WHAT'S NEW

NEWS ABOUT CURRENT PROJECTS AT WV NETWORK

FALL 2021

West Virginia NETWORK

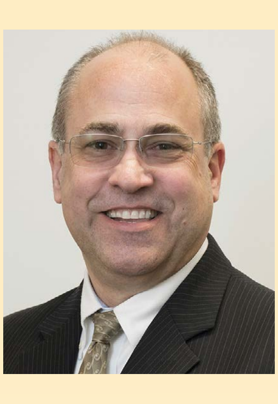
IN THIS ISSUE:

SAVE THE DATE | WVSTC 2022

WVNET and our K12 and Higher Education partners are excited to announce the return of the face-to-face West Virginia Statewide Technology Conference on July 18-20th, 2022 at the Morgantown Marriott at Waterfront Place. More information will be coming your way in the near future.

WVNET has recently adopted **Brightspace by D2L** as our new learning management system. We are working with our participating institutions to complete the implementation for the Spring 2022 semester.

If you have any questions about Brightspace, please contact Harmony Garletts at hgarletts@staff.wvnet.edu or join Cory Morrison on Tuesday afternoons at 1PM for Brightspace Office Hours by visiting our web page and clicking on Ask Your Questions (Password: Help2021).



Holiday Season + Cybersecurity

Dr. Carl Powell, WVNET Director

With the holiday season upon us, it's time to think about family gatherings, decorated houses, and . . . cyber criminals. Yes, the holidays do bring out the worst people online.

First, there is phishing – online con artists trying to trick you into giving away your login credentials or download malicious software. Then there are all of its relatives: spear fishing (targeting specific individuals), whaling (targeting senior executives), clone phishing (mimicking legitimate messages), vishing (voice phishing over the phone), and smishing (phishing over SMS text messages). Don't get me started on snowshoeing and hailstorm attacks! In short, there is no absence of criminal creativity.

And don't forget about your password. Or, I hope, your passwords. You want it to be difficult for others to guess but easy for you to remember. Remember one size does not fit all! You should use different passwords for your work email and your personal email, so if one is breached, the other is still safe. Also, I would recommend different passwords for your financial accounts and your email accounts. So, cracking your email doesn't give them access to your bank account.

The longer the password is, the more secure it is. According to the website HowSecureIsMyPassword.net, the time it would take for a hacker to brute force your password (only using numbers and letters) is:

6 characters = 1 second | **8 characters = 1 hour** | **10 characters = 7 months**

16 characters = 37 billion years

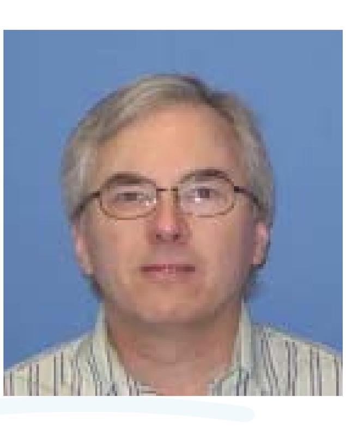
Adding symbols to your password greatly extends the time horizon – at least ten-fold!

Finally, if you find yourself using Post-It notes to "remember" your passwords, I strongly recommend using a commercial password manager or password vault.

Enjoy a safe and digitally-secure holiday season.

Milestones

35 YEARS OF SERVICE MILESTONE



Verne Britton, Lead Systems Programmer, joined WVNET in September 1985 and has reached **35 years of service!** Verne is currently responsible for Linux system management, creating virtual machines in a VMware environment, maintaining our public DNS servers, and provides webhosting consulting services to all WVNET clients.

Verne has worked with operating systems starting with the WVNET OpenVMS Cluster where he helped keep the cluster running continuously from 1996–2014, and later moved into the Linux and Windows environments. Verne graduated from Purdue University in 1980 with a Bachelor of Science degree in Computer Science.

Additionally, Verne has served as the WVNET representative to the Advisory Council of Classified Staff (ACCE) since 2002. ACCE is a state-wide committee comprised of 23 public colleges and universities in West Virginia promoting the interests and addressing the concerns of higher education employees in matters of institutional policies, legislative and executive branches of state government.

PROMOTIONS

Anita Davis – HR Manager. Anita has worked at WVNET since July 2019 as a HR Generalist. Previously, she worked in a variety of higher education roles managing and developing workforce & continuing education programs (Pierpont CTC), creating custom training for employees (WVU), and career services (MSU). She graduated with a Master's of Science in Industrial Relations from WVU (2005) and Bachelor of Arts degree in Psychology from WV State College (2003). She is certified as a Senior Professional in Human Resources (SPHR) and SHRM Senior Certified Professional (SHRM-SCP), is a member of the North Central Chapter of WV SHRM and volunteers for the Employer Support for the Guard and Reserve (ESGR). Anita is a U.S. Navy veteran and was stationed overseas in Japan and Guam as a Radioman (RM) telecommunications operator.

