NETWORKING 101

WEST VIRGINIA NETWORK (WVNET)

WV Higher Education Technology Conference 2015

West Virginia Higher Education Technology Conference 2015 "Technology in Education: Revealing the Magic" will be held at The Waterfront Place Hotel and Morgantown Event Center in Morgantown, West Virginia, on October 26-27, 2015. **Registration remains open!**

Dr. Corley Dennison, Vice Chancellor of Academic Affairs for the West Virginia Higher Education Policy Commission will be the Opening Keynote Speaker and talk about *Moving Forward: Higher Education in Transition.* Our General Session speaker will be Dr. Michael Adelman, President of the West Virginia School of Osteopathic Medicine, who will discuss *The Use of Technology in Medical Education.* On the last day of the conference, keynote speaker Dr. Robbie Melton, Associate Vice Chancellor of Mobilization Emerging Technology for the Tennessee Board of Regents will present the topic *Are Emerging Smart Devices Smarter Than You?*

WVHETC 2015 offers two Pre-Conference Workshops: *Blackboard System Administrator and XE Registration for Banner*; 45+ concurrent sessions *(on topics such as Big Data, Career and Professional Development, Distance Learning, Public Policy and Legislation, Enterprise Resource Planning, Innovative Technologies, Student Success, eLearning and others)*; poster sessions, and 25+ exhibitors. View an exhaustive list of conference sessions here: *http://www.wvhetc.com/sessions* There will be two receptions for *all* registered attendees and vendors, including a *Magic Show and Reception* after the general session on October 26 and the *Exhibitor Reception* to close the conference on October 27. View the conference schedule here: *http://www.wvhetc.com/documents/wvhetc_2015_conference_schedule.pdf*

It's not too late to register. Please visit: wvhetc.com to register and receive important conference updates.

See you at the conference!!

VOLUME 5, ISSUE 10

OCTOBER 2015

FROM THE DIRECTOR

They say that, if you keep your eye on the ball and just keep swinging, you will eventually hit a home run. This month, WVNET proved that this is true. We won the RFP from the Community and Technical College System to host their new analytics software and data. The CTCS plan is to use this effort to improve retention which will increase college completion. That, in turn, will help West Virginia build a better educated and trained workforce.

WVNET is very excited to be a part of this important initiative, and we are proud to have been chosen. We have a great team, we keep our eyes on the ball, and once again we have hit a real home run!

CUSTOMER SATISFACTION SURVEY
And this month's winner is...

The weather outside is starting to turn as is the color of the leaves. The threat of winter is very real but at WVNET the iron is still striking hot as we keep up with support of the many services we offer 24/7/365.

Each month, WVNET recognizes a customer who took the time to complete our Customer Service Survey to let us know how we are doing. We thank everyone who takes that extra few minutes to give us advice, kudos, or criticisms that can improve our service.

This month we would like to congratulate our winner, *Zana Durst*, an instructor at Mountwest Community and Technical College. Zana used our OZ ticketing system to relay an issue she had within Blackboard on a test for her students. She was assisted by two of our Network Operations' Staff, *Mike McDonald and Christopher Seckman*, with her particular issue, who both explained the problem and walked her through the process of correcting it.

Zana was pleased with her interaction, responding, *"I appreciate the patient help with the situation!"* This is another example of how WVNET, and in this scenario the Network Operations Center (NOC), is well versed in helping our customers with a variety of problems. One of the great things about our NOC is the fact that it could be absolutely anyone on the other end of the phone, with any sort of problem, and they take great pride in being able to identify the issue, clarify it, and assist customers in working towards resolution.

As always, at the end of each month, we will draw a winner, contact them by email and then send WVNET memorabilia in appreciation. Please complete our survey by looking within the incident email of any interaction that you have had with us. All comments are taken seriously and help to improve what we do on a daily basis.

