The NJAMHAA IT Project was recently asked to provide written instructions for administrators to wipe a phone in Office 365. Many agencies have turned to Office 365 to host their mail. It offers all the benefits of having your own Exchange server without the costs, time and effort.

However, loss of phones does happen, and when a phone is lost, you need to be able to wipe it quickly. The procedure is not quite the same as in Exchange, but is similar enough. NJAMHAA has made this document available on its website at:

http://www.njamha.org/it/resources/WipingaphoneinOffice365.docx

Please feel free to download it, along with other resources, as you need.
As Fiscal Year 2017 approaches, I happily pass the torch of this editorial section to Ron Gordon, the newest Director of the IT Project. But, all can be certain that I will be contributing to the content of Bits and Bytes and will continue to provide technical direction to our member agencies.

This surely has been a year of changes for everyone. New Jersey is moving to a Fee-for-Service environment and our members have been struggling with figuring out how they will pay their employees with inadequate reimbursement rates and potentially not being able to treat their current client population.

As we forge ahead to FY 2017, the IT Project is stronger than ever, and we encourage you to get involved. Join our Billing Supervisors’ Committee or our Quality Assurance and Performance Improvement Committee to gain a better understanding of how different organizations are handling the new changes that have already happened, and those that are pending. These are challenging times for everyone. We are all stressed to the limit. Join us at the August 22nd IT Professional Advisory Committee meeting and let us learn about what keeps you up at night. We are currently scheduled to have a presentation on why EHR implementations fail. Easter Seals Solutions will be on hand to answer any of your questions. But, a more important reason to attend is so your voice can be heard. As I’ve written in the past, we only meet four times a year, but the impact you have will go much further!

To join any of these groups, write to Ron at rgordon@njamhaa.org

Peace to all .. and my wishes for a fabulous and safe summer.

June Noto
VP, Information Technology, Human Resources and Administrative Services

“The IT Project is stronger than ever, and we encourage you to get involved.”

Not only does this new environment present challenges, but also the threats from afar, such as the potential to be attacked by cybercrime, or ransomware, or any other number of changes that put them at risk makes for extremely stressful times.

So, I want to let you know that the IT Project has your back! We always have! We don’t just provide technical assistance and advice, but we also have helped get budget modifications for EHR software and hardware requests approved. We have made many recommendations over the years that have assisted the NJ Division of Mental Health and Addiction Services to help you get what you need. But, many organizations do not realize that we perform these activities, so I encourage you to reach out for assistance. The staff at DMHAS are not technical, and don’t always understand how your request will impact your operations in a cost-effective way. So, we provide the guidance they need, so you can get what you need.
Ever since the Internet came to be, there have been people trying to use it for nefarious purposes. Viruses have been spread through floppy disks, e-mail and the Web. There is a new and nastier variant of virus called ransomware, and it is something of which every agency should be aware.

Ransomware is typically spread via the Web through a compromised website. It may be a website you go to often. It will download onto your machine and encrypt your files – not only those on your local computer, but also any files on a network drive that your computer can access. Once your files are encrypted, you will receive the option to pay a ransom (usually within two weeks) to get access to your files again, or the private key will be deleted after two weeks. Once the private key is deleted, your files are irretrievable. Payment is done via bitcoin, so it is not traceable.

With private-key encryption, it is simply not possible to crack the key in a two-week period. In most cases, people will pay the ransom to get access to their own files. This simply encourages the criminals to try again with slightly different versions of their codes.

Internet filtering can help mitigate this risk by blocking access to websites that are known to be compromised. The most important tool in your arsenal is a good backup strategy. If your backup strategy is solid, you can simply restore files from the previous day’s backup and avoid paying. Backup strategy has always been important, but ransomware makes it that much more important.

Don’t pay ransom for your own files. Make sure your backup plan is solid. It could save you thousands of dollars.

Ravi Ganesan
President
484-704-7412
rganesan@coresolutionsinc.com

Mike Carruthers
401.780.2300 ext. 115
www.smartnet.com
Since the release of the iPhone in 2007, smartphones have become part of our daily lives. Many of us rely on our phones not just for calls and texting, but also for e-mails, navigation and all the things that apps can provide. Many employees may use personal phones to get their agencies’ e-mail; other agencies issue agency-owned phones to employees.

It is doubtful that your agency will be dealing with the FBI. However, it is quite possible to run into similar situations: for example, a former employee with a copy of their work e-mail on a personal device, returning an agency-owned phone, which is now locked and unusable, or simply installing personal apps and games on an agency-owned phone.

Many agencies are using Office 365 as an e-mail system, which provides MDM at a cost-per-user basis. There are other systems available, like Meraki, which may be free for a certain number of devices. In any case, MDM has to be part of a modern IT structure. Is yours up-to-date?

In an article by Mathew J. Schwartz available at InfoRisk Today, cybersecurity expert Alan Woodward calls attention to the increase of online crime and how it is being addressed by international law enforcement agencies. Noting that these types of crimes have moved past the methods of independent individuals and into the realm of sophisticated criminal organizations, Schwartz points out there are greater risks to the victims. Estimates of fraud-related losses range from $3.4 billion to $18.7 billion annually. Joint efforts being conducted across Europe and North America have been able to track, shut down and prosecute many suspects.

