Our Fall 2023 Newsletter

November 7, 2023

In This Issue

WVNet Offices will be closed:

Thanksgiving, November 23-24, 2023
Christmas, December 25, 2023
New Years, January 1, 2024

WVSTC – TAKING A BREATHER IN 2024

In 2024, we're hitting the pause button on the West Virginia Statewide Technology Conference. But hold on, it's not a farewell; it's more like a "see you later." We're taking time to recharge, regroup, and we hope to come back in the future with a conference that's even better suited for our customers.

Your input and ideas are valuable, so don't hesitate to share them with us.

Keep in Touch

We may be on hiatus, but we’re not disappearing. Stay connected with us through our email list and social media for updates and developments. We’ll keep you in the loop as we prepare for the future.

UPDATE FROM THE EXECUTIVE DIRECTOR!

As we bid farewell to Cybersecurity Awareness Month, it is imperative to recognize that our commitment to cybersecurity should not conclude with the passing of October. Cyber threats are persistent and ever-evolving, and now, as the holiday season approaches, our digital defenses must remain as vigilant as ever.

The holiday season is traditionally a time of joy and celebration, a time when we gather with family and friends to create lasting memories. However, it's also a time when cybercriminals become more active, preying on the increased online activity and distracted individuals.

Here are some key points to consider as we navigate the holiday cybersecurity landscape:
1. Be Cautious of Phishing Scams: During the holiday season, phishing scams tend to surge. Cybercriminals often disguise their malicious emails as enticing holiday offers, e-cards, or fake shipping notifications. It's vital to stay vigilant and double-check the legitimacy of every email you receive.

2. Secure Your Online Shopping: Online shopping becomes the norm during the holidays. Ensure you shop on reputable websites with secure payment methods. Look for the padlock icon in your browser's address bar and use strong, unique passwords for each site.

3. Safeguard Your Personal Information: Be mindful of the personal information you share online. With increased online interactions during the holidays, ensure that you are not oversharing sensitive data on social media or other platforms.

4. Update and Secure Your Devices: Cybersecurity is only as strong as its weakest link. Make sure all your devices, including computers, smartphones, and IoT devices, have the latest security updates and patches installed.

5. Use Strong, Unique Passwords: Passwords are your first line of defense. Utilize strong, unique passwords for every online account, and consider using a password manager to keep track of them securely.

6. Educate Your Family and Friends: Share your knowledge about cybersecurity with your loved ones. Ensure they are aware of the risks and practice safe online habits.

7. Monitor Your Financial Transactions: Regularly review your financial statements and report any suspicious activity immediately to your bank or credit card company.

As the Executive Director of WVNET, I am proud of the work we do to enhance the cybersecurity posture of educational institutions and organizations throughout West Virginia. Our commitment to cybersecurity doesn't wane with the end of Cybersecurity Awareness Month; rather, it grows stronger, more vigilant, and more proactive.

In this digital age, maintaining our cybersecurity is not a choice; it is a responsibility. We must remain vigilant year-round, not just for the security of our institutions but for the protection of our individual privacy and safety. Cybersecurity is not a destination; it’s a journey, one that requires continuous learning and adaptation.

By staying alert, informed, and cautious, we can celebrate the holidays with peace of mind, knowing that we are safeguarding our digital frontier.

WELCOME NEW EMPLOYEES!

Welcome Andrew Davis!

Andrew Davis is a recent graduate of West Virginia Junior College, with an Associate’s degree in Information Technology. He joined WVNET in September as a Network Operator at WVNET and has demonstrated a sincere dedication in learning his new role. His passion for technology serves as both a career drive and a personal interest, with a mission to forge a successful IT career while providing for his family. Outside of work, Andrew finds joy in gaming, avidly following TV and movies, immersing himself in music, and passionately following ‘One Piece.’

Your satisfaction is very important to us. WVNET has implemented a customer satisfaction survey link in our OZ ticketing system. When a help ticket is closed, the reporter will receive an email update with a link to allow customers to fill out the survey, and, if desired, request a call from a manager. To access the form in the OZ email, click on the link.

