If you use Windows, you probably know all about viruses and malware. You’ve probably got an antivirus program on your computer. Malware outbreaks are a fact of life.

But, what about the smartphone in your pocket?

Smartphones today are fully fledged computers. They’ve become part of our lives. They can access the Internet, get your e-mail, and run programs just like a desktop. And they can get malware.

Phone infection is much rarer than PC infection. In the case of Apple, all apps can only be installed through the App Store unless you have jailbroken your phone. Android does allow a user to download and install apps by changing a setting.

If you’re issuing phones to your employees, the first thing you should do is forbid them from jailbreaking, rooting, and changing the security policies on their phones. A mobile device management system can help enforce this.

Both iOS and Android manufacturers push out updates for phones, and app developers update their apps. Make sure your phone is up-to-date! If your phone is too old to receive security updates, it’s time to think about replacing it.

Just because it’s rarer doesn’t mean it can’t happen. In 2015, an altered copy of Xcode, the software Apple makes available to developers to write iOS apps, was made available to developers. Apps written with this version had malicious code automatically inserted. Some of those apps made it through Apple’s testing process into the App Store. Apps infected with malware have also been found in Google’s Play Store.

Antivirus apps are available for both Android and iOS and can provide an additional level of protection. Many are by the same companies that provide antivirus programs for PC’s. These can help protect your phone or repair an infected phone.

Make sure you’re keeping an eye on your phone as a target for viruses. The hackers certainly are.
Welcome to 2017! I hope everyone has a healthy, happy and prosperous New Year.

I would like to take a few short paragraphs to call your attention to two great resources the IT Project offers that have been around for a long time. I guess with the New Year, I am looking back with nostalgia on projects the IT Project has started and have been successful. These resources are available to all Division of Mental Health and Addiction Services (DMHAS) funded agencies and NJAMHAA member agencies. The resources have helped staff at agencies over the years by answering questions, sharing information, developing a sense of community, giving support, providing access to state resources, providing information on changes in behavioral mental health and substance abuse and just a place to vent with members with colleagues who understand.

Have I got you curious? Of course, I am referring to the IT Project’s Billing Supervisors’ Group and the Quality Assurance (QA)/Compliance Group. Both of these groups meet quarterly at NJAMHAA and each has a website for members. The website is a private “Facebook” like community or, as the developer calls it, a “Groupsite.”

The Billing Supervisors’ Group
This group has a long history. It started as a CMHC5 user group; CMHC5 was a billing application many agencies used. At the meetings, many general billing questions were discussed. It was decided that a separate group should meet to discuss billing issues regardless of what applications agencies used and this group would be open to a larger community. I believe this was in the late 1980’s, The group has been going strong since and I believe there are still current members who were there from the beginning. By coming together to discuss billing issues and changes to rules and regulations, members and agencies have benefited from the shared knowledge. Sometimes new people have joined the group with little billing knowledge and the group has helped them figure out the ins and outs and where to find resources and even members have offered to go to other agencies to help out. Over the years, the group has had NJ Medicaid and State representatives come to meetings for trainings or to answer questions. Even though the current environment has become more competitive, members of this group come help each other out and share the good, the bad or just a good laugh.

The group is co-chaired by Michele Rowe from South Jersey Behavioral Health Resources, Inc. and Judy Rios from Cape Counseling Services. Both have long careers in billing and are excellent sources of billing knowledge. Michele commented, “I find that attending the Billing Supervisor meetings on a quarterly basis is the best way to learn what other agencies are doing. It is also a great time to see if other agencies have the same problems that we are having and learn how they are dealing with the issues and who they are talking with to get answers. It also helps to know you are not alone given all the changes going on with the move to fee-for-service. The group website is a great way to interact and ask questions in between quarterly meetings.”