Thank you, *Zana*, and thanks again to all our customers who continue to shape and improve WVNET. *(Guest article by Booker Walton, III, Customer Resource Specialist, pictured.)*

WEST VIRGINIA UNIVERSITY AT PARKERSBURG AWARDS BRIDGING THE GAP RFP TO WVNET

The nine community and technical colleges in West Virginia were awarded $25 million dollars of federal funds provided by the U.S. Department of Labor's Trade Adjustment Assistance Community College and Career Training (TAACCCT) grant program. The intention of the grant is to strengthen technical programs and their outcomes through the enhanced sector-driven career pathways, diverse instructional methods and modes, and expansion and individualization of student support.

Bridging the Gap
CONSORTIUM
WV Community and Technical Colleges

West Virginia University at Parkersburg was charged with selecting and implementing a data analytics solution to examine input from the consortium of technical colleges. The goal of the solution is to improve student retention and student services, and increase credential completion. One of the strategies for improving student success is to improve the quality and accessibility of information regarding a student's progress towards credentials earned. As the community and technical colleges of West Virginia evaluate institutional and program effectiveness, they confront many technical and organizational challenges in the collection, formatting, dissemination and reporting of information that indicates student and institutional performance.

Through a request for proposal process, a representative committee selected Blackboard Analytics as the data analysis solution vendor. In support of this vast and critical project, WVNET will remotely host and support the student data produced by the analytics software. WVNET is a vital piece in the success of WV institutions and has a proven track record of exemplary partnership and service working with higher education providers in West Virginia.

(Guest article by Kristin R. Sloter, MEd, Technology Transformation Leader, West Virginia University at Parkersburg.)

AWARD ANNOUNCEMENT

Post September 23, 2015 - Business Offices' RFP page on the website:

On September 2, 2015, West Virginia University at Parkersburg (WVUP), on behalf of the Bridging the Gap Consortium, published a request for proposal (RFP) for the remote hosting of the data analytics system. On September 23, 2015, WVUP is pleased to announce it will award WVNET the contract. We believe WVNET's experience as a partner of higher education in West Virginia will lead to the success of the data analytics program.
Thank you to the vendors who responded to the RFP for the remote hosting of the data analytics services. WVUP appreciates your participation and interest in meeting this need in the community and technical college system.

(Reprinted with permission from West Virginia University at Parkersburg, October 2015)

DON'T LET RANSOMWARE HOLD YOUR DATA HOSTAGE

Cybercriminals are making their attacks personal, remotely locking your computers and smartphones until you pay a hefty ransom.

The world of cybercrime is constantly evolving, but no area sees as much innovation and sheer creativity as that of **ransomware:** *software designed to hold a computer or smartphone hostage until the victim pays a hefty fine.*

***Ransomware** is a type of malware that prevents or limits users from accessing their system. This type of malware forces its victims to pay the ransom through certain online payment methods in order to grant access to their systems, or to get their data back. Some **ransomware** encrypts files (called Cryptolocker).*

In recent months, as the use of ransomware has skyrocketed, cybercriminals have devised devilish new ways to entice targets with growing sophistication in mimicking legitimate download installation files.

Ransomware often attempts to frighten users though social engineering. Social engineering works by convincing a victim to unwittingly comply with a malicious request through the use of trickery, fear, and emotional cues. For instance, a hacker might pose as your cable company in an email stating that they need you to fill out an attached form or else your cable will be disconnected. Cybercriminals are even using social media sites and newsgroup postings to spread the malicious code.

The methods of hiding the ransomware file from security software are improving. Curve-Tor-Bitcoin Locker (CTB Locker), which emerged in July 2014, uses embedded code to establish an anonymous connection to the Tor network. Previously, this type of malware used a Tor.exe file. Embedding Tor functions helps to avoid detection and adds an additional layer of protection for the criminals. This makes it harder for the authorities to locate and shut down the command and control servers, meaning that the malware will stay in circulation longer and its creators will have more time to develop even more virulent strains. Cybercriminals are also incorporating the latest cryptography in their file-encrypting ransomware attacks.

The FBI's Internet Crime Complaint Center (IC3) said, between April 2014 and June 2015, it received 992 CryptoWall-related complaints, with victims reporting losses totaling over $18 million. CryptoWall and CryptoWall 2.0 encrypts files on a computer's hard drive and any external or shared drives to which the computer has access. It's not just user PCs that are being targeted; a growing number of victims are being hit with ransomware that locks down mobile phones and demands payments to unlock them.