If you're not using OZ and you wish to take the survey, please feel free to complete the survey at **https://wvnet.edu/satisfaction-survey/**. We look forward to hearing from you. Have questions? Contact Harmony Garletts at **hgarletts@staff.wvnet.edu**.

Customer Satisfaction Survey

NEW SCHEDULE OF RATES

Effective July 2023, WVNET has a new schedule of rates.
Visit **https://wvnet.edu/resources/schedule-of-rates/** to find out more.

DEPARTMENT UPDATES

CLIENT SERVICES

What is AI?

Artificial intelligence (AI) refers to computer systems that can perform tasks that typically require human intelligence, such as visual perception, speech recognition, and decision-making. AI systems are powered by algorithms that learn from data to improve at specific tasks over time without explicit programming.

AI is transforming industries from healthcare to transportation. However, the term is sometimes misused or exaggerated in popular culture, leading to misunderstandings about what today's AI can and cannot do. So what are some key things to keep in mind when thinking about AI?

What AI is:

- Algorithms that learn. AI systems use statistical techniques to "learn" from large amounts of data, allowing them to improve at tasks without traditional programming.
- Pattern recognition. AI can perceive and understand inputs like images, audio, and text to complete tasks like image classification, speech-to-text, and language translation.
- Predictive capabilities. AI can analyze current data to make predictions about potential future outcomes. This is used for things like predicting equipment failures or forecasting disease spread.

What AI is not:

- Sentient or conscious. Despite depictions in science fiction, real-world AI systems do not currently have human-like consciousness, emotions, or intent.
- Infallible. AI systems can and do make mistakes if their training data or algorithms have biases or gaps. AI consistently requires monitoring and auditing for errors.
- Magic. While impressive, AI capabilities have limitations and do not manifest intelligences from nowhere. AI is the product of human ingenuity, labor, and oversight.

Understanding what AI truly is – and is not – will be important as these technologies continue advancing and impacting our lives. By dispelling the myths around AI, we can have productive discussions about developing and regulating AI thoughtfully.

Welcome to the Future: There's an AI for That!

In this age of rapid technological advancement, Artificial Intelligence (AI) has permeated every aspect of our lives, transforming the way we work, learn, and interact. We would like to introduce you to an innovative platform that stands at the forefront of this revolution: "There's an AI for That"!

"There's an AI for That" is a one-stop solution, bringing together a diverse range of AI applications designed to cater to various needs and interests. No matter what you are looking for, this platform has something for everyone. This tool has some intriguing opportunities for use in the education field, including resources for both students and faculty to enhance their learning journeys. Some examples of interesting resources found here are Excel formulas, explanations, and macro builders.

Ready to embark on your AI journey? Visit "There's an AI for That" today to explore the limitless possibilities of AI and discover how it can transform your world.

CLIENT SERVICES-BANNER

FAFSA Simplification

The FAFSA Simplification Act of 2020 made many changes to the way students apply, how the data is processed, and how schools handle the data received, beginning with the 2024-2025 FAFSA. The FUTURE Act (Fostering Undergraduate Talent by Unlocking Resources for Education) also enhanced the exchange of data between the IRS and the FAFSA Processing System (FPS) in order to streamline the application process for students. The following is a basic summary of information found in the *2024-25 Draft Student Aid Index (SAI) and Pell Grant Eligibility Guide* available at fsapartners.ed.gov.

The application has changed in that students, spouses, and both parents (all now known as "contributors") will have separate FSA ID's with which to log in and complete their portion of the FAFSA – necessary due to FUTURE Act requirements to authorize use of IRS data. The FUTURE Act also takes away the ability of a school to initiate the application FAFSA Partner Portal (was FAAAccess) due to needing authorization to match IRS data. Some questions have been removed, such as those pertaining to selective service and drug conviction. Demographic questions have been added and algorithms have been altered to better guide the family through the application.

The FAFSA collects data from the applicant and uses it to calculate their eligibility for federal

financial aid programs. The FAFSA eligibility determination that was called an Expected Family Contribution (EFC) will be the Student Aid Index (SAI) beginning in 2024-2025. The Student Aid Report (SAR) the student receives is now the FAFSA Submission Summary. So far, the ISIR (Institutional Student Information Record) that the school receives from the processor is still an ISIR.