EMPLOYEE TRAINING & PROFESSIONAL DEVELOPMENT

WVNET employees have recently completed the below-listed sessions and courses:

- FIRE SAFETY AND FIRE EXTINGUISHER TRAINING WITH ANDY DOTSON, FIRE MARSHAL AND PUBLIC EDUCATION COORDINATOR, FROM THE MORGANTOWN FIRE DEPARTMENT
- SOCIAL ENGINEERING RED FLAGS, INTERNET & MOBILE DEVICE SECURITY
- SEXUAL HARASSMENT AND DISCRIMINATION PREVENTION
- DRUG-AND ALCOHOL FREE WORKPLACE
- FIRST AID/CPR/AED CERTIFICATION COURSE FROM WV PUBLIC SERVICE TRAINING

JOB OPENINGS

Thank you for your interest in joining the WVNET team! Below is a list of current positions available. Visit wvnet.edu/about/careers/

MANAGER OF TELECOMMUNICATIONS

TELECOMMUNICATION NETWORK SPECIALIST II

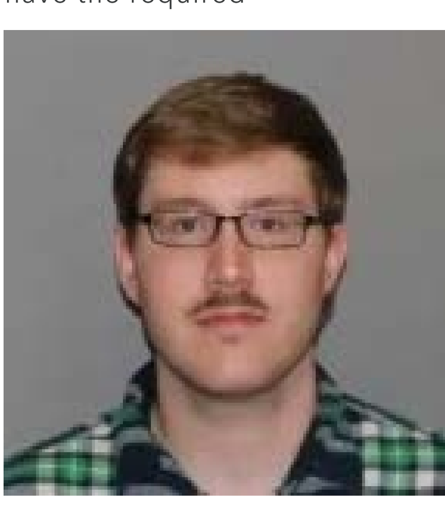
NETWORK OPERATOR (FULL-TIME)

DEPARTMENT UPDATES

Systems Update

Advancing from Within: WVNET Systems Group Welcomes Blaine Murphy

From finding those individuals who want to stay in the area, to dealing with hiring issues related to COVID, finding knowledgeable staff has always been a challenge. At WVNET, we have been fortunate enough to be able to hire those individuals that have the required skillsets to be able to perform the duties necessary for their position. However, this is not always the case. It is at times like these we often look internally at current staff and their aptitude for improvement.



WVNET maintains a 24x7x365 Network Operations Center (NOC) to ensure that our customers can receive support no matter when an issue occurs. This Network Operations Center is operated by a group of staff that work long hours to ensure that there is always someone there to talk to for providing basic support, or escalation if the issue is on a larger scale. The NOC staff members have a technical background and always perform their duties well, but some view their time in the NOC as an opportunity to start with WVNET and move up into more technical roles.

This transition to new advanced roles is something that has occurred many times in the past at WVNET. Not only have these staff members changed roles, but they have also shown a great aptitude for their new positions.

Blaine Murphy is one example of the successful transition from Network Operations to the Systems group. An opportunity arose with a recent position opening for an Information Systems Specialist and after working and gaining invaluable experience for 3 years in the Network Operations Center, Blaine seized the opportunity and applied for the position. Blaine has been a computer and electronics hobbyist for many years. He spends much of his free time working on projects involving amateur radio, embedded software, web development, and audio processing. While working in the NOC, Blaine built a small software application to help the NOC with notifications and information at a glance. His desire to learn more along with his knowledge of Linux, made him a great candidate with a vast amount of future potential and WVNET is happy to have him join our Systems team. Blaine is learning a lot in the early days in his new role and is already working to assist with management of the Linux servers hosted at WVNET, learning from the beginning about our cloud migration, as well as working on software interfaces and integrations of multiple services.

Welcome Blaine!

Finance and Business

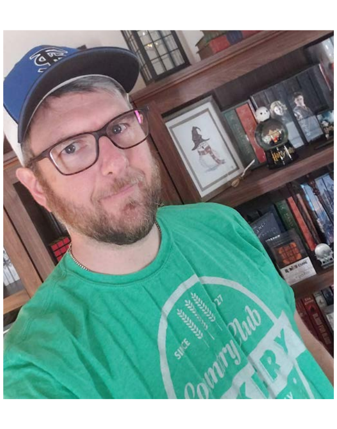
June through mid-October was a very busy time for the WVNET Finance-Business Office, as it required wrapping up the previous year's financial processes while performing the day-to-day operations of the current fiscal year, as well as submitting the budget for the next fiscal year.