Recommendations for ransomware victims are to first turn off your infected computer and disconnect it from the network it is on. An infected computer can potentially take down other computers sharing the same network. Ransomware removal steps depend upon the type and version. Removing the malware is the easy part; accessing your data is a whole different story. Latest versions of ransomware are using advanced cryptography that make recovering files nearly impossible without the necessary key to unencrypt.

To pay or not to pay....if you are infected with ransomware and have data that you require and are considering paying, the cybercriminal will probably expect the ransom in Bitcoin or some other virtual currency making the payment untraceable. It's conceivable that criminals may restore your data if you pay them, but the official advice is that you never should. Once the hackers have your money, there's little incentive for them to restore your files. Also, seeing that they've found a victim, they might come right back and target you again.

Ransomware continued on next page

West Virginia NETWORK
Enhancing Education through Technology

Dan O'Hanlon, Director
837 Chestnut Ridge Road
Morgantown, WV 26505
304.522.7303
dohanlon@mail.wvnet.edu

Fran Barnes, Editorial Assistant
fran@mail.wvnet.edu

Also edited by:
Mike Karolchik, Manager
WVNET Media Services
mike@wvnet.edu

follow us on twitter

Follow @_wvnet

News

Newsletter Archives Here
www.wvnet.edu

So what are the best ways to avoid or mitigate ransomware dangers?

⇒ **Always use antivirus software and a firewall.** Protect your computer (and your cell phone) by using antivirus software and a firewall from a reputable company.

⇒ **Update your software regularly.** The regular reminders to update your browsers and other software can be annoying, but they are sent for a good reason. These updates protect against the constantly evolving viruses and system vulnerabilities. Most of these have automatic updates available.

⇒ **Enable popup blockers.** Popups are regularly used by scammers to spread malware. Prevent them from appearing in the first place by adjusting your browser settings.

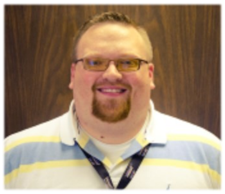
⇒ **Be skeptical.** Don't click on email links or open attachments you don't recognize, and avoid suspicious websites. For smartphones, never download applications from outside the office, Google Play Store or Apple App Store.

⇒ **Always back up the content on your computer.** If you back up your files, ransomware scams will have limited impact. If you are targeted, you can simply have your system wiped clean and reload your files.

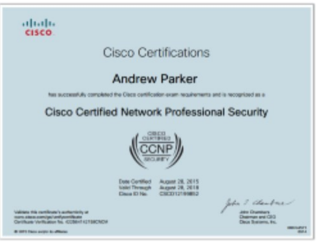
If you receive a ransomware popup or message on your device alerting you to an infection, immediately disconnect from the Internet to avoid any additional infections or data losses. Alert your local law enforcement personnel and file a complaint with the FBI's Internet Crime Complaint Center at www.ic3.gov

(Guest article by WVNET staff members Steven White, Randall Long and Barbara Long)

ANDREW PARKER RECEIVES CCNP SECURITY CERTIFICATION



WVNET's Andrew Parker recently earned his *Cisco Certified Network Professional Security (CCNP) certification*. The CCNP Security Program is a three-year certification program intended to distinguish Cisco network security engineers who have the necessary skills to test, deploy, configure, maintain, and troubleshoot Cisco network security appliances and Cisco IOS software devices that establish the security posture of the network. Before attempting the CCNP Security Certification or any of its associated security specialist certifications, individuals must meet the requirements for the Cisco CCNA Security certification and have at least one to three years of experience. *Congratulations Andrew Parker!!*



cisco

Cisco Certifications

Andrew Parker

has successfully completed the Cisco certification exam requirements and is recognized as a

Cisco Certified Network Professional Security

CISCO CERTIFIED CCNP SECURITY

Date Certified August 28, 2015
Valid Through August 28, 2018
Cisco ID No. [illegible]

Validate this certificate's authenticity at
[illegible]
Certificate Verification No. [illegible]

John T. Chambers
Chairman and CEO
Cisco Systems, Inc.