Determination of Pell Grant eligibility no longer directly applies the FAFSA result (EFC/SAI) to a Pell Grant Award and Disbursement Schedule. The new formula uses family size and income, which is compared to percent of poverty level income in the dependent student's parent's state of legal residence or the independent student's state of legal residence. If the student is not eligible for Pell using this test, but they have an SAI that is between the minimum and maximum Pell amounts, they may still be eligible for an amount of Pell based on the difference between their SAI amount and the maximum Pell award amount. For example, let's assume the maximum Pell award for the aid year is $7000 and the student's family income is greater than the maximum allowed for a Pell Grant based on a comparison to poverty level in their state. The student's SAI of $500 would be subtracted from the maximum Pell award of $7000 and a Pell Grant would be awarded for $6500. A student attending less than full time will get a reduced amount based on enrollment as a percent of full time (92% of the full time award would be awarded for a student carrying 11 credit hours, for example).

All of these changes have delayed the availability of the 2024-2025 FAFSA to December 1, 2023 from the usual October 1. Another complication for schools is that Ellucian will not be able to provide the 2024-2025 ISIR dataload software until mid-December. Testing will need to wait until the software is available. In the meantime, schools will be required to submit Federal Work Study (FWS) earnings data via Common Origination and Disbursement (COD) system so that it's available when the student completes the FAFSA – students no longer need to enter the FWS amount onto the FAFSA. Ellucian delivered a process that will populate a new table with FWS earnings data and two new processes to extract the data for submission to COD and to import the acknowledgement back into Banner.

This isn't the first major overhaul of the financial aid delivery process and it will probably not be the last. Some years require extra training and others leave scars. Let's hope this one just involves some tweaks, a little extra training, and a few procedural changes.

SYSTEMS UPDATE

Introduction:

Nearly all essential business operations in the modern age hinges on the dependability and security of systems that operate behind the scenes, often imperceptible to the daily users. These systems are akin to a "blackbox" for most individuals. At WVNET, we boast a team of proficient system administrators, adept at leveraging modern techniques to bolster security, automate processes, implement updates, and meticulously monitor a multitude of critical systems that are crucial for the seamless functioning of organizations in West Virginia.

Automation:

WVNET's system administrators employ a suite of automation tools that are widely recognized as industry benchmarks for proficient administrative teams. Manual execution of tasks such as server deployment and configuration not only introduce the possibility of minor discrepancies resulting from human error but is also more time-consuming and lacks a comprehensive overview of the system configurations from an abstract standpoint. The adoption of Infrastructure as Code tools enables our team to effect swift changes across all automated systems and serves as a documented record of these configurations. Terraform is the preferred tool for automating the deployment of virtual machines on our cloud-based hosting service, which plays host to web servers and other critical mediators for processing and transmitting data across the state. Puppet, on the other hand, is our favored choice for configuring and managing systems. The combined use of these tools centralizes deployment and configuration management in key locations, facilitating effortless system updates and security patching.

Monitoring System Health / Recovery Methods:

At WVNET, we deploy an array of tools to fortify data security and maintain a vigilant watch over the health and status of our systems. Central to our toolkit is Nagios, a versatile and widely adopted monitoring system that shoulders the responsibility of overseeing the majority of our servers. Nagios not only provides invaluable insights when errors occur but also promptly alerts us to instances of dwindling system resources, generates comprehensive uptime reports, and issues a diverse spectrum of alerts. Its real-time capabilities grant us immediate visibility into the status of servers, applications, and network devices, empowering our team to proactively address issues by delivering timely alerts and notifications. Nagios is our steadfast solution, whether we're detecting server outages or closely monitoring resource utilization. Together with our Network Operations Center (NOC) staff, it serves as the cornerstone in upholding the dependability and stability of our server infrastructure at WVNET.

In conjunction with our robust monitoring efforts, we prioritize data security through the implementation of multiple backup techniques. These encompass file-level backups, which safeguard individual files, and daily disk snapshots with replication off-site. This multi-tiered approach ensures that critical data is protected, and system recovery remains reliable, fortifying our commitment to data integrity and system stability.