Throughout the year, day-to-day operations include, among other responsibilities: negotiating and renewing contracts, paying vendors, closing out each end-of-month, and managing payroll. During these especially hectic months, the Finance-Business staff responds to requests from the financial auditors for the prior year financial statements, updates a full-year expense projection into the current fiscal year, and submits the following fiscal year's budget to the State.

The hard work and dedication provided by the Finance-Business staff is what keeps WVNET moving forward.

Updates from the Development Team

Over the last few months, the WVNET Development Team has been keeping busy with various projects and working on implementing standard project management processes. For the first time, WVNET has a project manager on staff to help us plan and keep projects on track.



Chevee Dodd, assumed the role of Project Manager of IT & Application Development in July and is already assisting in formalizing our project onboarding and proposal process. We are currently working on projects for a variety of customers as well as maintaining operational support for existing websites and applications.

Once of the areas we are focused on improving right now is the initial scope and planning process. We have started creating project charters for each project to make sure everyone involved understands and is in agreement about the scope of the project and what will indicate it is completed.

Additionally, our proposal process will use those requirements to prepare estimates for the general task areas for the project and provide the customer the opportunity to understand the time and costs involved. Once the customer accepts both the project charter and the proposal, we begin work.

We are taking an agile approach to our development process and still learning what works and doesn't work for us as a team, but adding formal planning is keeping us on track and helping us stay focused.

To discuss web or application development projects with the Development Team, send an email to wvnet-support@staff.wvnet.edu to schedule a meeting and review your project requirements.

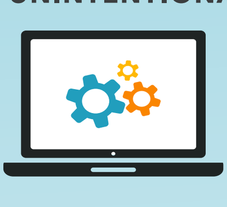
HACK THE HUMAN: END-USER TRAINING AND TIPS TO COMBAT SOCIAL ENGINEERING

From the desk of **Carlos Kizzee** MS-ISAC Chair

We like to think we can trust our co-workers to do the right thing. Unfortunately, this is not always the case. Some people become insider threats; that is, they use their authorized access to systems to harm their organization. For example, someone may sell information from a database to a third party.

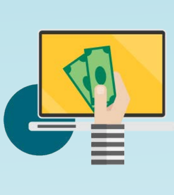
THERE ARE THREE TYPES OF INSIDER THREATS:

UNINTENTIONAL



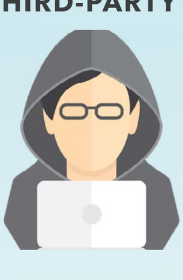
This person does not intend to cause a threat, but they do so through carelessness. They may misplace their laptop or flash drive, fail to update software, or ignore instructions when setting up software or cloud storage. Their attention to detail may be poor and they can make mistakes that damage the organization, such as causing a breach by emailing data to the wrong person.

INTENTIONAL



This person intends to harm their organization and is often called a "malicious insider". They may be in it for financial gain, to get revenge for some perceived slight, or for some other motivation. They may leak information to third parties for money or political beliefs, steal information to advance a side business, or destroy data to sabotage the organization.

COLLUSIVE OR THIRD-PARTY

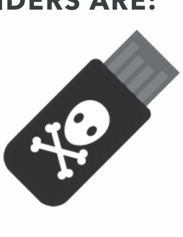


Collusive threats occur when an insider collaborates with an outsider to compromise an organization. The outsider may recruit an insider to obtain information to commit fraud, intellectual property theft, espionage, or some other crime. Some insiders may be manipulated into becoming a threat and may not recognize that what they are doing is harmful. Third-party threats occur when the insider works for a contractor or vendor who has access to the organization's network or facilities.

SOME OF THE INDICATORS OF AN INTENTIONAL INSIDER THREAT INCLUDE:

- Life changes, such as financial, relationship, family, or work problems.
- Behavioral changes, such as signs of depression, anger, or possible drug or alcohol addiction. However, a colleague who seeks help is showing good judgment.
- Changes in work habits such as working through lunch, accessing or asking questions about information or systems not part of the scope of the colleague's employment, or a disregard for security policies and practices.

MANY UNINTENTIONAL INSIDERS ARE:



- Poorly trained in cyber hygiene, either because the organization does not train staff or because they do not pay attention.
- Disorganized; loses laptops or flash drives.
- Unfamiliar with technology or thinks they know more than they do and do not follow instructions when installing new software or setting up cloud storage.

We all make mistakes, but many unintentional insiders simply do not pay attention to what they are doing. The lack of attention to detail puts their organization at risk for breaches and malware.

To reduce the likelihood of an insider threat, organizations should develop a comprehensive program that includes knowing the people within the organization, identifying the assets and prioritizing the risks, and establishing the proven operational approach of detect and identify – assess – manage. Organizations should take extra steps to vet third party service providers to ensure they can access only necessary systems and areas of the building.

The Cybersecurity and Infrastructure Security Agency (CISA) has more information about insider threat mitigation at cisa.gov/insider-threat-mitigation.