With all the changes happening with fee-for-service, I think this is a great resource to take advantage of. If no one from your organization is a member of the group and website, please join! The next group meeting will be on March 9th at 10 a.m. in the NJAMHAA conference room. If you cannot get here, you can call in to the meeting. If you’d like the number to call in to the meeting, contact Ron Gordon. To join the Groupsite, go to njamhaa.billing.groupsite.com/login and click on the Join Now link.

The next QA and Compliance meeting will be on January 19th at 10 a.m. in the NJAMHAA conference room. To join the Groupsite, go to njamhaa.groupsite.com/login and click on the Join Now link.

Regards,

Ron Gordon
Director, IT Project
RGordon@njamhaa.org

From the Director

Staff Contributors

Copyright © 2016 New Jersey Association of Mental Health and Addiction Agencies, Inc. Reproduction in any manner, except as authorized by the Copyright Act of 1976, is prohibited. All rights reserved.
Wi-Fi is a great convenience, and almost ubiquitous. Wi-Fi access points are inexpensive and they only need to be purchased once and configured once, and that’s it. It makes life much easier to be able to carry your laptop wherever you like in your office without having to worry about finding a network port or carrying a cable. It’s backwards compatible so when you buy a new laptop with the latest version wireless card, it will join your older network without a problem. Once you enter the Wi-Fi key, your laptop and phone will connect again automatically.

Many agencies have a very simple Wi-Fi setup. They bought access points a while ago, set up internal SSIDs, and handed out the passwords. That was good enough ten years ago, but these days, you might want to consider segmenting things off.

For one thing, anyone who gets on your Wi-Fi could be inside your network. Salesmen and consultants who have their own machines that you have no control over may ask for your Wi-Fi password to check e-mail or give a presentation. That machine is now behind your firewall. If it’s infected or compromised, you no longer have your firewall or filtering service to protect you. If the people in the office next door asked to use your Wi-Fi while their Internet was down, they could still be connecting to it.

For another, many people have smartphones today. Employees may want to put their phones on your Wi-Fi to save on their data plans. If several of them are watching YouTube or streaming Internet radio, your Internet speeds suffer.

Many modern routers and access points are capable of setting up a guest Wi-Fi or more than one network. This is a good idea. You can set up VLAN’s (virtual LAN’s) so that someone connected to the guest Wi-Fi has no access to the internal network, just the Internet. A third network can segment off personal property, like phones. It’s often possible to limit the bandwidth available to each VLAN so that Internet speeds remain fast for work purposes.

SonicWALL routers, Unifi access points, and many other access points have this capability. If you haven’t updated your Wi-Fi anytime recently, it’s something you should strongly consider. A short time of configuring guest access could save you a lot of time.
So, you want to move your data to Office 365? There are many advantages to this, but there is also a disadvantage. Most users will be uncomfortable using the web to access their files. To get around this, you could use the OneDrive for business sync, but this is very unreliable and it downloads your files to the local computer, so you may end up with multiple copies of a document.

So, how do you get around these limitations? The first way is to go in and manually map the drives every time you boot the computer, but this can be time consuming and users may not be able to do this for themselves. However, a network engineer came up with a PowerShell script called OneDriveMapper that can do the work for you. This little script can take users from active directory, hard coded in itself, or prompt for the username and password. It will then map the OneDrive for business drive and it can map other SharePoint document libraries that you specify.

Before you can use this handy little script, you will need to have a few configurations done on the computers. First, PowerShell 3.0 needs to be installed on the PCs. Next, the Windows WebClient service needs to be enabled (it uses the WebClient service to map the drives). The OneDrive for business and SharePoint sites also needs to be added to the trust sites zone in Internet Explorer. User account control needs to be set at the default level to allow PowerShell to run the script as a user. Finally, the execution policy in PowerShell needs to be set to “remotesigned”; this needs to be done as an administrator in PowerShell by using the following command: Set-executionpolicy remotesigned.

Once you have downloaded the script and configured those settings on the local computers (most of them can be set via a GPO), you will need to do some simple modifications to the script for your organization.

