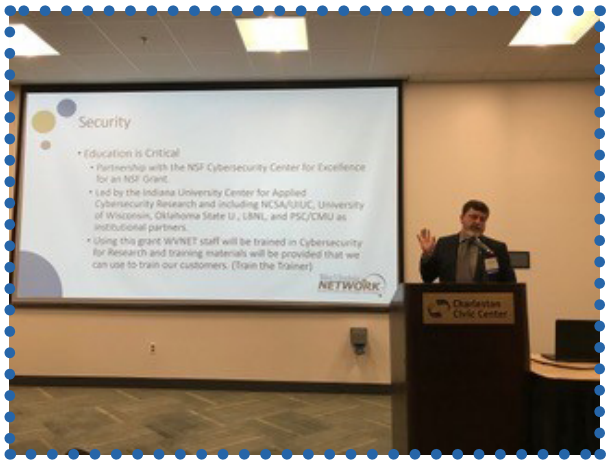
Networking 101

April 2019

Volume 9 - Issue 4

WV Local and State Government Cybersecurity Partnering Workshop



Several WVNET staff members participated in a cybersecurity workshop held at the Charleston Coliseum and Convention Center on April 18. The objective of the West Virginia workshop was to develop West Virginia specific recommendations to strengthen West Virginia local and state government cybersecurity governance and to facilitate cybersecurity partnering between West Virginia local governments and West Virginia state government. The workshop was part of the *George Mason-National Science Foundation Cybersecurity City and County Cross Jurisdictional Collaboration project*, having the goal of furthering U.S. city and county cybersecurity efforts by developing foundations and policies that enable and foster city and county cybersecurity partnerships.

The workshop included talks by: *Josh Spence*, West Virginia Chief Technology Officer; *Ron Hamilton*, CISO and *Eric Burgy*, Telecom Manager, WVNET; and *Greg Herbold*, Director, U.S. State/Local Government and Education (SLED), Palo Alto Networks.

Ron Hamilton, WVNET CISO, (*pictured*) presented on Cybersecurity and WVNET. Ron discussed the importance of education and a partnership with the NSF Cybersecurity Center for Excellence for an NSF Grant. Using this grant, WVNET staff will be trained in Cybersecurity for Research, and training materials will be provided that can be used to train WVNET customers (Train the Trainer).

West Virginia NETWORK
Enhancing Education through Technology

837 Chestnut Ridge Road
Morgantown, WV 26505
304-293-5192

Fran Barnes
Newsletter Editor
newslettereditor@wvnet.edu

Abbyrose Sisler
Intern Graphic Designer

STRATEGIC MILESTONE UPDATES

Network Operations Center

—Kim Jenkins, WVNET Operations Manager

During the month of March 2019, the WVNET Network Operations Center logged a phenomenal 935 tickets. WVNET provides technical support for our customers **24/7/365**. You may call any time to report a problem and ask for assistance. In many cases, you should be able to find an answer to your question in the information provided on our website. Our goal is to solve your problem and get you back to computing in a timely and friendly manner. Connect with us on the web at: http://wvnet.edu/resources/help-desk/ or call 304-293-5192.

Blackboard Analytics for Learn (A4L) Demo

—WVNET Distance Learning Team Lead Harmony Garletts

Interested in finding out how your Blackboard use impacts student performance? For more information on the product, please visit the Analytics Datasheet. WVNET hosted a demo of the Blackboard product Analytics for Learn on April 16. The recording is now available for viewing by request. For additional information, please contact Harmony Garletts at hgarletts@mail.wvnet.edu or 304-293-5192 x 240.

WVNET is Hiring

Come join our team! We have opportunities for a **Human Resources Generalist**, **Telecommunications Network Specialist I-II**, and **Telecommunications Network Specialist III**. These positions serve the WVNET located at 837 Chestnut Ridge Road, Morgantown, West Virginia 26505. We are one of the nation's oldest research educational networks and we're dedicated to providing service to state government, K-12, public libraries, county governments and non-profit agencies.

For more details, visit: https://wvnet.edu/about/careers/

Fond Farewells and New Faces

WVNET said goodbye to two familiar faces in March 2019, Frank Seesink and Khristan Crooms.

Frank Seesink came to WVNET in October 1998 as a Telecommunications Specialist III working with Deputy Director Allen Daugherty and the telecommunications crew, then later with Eric Burgy. Frank assisted with the design of local, campus and wide area networks, analyzed their efficiency and effective data transmission rates and prepared standards and procedures for maintenance and operation of these networks, among other things, too numerous to mention. **Best of luck, Frank, in your new endeavor!**

Khristan Crooms joined our team in May 2018 as an Intern-Web Developer. Khristan was a computer science major at WVU, and his efforts with us involved web page design and development. **Best of luck, Khristan, in your new endeavor!**

Alex Keefover recently joined the staff and became a member of the WVROCKS team helping design and manage courses. Alex earned his Bachelor of Science majoring in Mathematics, minoring in Computer Science, and his Master of Education majoring in Digital Media, New Literacies and Learning. In grad school, Alex learned how instructional designers work and how to teach math online. From Pleasant Valley, WV, when Alex is not working and has time, he likes to volunteer for the organization where his service dog came from, exercise, and take his service dog KINGSLEY for walks, play video games, and read comic books. KINGSLEY is a paws4people mobility assistance dog who helps Alex pick up things he drops, helps him remove his coat and socks, helps to push buttons for automatic doors, and so much more. **Welcome to WVNET, Alex!**

