total installed memory by restarting your PC to ensure that nothing is loaded into memory before the test begins. Using the resource monitor will allow you to see how your CPU, disk, network and memory are being affected by the processes running on your computer. The performance monitor will gather data from many different sources through a time period that can tell you how changes have affected your system performance.

The broad spectrum of Computer Management and Administrative tools contains many Microsoft Management Console (MMC) elements to assist you in the maintenance of your system. These tools can be found either by name in the Start menu or by searching in the menu. Other more powerful and possibly damaging tools affecting user accounts, disk cleanup, local group policy, registry edits and system configuration are available. These should be researched and understood before using.

Please see articles at tinyurl.com/ybkjyr7q and tinyurl.com/ycg9kz5v for more information.

Windows 10 Creators Update Features Several Enhancements

Most people run Windows, and that means updates. Every week, there are at least a few updates, patching bugs and security holes, offering improvements, and the like. Microsoft has recently come out with Windows 10 Creators Update, which is a large update for Windows 10.

Creators Update includes improvements to Cortana. Have you ever used Siri or Google Now on your phone? Cortana is Microsoft’s virtual assistant, and you can use it to talk to your computer in the same way. Creators Update allows Cortana to plug into more apps and increases its functionality.

There are also improvements to Microsoft’s new Edge browser. Edge was built as a completely new browser and has no code from Internet Explorer. Most of us use tabs in a browser to open several websites at a time. Creators Update adds a preview ability. By tapping on a drop-down arrow at the top of an Edge window, you can see a preview of every tab you have open.

There is also a Maps update to encourage use of the Maps app. You’ll need a touch screen for this. If you draw a route in the Maps app, it will instantly calculate the distance between the starting point and the endpoint. It’s just the thing to determine if the shortcut your co-worker knows about actually is shorter.

As with any update large or small, you should test Creators Update to make sure it works with your current system, programs, and web applications. If it passes the test, it can make your PC work a little better.
Less expensive equipment can often do the job perfectly well. Are you keeping an eye on the budget? Who isn’t? Good enough phones and computers can cost hundreds less than their more expensive counterparts. Sometimes good enough is good enough.

For many years, you had to spend money for quality. If you wanted a good computer, you had to spend a fair amount of money. If you wanted a good smartphone, you had to spend a fair amount of money. Budget laptops and phones were often so underpowered that using them was miserable. That’s not as true as it once was. The most extreme example is the Raspberry Pi. This $35 microcomputer is used by hobbyists to run just about anything you can think of – weather stations, Wi-Fi access points, smart home systems, and the like. It’s not a very high-performance machine, but it can do a lot. There are even people who use Raspberry Pi as desktop computers. It does have USB ports for a keyboard and mouse and will plug into an HDMI monitor. With a specialized version of Linux, it can make an acceptable desktop computer.

Now, it’s not likely that your agency is going to start issuing Raspberry Pi computers in place of the desktops and laptops that you currently use. But, it does raise a question. Do you always need the best?

Perhaps you issue agency-owned smartphones to your staff. The iPhone 7 is going to cost $700 new. Top-end Android phones cost a similar amount. While those are very capable phones, there are also phones like Motorola’s Moto G and OnePlus’s line of phones. These phones may not have all the bells and whistles like near field communication or a fingerprint scanner, but they come with a processor that is capable enough and provide a very usable experience.

If you’re buying many phones, those savings can add up.