For the complete article, please use the following link:
http://tinyurl.com/jo4ntc4
Lessons Learned (the hard way)

They say that experience is the best teacher. However, a lot of times, the cost of these “lessons” can be very high indeed. The following article will talk about an issue that has happened and what should have been in place before that would have made recovery a lot easier.

Active Directory Recycle Bin
Have you ever accidentally deleted a user from an active directory? Was the user mail enabled? If you answered “no” to these questions, be very thankful and learn this lesson from the people who answered “yes.”

The first thing on this issue is to make sure that your domain is at a minimum of Windows 2008 R2 functional level. At this level, there is a recycle bin from which you can quickly restore an object. Unfortunately, this feature is NOT a standard feature. That means that it is not turned on by default and after you deleted the object is not the time to find out that you do not have this ability. And you will be forced to go to backups and cause downtime while you do an authoritative restore and then fix all the group memberships. Or you can run the following command right away:

```cmd
Enable-ADOptionalFeature -Identity 'Recycle Bin Feature' -Scope 'Forest' -Target DOMAIN
```

To do this, log onto your operations master and make sure that you are at the correct functional level. The easiest way is to go into Administrative Tools, open Domains and Trusts, right click the Domain and select Raise Functional Level. This will tell you the level and allow it to be raised if needed. Next, from the Administrative Tools, right click on Active Directory Powershell and run it as an Administrator. Input the command changing DOMAIN to the netbios name of your domain. The command will run and you will need to click on “yes” to allow this.

Once you have the Recycling Bin for the Active Directory, you will have to use LDP.exe to restore the user. By default, the container with the deleted objects is not displayed. The following steps will allow you to see the container with the deleted objects.

To Display the Deleted Objects Container
1. To open LDP.exe, click Start, click Run, and then type ldp.exe.
2. On the Options menu, click Controls.
3. In the Controls dialog box, click Load Predefined drop-down menu, click Return deleted objects, and then click OK.
4. To verify that the Deleted Objects container is displayed:
   1. To connect and bind to the server that hosts the forest root domain of your AD DS environment, under Connections, click Connect, and then click Bind.
   2. In the View menu, click Tree, and in BaseDN, type DC=\mydomain, DC=com, where \mydomain and \com represent the appropriate forest root domain name of your AD DS environment.
   3. In the console tree, double-click the root distinguished name (also known as DN) and locate the CN=Deleted Objects, DC=\mydomain,DC=\com container, where \mydomain and \com represent the appropriate forest root domain name of your AD DS environment.

Once you have enabled the container to be displayed, you can now restore deleted objects from the Active Directory. Below are the steps to recover a single item from the recycle bin using LDP.exe.

To Restore a Deleted Active Directory Object Using Ldp.exe
1. Open LDP.exe from an elevated command prompt. Open a command prompt (Cmd.exe) as an Administrator. To open a command prompt as an Administrator, click Start, in Start Search, type Command Prompt. At the top of the Start menu, right-click Command Prompt, and then click Run as Administrator. If the User Account Control dialog box appears, enter the appropriate credentials (if requested), confirm that the action it displays is what you want, and then click Continue.
2. To connect and bind to the server that hosts the forest root domain of your AD DS environment, under Connections, click Connect, and then click Bind.
3. On the Options menu, click Controls.
4. In the Controls dialog box, expand the Load Predefined drop-down list, click Return Deleted Objects, and then click OK.
5. In the console tree, navigate to the CN=Deleted Objects container.
6. Locate and right-click the deleted Active Directory object that you want to restore, and then click Modify.
7. In the Modify dialog box:
   1. In Edit Entry Attribute, type isDeleted.
   2. Leave the Values box empty.
   3. Under Operation, click Delete, and then click Enter.
   4. In Edit Entry Attribute, type distinguishedName.
   5. In Values, type the original distinguished name (also known as DN) of this Active Directory object.
   6. Under Operation, click Replace.
   7. Make sure that the Extended check box is selected, click Enter, and then click Run.

A key point to understand and remember with AD Recycle Bin is that you must restore hierarchically: a parent object must be restored before a child object. So, if you were to delete an entire OU and all its contents, you must first restore the OU before you can restore its contents.

In Windows 2012, Microsoft has made this a mandatory feature and has also hardened the delete to make it harder for this mistake to happen.
A little over a month ago, Microsoft released Windows 10 to the wild and by all reports, there have been a decent sample of early adopters (approx. 5 percent of OS’s are now Windows 10). The main focus on this article will not be if you should install it, but some of the pitfalls and good and bad of the operating system.