1. Line 79 - Add your domain.
2. Line 80 - Specify the drive letter.
3. Line 82 - If you have a custom directory, change it here.
4. Line 83 - You can specify a label for the drive.
5. Line 84 is the name you used to sign up with Office 365. (This is the part before .onmicrosoft.com.)
6. Line 89 - User lookup mode specifies how to get the user ID.
7. Line 108 is used to add mappings to other SharePoint sites. You can copy that line and insert it afterwards to add multiple drive mappings.

The script can be called from a login script or a Group Policy, to automate the procedure for adding a SharePoint or OneDrive for business site as a network drive.

Now comes the really great part. This script is a free download from the Microsoft TechNet gallery (http://tinyurl.com/zankqa).

Use of Scripted Drive Mapping for Office 365 Builds Comfort Accessing Files Using the Web

Tanner Melton tmelton@reliaslearning.com 919.655.1827
Decryption Codes Available for Ransomware

According to an article by Stu Sjouwerman of KnowBe4, the website, Pastebin, has posted decryption keys for the Crysis ransomware. This will allow victims of this ransomware to decrypt their encrypted files without having to pay the price to do so. How and why these keys were acquired and posted is not confirmed, but speculation hints at pressure from law enforcement on the responsible developers. More sources of ransomware decryption assistance can be found at bleepingcomputer.com and the RakhniDecrypter decryption tool provided by Kaspersky.

For more information, please check the following websites:
- KnowBe4’s Security Awareness Training Blog at http://tinyurl.com/h35h9pr
- BleepingComputer.com at http://tinyurl.com/zqc23dd

Ransomware is not the only intrusion to be wary of in today’s world. A new scam sometimes labelled as Blackmailware has been found to utilize social media information to intimidate users to pay to protect their reputations. A variant called Ransoc has been found to affect RedEdit, MSconfig and Task Manager, but not to destroy or encrypt users’ data.

For more information, please read an article on the Proofpoint website (http://tinyurl.com/he5uhb9).

Mike McLafferty
Sales Executive
mikem@go-domain.com
609.395.6900 x6

Chris Mangano
Vice President, Sales & Marketing
Cmangano@mercadien.com
609.689.2320

Mercadien
Leading by example.

domain computer services

Mike McLafferty
Sales Executive
mikem@go-domain.com
609.395.6900 x6

Chris Mangano
Vice President, Sales & Marketing
Cmangano@mercadien.com
609.689.2320
Microsoft is always issuing updates. Many people are still running Windows 7. If you have older computers, Windows 10 may run a lot slower while Windows 7 runs fine. As long as Microsoft is still updating Windows 7, that’s fine.

However, sometimes updates get stuck. Is your PC hanging on “Checking for Updates” for hours and never budging? It’s a common problem. There can be several reasons, but the most common is that the Windows Update agent itself is always being updated. The Windows Update agent is also running all the time in the background.

Getting unstuck isn’t always an easy process, but it’s not as hard as it seems. You’ll need to know how to stop a service, run a batch file, and manually download some updates from the Microsoft website. The first thing you’ll have to do is create a batch file.

Open Notepad and type the following text into it:

```bash
@ECHO OFF
echo Simple Script to Reset / Clear Windows Update
echo.
PAUSE
echo.
attrib -h -r -s %windir%\system32\catroot2
attrib -h -r -s %windir%\system32\catroot2\*
net stop wuauserv
net stop CryptSvc
net stop BITS
ren %windir%\system32\catroot2 old
ren %windir%\SoftwareDistribution old
ren %ALLUSERSPROFILE%\application data\Microsoft\Network\downloader old
net Start BITS
net start CryptSvc
net start wuauserv
echo.
echo Task completed successfully...
PAUSE
```

Save it as wupdate.bat. You’ll have to change the file type from .txt to .bat. Right-click on it and choose “Run As Administrator”.