Adam McKeown recently joined the staff as an operator in the NOC. Born in Princeton, Adam moved to this area and attended West Virginia Junior College where he obtained a degree in Information Technology. Prior to coming to WVNET, Adam worked at Monongalia General Hospital on their help desk. Adam applied for the operator position after being encouraged by his friend Nathan Justice. Adam enjoys playing guitar with his friends and baking. **Welcome to WVNET, Adam!**

Years of Service to WVNET

WVNET has a long history of service to West Virginia education. Its talented staff consists of bright new minds along with dedicated employees who have been with us for many years. WVNET is certainly grateful to retain some of the expertise, experience and history as it is passed on to new generations. We acknowledge these staff members who have reached significant milestones in their careers with us during April 2019:

George Tilko – 13 years
Donna Meadowcroft – 7 years
Mary Stewart – 7 years

Walk 100 Miles in 100 Days

The Walk 100 Miles in 100 Days annual walk began on April 15 and ends on July 23. It is the largest exercise program in the state. WVNET walkers participate as community members along with other businesses and organizations from the area. WVNET employees that wanted to participate and receive a shirt paid a $10 registration fee to the Wellness Center at WVU Medicine who organized the event. WVNET has a total headcount of 15 participants. Even though the goal is to walk at least 1 mile per day, this year's walkers will be attempting to outwalk the 2018 team that walked a total of 2,987.69 miles in 100 days, an average of almost 3 miles per person per day.

April 2019
Volume 14, Issue 4

Share Your Information With Care

837 Chestnut Ridge Road, Morgantown, WV 26505
Visit: www.wvnet.edu or call 304-293-5192

From the desk of WVNET

It is very easy to find any information you need in today's connected world. Have you ever Googled yourself to see what information about you is online? A search can often provide your address history, phone number, age, birthdate, employment information, public records, and social media accounts. Consider what can be done with Personally Identifiable Information (PII) from the perspective of a cyber-criminal looking to commit identity theft or other crimes.

Children, teens, and senior citizens are all groups who especially may not realize how vulnerable they are to being a victim of cyber-crime. Senior citizens may be more trusting of the material that is presented to them online. Children and teens are growing up with technology, and may be using it to communicate with each other with only a recreational level of understanding. They may not realize that once you post online, it rarely goes away.

In order to keep information safe or private, we need to take care in sharing it, and teach cyber hygiene to those who may not understand its importance. Here are examples of how we are asked to provide information, or how people share information that should be kept private:

Store loyalty and other accounts online – When you sign up for a store loyalty program or other online accounts, you are asked to provide information such as name, address, phone number, birthdate, email address, etc. By providing this, you can get discounts on the merchandise they are selling, or can receive promotions by email. However, is that information you provide kept private, or is it sold to other companies so they can market to you? Read the terms of use and privacy policy before signing up for such a program.

Phishing Emails – Cyber criminals will offer false and unbelievable deals to get you to click on a link and provide them with your information. You may hear about a loan offer, or a notification that your order shipped and that you need to log in by clicking their link to track it. Criminals seek your information in an effort to steal your identity and use it to open up fraudulent accounts in your name. Always shop with trusted vendors, and never follow an unsolicited link in an email

asking you to log in to an account. Instead head to the website you normally use by typing it into your browser to check on your account.

Fraudulent phone calls (Vishing) – Criminals may call saying they are from Microsoft or another device/software company, telling you that your software has expired or your device is infected with malware. They may ask for money to renew a license, as a method to complete the fraudulent activity. Other criminals may pose as the IRS, pressuring you into paying taxes. Never offer payment information or personal information to someone calling you unsolicited. Always end the call and attempt to contact the organization through a publicly listed phone number that is legitimate, then see if you need to work with them on a problem.

Social Media Sites – These sites provide a relaxed atmosphere where you can chat with friends and family. The issue is that anything you post or share is likely a permanent submission that many others can access online. Oversharing on social media may lead to you voluntarily giving up answers to account security questions, like the color of your car or the town where you were born. Also, posting about being on vacation sends a signal to criminals that your home may be unoccupied and a great target for a robbery! With all this information about you on social media, be sure to set your account privacy settings so only friends can view your content. Lastly, consider deleting old, unused social media accounts to cut down on your digital footprint.

Whenever communicating with people or posting online, avoid sharing too much. When receiving emails, mail or calls asking for sensitive information (birthdate, social security number, credit card, etc.), always contact them at the legitimate address or phone number you normally use for that organization. Do not share information if you do not initiate the communication!

Below are resources on protecting privacy and identity along with practices for online security. These help you to protect yourself, your children, and your elders from being victims of a crime.

Resources:

Federal Trade Commission:
https://www.consumer.ftc.gov/topics/privacy-identity-online-security
https://www.consumer.ftc.gov/articles/0033a-share-care
https://www.consumer.ftc.gov/topics/protecting-kids-online
Stay Safe Online:
https://staysafeonline.org/
Family Online Safety Institute:
https://www.fosi.org/good-digital-parenting/ftc-share-care/
Protect Seniors Online:
https://www.protectseniorsonline.com/

MS-ISAC
Multi-State Information Sharing & Analysis Center

STOP | THINK CONNECT™