On the whole, it functions similarly to Windows 7. So, there should not be too steep of a learning curve on how to use it. This is similar to when Microsoft went back to the more traditional file menu in Office 2010 after the pearl style that they used in Office 2007. The return of the traditional start button is much appreciated. Those who have gotten used to the metro menu can still use that if they want. But, how many of us on Windows 8 bought one of the start menu emulators? Boot speed is much improved over Windows 7, even on older equipment. In newer OS’s, boot systems appear to operate at similar speeds as in the past.

Microsoft is also talking about the new edge browser. The company claims it is faster, but let’s face it, Internet speed is much more dependent on the ISP connection than the browser you use to get to the Web. So, you will probably not see a large amount of improvement there.

Another thing that needs to be discussed is updating. By now, we have all heard and discussed how Microsoft no longer lets you decide which updates to install and when. It only allows you to delay updates. For an IT person who wants to know what is going onto your systems and what will be affected, this is not the best idea. So, we will pass on that and move to what is a potentially worse problem. Built into Windows 10 is the ability for Microsoft to use any system as an update deployment system. What this means is that once a machine has the updates, Microsoft can publish that machine and use it to download updates and apps to other computers. Microsoft says they are doing this to speed up the delivery of the updates and apps. This should be turned off on PC’s on your network. You can do this by using a registry key or going through the menus in the system settings. There are many places on the Web that can show you the steps on how to disable it. The main concern is this seemingly innocuous feature could be exploited by a hacker somewhere.

The last area we need to discuss is program incompatibility. During the upgrade, Windows 10 checks your system to find what programs are compatible. The first one it finds a problem with is Symantec 12.1 Antivirus. Since this is one of the more popular antivirus programs, this is a potential major issue. There is a maintenance patch that will allow you to do the install. Another group of programs that have had issues are VPN software. The standard Cisco client will not work on Windows 10 at all. You can get around this by installing third-party software such as Shrew Soft VPN. For those who have a SonicWALL VPN, the latest version of the software will work with Windows 10. Most older DOS-based programs will require modifications to get them to work, and older FoxPro-based databases will not work at all. You need to be aware of what programs are being used and what ones need to be tested for compatibility before installing upgrades.

In conclusion, Windows 10 is a vast improvement over Windows 8.1, but less so over Windows 7. There are significant areas that need to be looked at for security and functionality. And as with any major upgrade, thorough testing and identifying the software you use is a must. Windows 10 is the way of the future and we will need to embrace it, but remember, testing of all areas should be done.
A recently revealed security risk has many users wondering if even the most seemingly innocent electronic devices can open the door to a hacker. This threat takes the form of your wireless keyboard or mouse using a USB dongle to transmit its signal. Chris Rouland, CTO for cybersecurity firm Bastille, states the operation known as a ‘MouseJack’ can be implemented for an inexpensive amount of hardware and some malicious lines of code.

Considering that almost all personal computers using Windows, Mac or Linux operating systems can utilize wireless keyboards and mice, this flaw can have huge consequences for individuals and large corporations. If you use any of these devices in question, it is strongly urged that you contact the manufacturers to see if you are at risk.

For more detailed information please see the following article: http://www.foxnews.com/tech/2016/02/25/wireless-mice-keyboards-open-to-mousejack-attack.html?intcmp=hpff
The Internet has changed our lives. Instead of writing letters, we send e-mail. We store Word documents on network drives and Sharepoint instead of placing paper printouts in manila folders. We can even place phone calls from our laptops and video chat with people all around the world.

Nowadays, even your television and refrigerator can get in on the action. Smart TVs allow you to access Netflix and Hulu as easily as NBC and CBS. You can keep an eye on your infant with a Wi-Fi-enabled baby camera from anywhere in the world. You can unlock your door and turn on your lights, too. Your children can play with Wi-Fi-enabled dolls that will talk back to them. But, are all these things safe?

The answer is, “Not always.”

There have been several cases of baby cameras being hacked, allowing total strangers to see (and, for cameras equipped with speakers, talk to) children. DVR’s can be hacked as well. Samsung’s smart TV was recently compromised, making it possible for a hacker to access the microphone and webcam built into the TV. Yes, it’s entirely possible for the TV to watch you.

The best thing to do about the Internet of Things is the same things you should be doing for the Internet in general. Perhaps the simplest thing you can do is to change the default logon and password. Make it something secure and hard to guess. Skilled hackers may yet find a way in, but this will discourage quite a few of them. If you have a firewall at your agency, it should be configured with new devices in mind. Is it really necessary to share your DVR with the world, or only with a few select people?

Likewise, check with the manufacturers for updated firmware. DVRs, smart TVs, smart cars, smart refrigerators – all of these things are computers, and their manufacturers will issue updates for them. As new vulnerabilities are discovered, they will be patched, but you have to keep on top of it.

If your IT infrastructure allows for “guest” Wi-Fi networks, make a guest network and separate it from your existing network. Your cameras need to access the Internet; they don’t need to access your file server or your PC’s.

The Internet of Things will further change things, and give you abilities you never had before. If you have smart devices in your network (at home or at work), make sure they are included in your plan for security.

Watch the TV; you don’t want it to watch you.

Adam Feldman
adam.feldman@qualifacts.com
615.386.6755