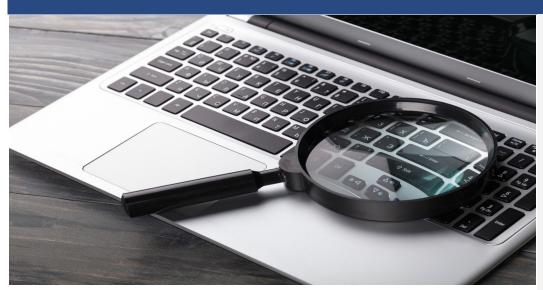
#### Mobile Banking App is HERE!



#### JULY 2019 Issue 7



## IS YOUR HOME NETWORK SECURE?

There is lots of talk about corporations and businesses keeping their networks secure, that sometimes it's easy to forget about your home network. Several years ago, home networks were relatively simple. They were usually nothing more than a wireless access point and a computer or two used for surfing the Internet, online shopping, or gaming. However, home networks have become increasingly complex. We now connect far more devices to these networks and use them for more than just web browsing or consuming media. This month, we cover how you can create a secure network at home for you and your family.

Almost every home network starts with a wireless network (sometimes called a Wi-Fi network). This is what enables you to wirelessly connect any of your devices to the Internet, from laptops and tablets to gaming consoles and televisions. Most home wireless networks are controlled by your Internet router, which is the device your Internet service provider installed in your house to connect you to the Internet.





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

However, in some cases, your wireless network may be controlled by a separate system called a wireless access point, which connects to your Internet router. Regardless which one your wireless network uses, they both work the same way: by broadcasting wireless signals. The different devices in your house connect to your wireless network via these signals. From there, these devices can then connect to the Internet, as well as any other devices on your home network. This means securing your wireless network is a key part of protecting your home. Here are some steps to secure it:

Change the default administrator password for your Internet router or wireless access point, whichever is controlling your wireless network. The admin account is what allows you to configure the settings for your wireless network. The problem is many Internet routers or wireless access points are shipped with a default admin login and password that are well known and often posted on the Internet. As such, be sure to change the admin password to a strong, unique password that only you know.

Change the default name of your wireless network (sometimes called SSID). This is the name your devices will see when they search for a local wireless network. Give your network a name, something unique so you can easily identify it, but make sure it does not contain any personal information. There is little value in configuring your network as hidden (or non-broadcast) as most wireless scanning tools or any skilled attacker can easily discover hidden networks.



Ensure that only people you trust can connect to and use your wireless network, and that those connections are encrypted. Do this by enabling strong security. Currently, the best option is to use the security mechanism called WPA2. By enabling this, a password is required for people to connect to your home network. Once connected, their online activities are encrypted. Be sure you do not use older, outdated security methods, such as WEP, or no security at all, which is an open network. Open networks allow anyone to connect to your wireless network without any authentication.

Ensure the password people use to connect to your wireless network is a strong one and that it is different from the admin password. Remember that you most likely only need to enter the password once for each of your devices, as they can store and remember the password. Many wireless networks support what is called a guest network. This allows visitors to connect to the Internet, but protects your home network, as they cannot connect to any of the other devices on your home network. If you add a guest network, be sure to enable WPA2 and a unique password for this network.

Disable Wi-Fi Protected Setup or other mechanisms that allow a new device to connect to the network without knowing the password and con-figuration options. If you have difficulty remembering all these different passwords, possibly look into using a password manager tool to securely store them for you.

**Consider setting up a VPN (Virtual Private Network).** A VPN adds two layers of security to your online connection. It does this by adding another layer of encryption (on top of the AES encryption provided by your router's WPA2 AES) as well as replacing or hiding your true IP address.

Also make sure your devices are always running the latest version of their operating system. Whenever possible, enable automatic updating on them. If any of your devices require a password, always use a unique, strong password. Finally, when in doubt reaching out to your Internet service provider is always a good idea. They can walk you through all the steps to ensure your set up is accurate and safe. Be sure to visit their website, as they may provide free tools to help you secure your home network.

# WHAT

### IS 5G?

There will be lots of technology coming in the next couple of years and one in particular that has received a lot of buzz is 5G. Many people don't know what 3G, 4G, or even 5G means other than it's the symbol normally located on the top of your smart phone's home screen!



Below is a brief explanation of 5G and why many are looking forward to the new 5G capability.

The "G" means generation. Like previous generations before, they are defined by their speed and other components. 1G was analog cellular; 2G were the first generation of digital cellular technologies; 3G technology has speeds from 200kbps to a few megabits per second; 4G is up to hundreds of megabits and even gigabit-level speeds. 5G, the fifth generation of cellular network technology, will be virtualized and software-driven.

Like other cellular networks, 5G networks use a system of cell sites that are small, divided geographical areas and send encoded data through radio waves and is designed to operate on much larger channels than 4G and can carry higher speeds.

The 5G network will not only produce more speed, but it will simplify mobility, with seamless open roaming capabilities between cellular and Wi-Fi access. Mobile users can stay connected as they move between outdoor wireless connections and wireless networks inside buildings without user intervention or the need for users to reauthenticate. It also should improve connectivity in underserved rural areas and in cities where demand can outstrip today's capacity with 4G technology.

5G is already available in some areas in various countries but has not been introduced world wide yet. Experts expect to see a full fledge roll out of the new technology in 2021 or 2022. But many are anticipating great benefits. One being the ability for the health industry to monitor at-risk patients from afar. Patients connected to devices will allow health professionals to see data of key health indicators, such as heart rate and blood pressure, which will allow them to intervene sooner and administer help faster. Another benefit will be to the car industry. 5G combined with ML-driven algorithms will provide information on traffic, accidents, and other road way disturbances and allow motorists to share information with other vehicles and entities on roadways which, in turn, can provide more safety.

The message is very clear from internet companies and cell phone makers: 5G is on its way! Several cities in the United States already have access. Soon it will be in yours!