Reboot your PC.

Next, you’ll need to download Windows6.1-KB3020369-x64.msu from the Microsoft website. Install it and reboot.

Run the batch file again.

Download and uninstall windows6.1-kb3125574-v4-x64_2dafb1d203c89642394a30b48b5d4b1264cd93eb9.msu.

This is a rollup package that contains more than 100 hotfixes and packages. It’s about 476 MB and may take some time to install.

Reboot your PC.

Now you need to stop the Windows Update service. Go to Start, Control Panel, Administrative Tools, Services. Scroll down to “Windows Update”. Right-click on it and choose “Stop”. Stopping takes a few seconds.

Download and install Windows6.1-KB3161664-x64.msu.

Reboot your PC.

Stop the Windows Update Service again.

Download and install Windows6.1-KB3172605-x64.msu.

Reboot your PC.

You’re done! Run Windows Update. It may take a while to get all the remaining updates, but Windows Update will work.

This is easier than it sounds.
Eighteen months ago, Microsoft released the latest version of its Windows operating system, Windows 10. Its predecessor, Windows 8, had not been widely adopted. Windows 10 brought back the beloved Start Button and integrated Cortana, Microsoft’s voice assistant, into the OS.

Until July 29, 2016, it was possible to upgrade from Windows 7 or Windows 8 for free. Many people took advantage of this offer to get Microsoft’s new OS. That upgrade offer is over, however, and now, if you want to upgrade to Windows 10, you’ll have to pay. The upgrade for Windows 10 Home is $99 and Windows 10 Pro costs $199. As nonprofits, many of us are eligible to purchase from Techsoup for significantly lower prices than that.

As of December 2016, Windows 10 is running on 23.76% of all machines. Windows 7 has not yet been dethroned, running on 47.17% of all devices. For many people, Windows 7 does the job well enough. Others changed over, reasoning that Windows 10 will be receiving updates and patches for much longer than Windows 7.

Windows 10 Pro also includes BitLocker, a hard drive encryption program, which was only available in Windows 7 Enterprise. With laptops that may contain PHI, encryption is necessary to prevent a HIPAA breach.

If you’re still running Windows 7, are you planning to move to Windows 10 in 2017?

If you still aren’t certain, call the IT Project Help Desk at 609.838.6064 for advice!
In the recent election, Wikileaks and its publishing of John Podesta’s e-mail was all over the news and the Internet. Podesta’s Google e-mail had been hacked by an unknown party. But how did this happen? Was there a vulnerability in Google’s servers? A spy on the inside? A disgruntled employee?

As it turns out, John Podesta was targeted in a technique called spear phishing. Spear phishing is a method in which the attacker sends an e-mail purportedly from someone with whom the victim interacts. In this case, it was a forged e-mail, which stated that Podesta’s e-mail had already been hacked and offered him a link to change his password. Unlike phishing scams of before, where the text was often misspelled, this looked quite legitimate – enough that even the Clinton campaign’s IT staff were fooled. They replied that the e-mail was legitimate and that he should change his password through accounts.google.com. They also suggested turning on two-step authentication, which requires him to log in by entering a numeric code texted to his phone, as well as his password.

Instead, he clicked the “Change Password” button in the original e-mail, was directed to what looked like a Google page, logged in with his username and password...and handed his credentials to someone who logged in and began sending those e-mails to Wikileaks.

What we can take away from this is to always be careful. Bringing the mail to the attention of the IT staff was a very good idea. However, using the link in the e-mail was the mistake. If you receive an e-mail claiming to be from your e-mail provider, electronic health record, IT staff, or anyone you deal with, never use the password reset link offered in the e-mail. There will always be another way to reset your password. Use of two-step authentication can also help secure your account.

Anyone can be a target of hackers. Hackers often rely on users choosing the easier way rather than the more secure way. Being security-conscious and careful can make all the difference.