Bank of Botetourt

August 2021 Issue 8

Member FDIC

EQUAL HOUSING LENDER

# Securing Your Home Network

The ongoing pandemic remains to be a major factor in the increased numbers of employees working from home. This continues to be lucrative for hackers, who know home Wi-Fi's can be a bridge to corporate networks. Because of this, it is important that your home Wi-Fi is just as secure as your network in the office. As we begin a new year it is important to take care of a few house keeping security items. Below are a few tips to help.

## Keep Router Firmware Up to Date

A router runs low-level software called firmware. The firmware sets the security standards for your network and defines the rules about which devices can connect. The firmware should be updated to protect the network security of your home. The router's firmware like any other type of software can contain vulnerabilities that hackers can exploit. Most routers won't have the option of an auto-update so a manual update to the software will be required to ensure your home network is protected.

## Passwords

Password safety is another relatively easy way to protect your home Wi-Fi connection, but picking the right password is important. Using the same password across multiple accounts is not good practice. Each account should have its own unique password and that includes your Wi-Fi. Having a strong Wi-Fi password will stop any unwanted devices from connecting to your network.

## Know Who is on Your Network

It's important to know who and what devices have access to your home network. Many routers have an option in their management pages that show which devices have connected recently. It should be checked often to see if there are devices accessing your home network that shouldn't be. If there are, disconnect them immediately.

*Continue on Page 2*

**Bonsack**

**Buchanan**

**Care Center**

**Cave Spring**

**Daleville**

**Eagle Rock**

**Fairfield**

**LakeWatch**

**Lexington**

**Natural Bridge**

**Peters Creek**

**Salem**

**Troutville**

**www.bankofbotetourt.com**
**www.facebook.com/botetourt**
**(540) 591-5000**

## Encryption

Encryption is extremely important. Almost all wireless routers come with an encryption feature. By default, it is turned off. Turning on your wireless router's encryption setting will scramble the information you send over the internet into a code so it's not accessible to others.

## Use a VPN When Necessary

A virtual private network is an essential privacy tool. When using your home Wi-Fi network to access your office network it is very important to keep outsiders from seeing your internet activity. This protection can help take some of the danger out of connecting to the internet.

## Consider using a Firewall

Firewalls are designed to protect computers from harmful intrusions. Wireless routers generally contain built-in firewalls but are sometimes turned off as a default. Be sure to check that the wireless router's firewall is turned on. In case your router doesn't have such a firewall, consider installing a good firewall solution on your system to watch for malicious access attempts to your wireless network.

## Scan

USBs and other external devices can be infected by viruses and malware. Use your security software to scan them.

## Back up Your Data

Protect your valuable information such as your work, music, photos and other digital information by making electronic copies of your important files and storing them safely.

*Sources:*
*Keep Your Home Wi-Fi Safe in 7 Simple Steps | Norton*
*https://www.computerworld.com/article/3532352/12-security-tips-for-the-work-from-home-enterprise.html*
*https://www.comparitech.com/blog/information-security/security-remote-working/*
*Securing Your Home Network - Stay Safe Online*

# Oversharing Can Be Risky

It has been over a year since the pandemic started and many of us have settled into this new digital way of life. From ordering groceries online to Zoom calls with family and Microsoft Team meetings with colleagues, we have all tried to adjust to the new normal. Remote working will likely continue and get easier and more efficient as time goes by. But at the center of all this new digital freedom has always been the worrying factor of security. It was inevitable that cyber criminals would take advantage of the opportunity to exploit workers while they work remotely, but the truth is, sometimes we unwittingly aid these criminals in their quest by oversharing information.

Truth be told, Zoom calls and Microsoft Team meetings are one the best technology advancements of this new normal. We can meet with colleagues, customers and business partners online and conduct business as usual just as if we were in a conference room all together. Even on Facebook, we are able to conduct meetings and live video chat with friends and family. But do we ever stop to think about what we are really sharing while using these platforms? There have been numerous memes and gifs circulating on the internet about Zoom calls gone wrong with images such as cats replacing the moderator and toddlers unexpectedly entering the camera frame. Their has also been the great filters that allow you to change your visual background but many just opt for their home office, their kitchen and yes, sometimes their bedrooms as their background! But images of your new home office set up can be compromising and can share a lot of information that can be extremely helpful to a cybercriminal.

Email security firm Tessian conducted a study that found 84% of people post on social media every week and 42% post every day. Such posts consist of photos that share lots of data such as locations, family members and work environments. Sharing these types of photos seem innocent, however those photos can be just what a criminal needs to commit a crime, especially if the photos are of your workspace. That same study also showed 93% of workers in the U.S. update their job status on social media, while 36% share information about their job and 26% post about their co-workers or clients. These types of photos expose employees as well as their companies' networks especially if they use hashtags. For example, if an image of an employee's laptop or paperwork on their desk is captured, a skilled hacker can extract pertinent information from those pictures, such as email addresses, confidential company information and vendor information. Those same pictures can also reveal the types of software and devices are being used. name which makes it feel more personalized therefore disarming your natural instincts to be suspicious.

The attacker can use the details found in the pictures to craft phishing attacks, Business Email Compromise (BEC) attacks and ransomware attacks. They also will have the ability to personalize their scams using your name, or someone from your organizations name which makes it feel more personalized therefore disarming your natural instincts to be suspicious.

We have to remember cybercriminals have nothing but time on their hands. The can be extremely patient and just wait for their victims to make unfortunate mistakes. But there are some things that can be done to protect yourself and your organization when engaging in video calls:

⇒ ***Be mindful of your background when you are on video calls or when you post a picture. Limit visibility of your laptops, mobile devices, personal photos or any work-related content.***

⇒ ***Use a virtual background. Technology has allowed users to make video calls not only productive but also fun! There are all sorts of visual backgrounds to choose from, just make sure they are appropriate for the work environment. Also consider blurring your background, to prevent a hacker from seeing it clearly.***

⇒ ***Think before you post that next work from home photo with hashtags #workfromhome, #remotework, or #homeoffice. Hashtags are used to help others who are interested in a certain topic quickly find content on that same topic but they can also be an easy road map for a cybercriminal looking for their next victim.***

Oversharing has always been an issue in this digital era but even more so now since the pandemic. Because of this, cybersecurity crimes have been on the rise, but taking necessary precautions to protect yourself as well as your organization will help mitigate some of the risk associated with embracing this new way of life.

Sources:
Home-Office Photos: A Ripe Cyberattack Vector | Threatpost https://threatpost.com/home-office-photos-cyberattack-vector/164460/
93% of workers overshare online, causing security risks - Help Net Security https://www.helpnetsecurity.com/2021/02/03/workers-overshare-online/