Internal Security and Threat Detection:

In addition to managing and automating our systems, WVNET places a strong emphasis on internal security to safeguard against potential threats. We employ a multi-faceted approach that includes the utilization of security assessment tools such as Nessus and OpenVAS. These tools are instrumental in scanning our network and systems for vulnerabilities, ensuring that we identify and address potential weaknesses before they can be exploited by malicious actors.

Nessus is renowned for its comprehensive vulnerability assessment capabilities. It scans our network infrastructure, servers, and applications to pinpoint potential security issues, assess their severity, and provide actionable recommendations for remediation. By regularly conducting Nessus scans, we bolster our proactive stance against vulnerabilities and ensure that our systems remain

resilient against emerging threats.

OpenVAS, an open-source vulnerability assessment tool, complements our security strategy. It conducts in-depth scans to identify weaknesses in our systems and applications, providing us with detailed reports and risk scores. These insights allow us to prioritize remediation efforts and continually enhance our security posture.

To further strengthen our security and effectively manage the vast amount of security data generated by our systems, we've implemented the Wazuh Security Information and Event Management (SIEM) system. Wazuh is instrumental in real-time threat detection, incident response, and security monitoring. It aggregates and analyzes security events, identifies potential threats, and notifies our team of any suspicious activity. By centralizing and automating the analysis of security data, Wazuh helps us respond promptly to security incidents, minimizing potential damage and ensuring the integrity of our systems and data.

Incorporating Nessus, OpenVAS, and Wazuh SIEM into our security framework underscores our commitment to maintaining a robust and proactive internal security infrastructure. By continuously assessing and monitoring our systems for vulnerabilities and threats, we strive to provide our clients with the highest level of protection for their critical data and business operations.

Conclusion:

Preserving the security and accessibility of information with a high level of confidence is paramount to the operational success of our clients' businesses. Deprived of reliable access to our systems for their data, the cost could extend beyond mere financial implications, impacting their public image as well. Moreover, the assurance of data recovery through our backup systems in times of catastrophe instills confidence that not all is lost during dire situations.

TELECOM UPDATE

Welcome to the WVNET Telecom team Kyle Atkins!

Kyle joined the team after previously working in WVNET'S Network Operations Center (NOC). Kyle is originally from Madison, WV and now lives in Arthurdale, WV. He graduated from West Virginia Junior College with an Associate Degree in Network Administration and Security. Before West Virginia Network, Kyle worked for AT&T. He is married to Samantha, and they have three adopted daughters – Rhi, Nevaeh, and Alexis, one son – Buster, and seven pets – three dogs (Jade, Dexter, and Kane), two cats (Jackson and Oscar), and two pot belly pigs (Dale and Julia).

Useful Cybersecurity Resources

Cybersecurity & Infrastructure Security Agency (CISA) works with partners to defend against today's threats and collaborate to build a more secure and resilient infrastructure for the future. CISA offers cybersecurity essentials for small and local government agencies.

Cyber Essentials:
https://www.cisa.gov/resources-tools/resources/cyber-essentials

Launched in 1989 as a cooperative for information security thought leadership, and now the world's largest cybersecurity research and training organization, SANS (SysAdmin, Audit, Network, Security) specializes in helping reduce organizational risk. Check out these helpful resources from SANS on password managers and online security for kids:

The power of Password Managers (everyone should use one)
https://www.sans.org/newsletters/ouch/power-password-managers/

Online security for kids
https://www.sans.org/newsletters/ouch/online-security-kids-23/

This summer hackers are believed to have targeted a wide range of organizations, including federal and state agencies as well as corporate entities by using flaws in popular file-transfer tool MOVEit. **These helpful links provide ways organizations can work to protect their identities after the breaches:**

How to protect your identity after MOVEit breaches:
https://www.axios.com/2023/06/23/moveit-breaches-identity-theft-protection

The Biggest Hack of 2023 Keeps Getting Bigger
https://www.wired.com/story/moveit-breach-victims/
