NOVEMBER
Issue 11

UNION BANK

Middlebourne Office
103 Dodd Street
Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street
Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street
St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy,
Hundred WV 26575
304-775-2265

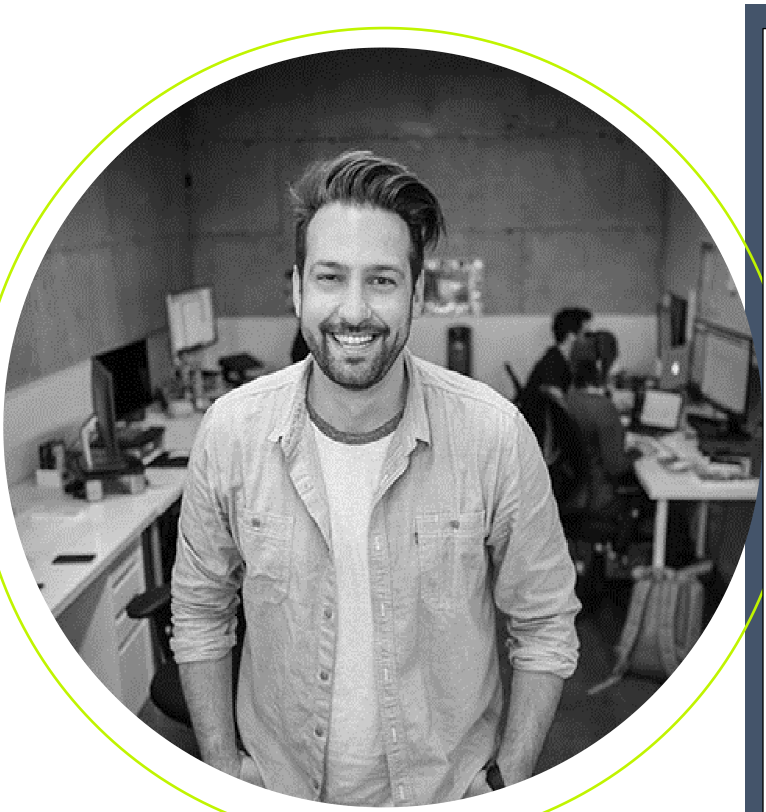
Ellenboro Office
90 Main Street
Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street
Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave.
Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
Kroger Plaza 19 Acme Street
Marietta, OH 45750
740-374-0010
This is not a full service location. Deposits/withdrawals cannot be processed at this location.

New Martinsville Office
638 N SR 2
New Martinsville, WV 26155
304-455-2967



CYBERSECURITY AWARENESS

October was National Cybersecurity Awareness Month. But cyber security is not something we should only think about once a month but instead every day. Now in its 18th year, National Cybersecurity Awareness Month (NCSAM) continues to raise awareness about the importance of cybersecurity across our nation, ensuring that we all have the resources to be safer and more secure online.

Each year, the campaign tries to raise awareness and educate the public and businesses on the dangers that lurk on the Internet while also addressing certain themes. The 2021 theme was “Do Your Part. #BeCyberSmart.” This theme encourages individuals and organizations to own their role in protecting their part of cyberspace, stressing personal accountability and the importance of taking proactive steps to enhance cybersecurity. Each day we depend on technology to complete our daily activities as well as perform some of our most important civic duties.

The Cybersecurity and Infrastructure Security Agency (CISA) has provided great tools and resources on their website to help educate online users and encourage everyone to spread the word through social media hashtags or just through simple conversations with friends and loved ones. In the age of misinformation and disinformation it is important to use reliable sources for cybersecurity information and to ensure you have the most up to date information.

The STOP. THINK. CONNECT. campaign is a great tool used to reach a global audience to promote a more secure online environment. This campaign not only educates, but it also provides great tools as well. STOP. THINK. CONNECT. is part of an unprecedented effort among federal and state governments, industry, and non-profit organizations to promote safe online behavior and practices. It is a unique public private partnership, implemented in coordination with the National Cyber Security Alliance and it encourages Americans to view Internet safety as a shared responsibility–at home, in the workplace, and in our communities.

One of the great things about the STOP. THINK. CONNECT. campaign is that it does not just deal with the threats that can possibly affect companies and organizations, but also deals with everyday situations that children and parents deal with such has tax cyber scams, online shopping and cyber safety rules for kids. The website provides informative articles written by industry leaders; tips on how to educate employees on cyber threats and how to prevent breaches, the latest cyber regulatory and policy information, how to talk to your teens about conducting themselves online and much more.

Our world is becoming more digitalized. While that brings more efficiency and cost savings, it also brings the possibility of cyber threats and attacks. These are best combated by sharing vital information and making sure each one of us is educated on the potential risk. It is not only important for businesses and families, but it also protects our nation’s economic future and supports our national interest. So, take some time to visit some of the below websites. Learn how you can get involved and be empowered to protect not only yourself while you are at work but, your friends, family and your community.

CISA Cybersecurity Resources | CISA-
https://www.cisa.gov/cisa-cybersecurity-resources

STOP. THINK. CONNECT. ™ | CISA -
https://www.cisa.gov/stopthinkconnect

Sources:
https://www.cisa.gov/stopthinkconnect
https://www.cisa.gov/cybersecurity

PRIORITIZING CYBERSECURITY IN A HYBRID WORKPLACE

In this day and age, employees are more connected than ever. The hybrid workplace is here to stay, and for employees, this means relying on connected devices from their home office setups. According to recent data, smart home systems are set to rise to a market value of $157 billion by 2023, and the number of installed connected devices in the home is expected to rise by a staggering 70% by 2025. In this new normal where smart devices and consequently online safety are a must, here are some tips for securing those devices.

Remember smart devices need smart security
Make cybersecurity a priority when purchasing a connected device. When setting up a new device, be sure to set up the privacy and security settings on web services and devices bearing in mind that you can limit who you are sharing information with. Once your device is set up, remember to keep tabs on how secure the information is that you store on it, and to actively manage location services so as not to unwittingly expose your location.

Put cybersecurity first in your job
Make cybersecurity a priority when you are brought into a new role. Good online hygiene should be part of any organization's onboarding process, but if it is not, then take it upon yourself to exercise best practices to keep your company safe. Some precautions include performing regular software updates and enabling MFAs.

Make passwords and passphrases long and strong
Whether or not the website you are on requires it, be sure to combine capital and lowercase letters with numbers and symbols to create the most secure password. Generic passwords are easy to hack. If you need help remembering and storing your passwords, don't hesitate to turn to a password manager for assistance.

Never use public computers to log in to any accounts
While working from home, you may be tempted to change scenery and work from a coffee shop or another type of public space. While this is a great way to keep the day from becoming monotonous, caution must be exercised to protect yourself and your company from harm's way. Make sure that security is top of mind always, and especially while working in a public setting, by keeping activities as generic and anonymous as possible.

Turn off WiFi and Bluetooth when idle
The uncomfortable truth is, when WiFi and Bluetooth are on, they can connect and track your whereabouts. To stay as safe as possible, if you do not need them, switch them off. It's a simple step that can help alleviate tracking concerns and incidents.

These are just a few simple steps towards achieving the best online safety possible. Staying safe online is an active process that requires constant overseeing at every stage - from purchasing and setting up a device, to making sure that your day-to-day activities are not putting anyone at risk. By following these steps, you are doing your part to keep yourself and your company safe from malicious online activity.

Sources:
https://staysafeonline.org/resource/cybersecurity-awareness-month-articles/