Bank of Botetourt

May 2020 Issue 5

8 Video Conference Security Tips

The Coronavirus (COVID-19) outbreak has forced many companies to adopt a work from home policy that keeps at-risk staff away from the office to help flatten the curve, while still trying to maintain some type of normalcy within their daily work activities. There are great tools that can make the transition to a remote environment seamless, allowing an employee to continue to be productive and still servicing customers, all while being away from the office. Video conferencing is one of the tools many see as beneficial. Organizations have embraced video chats and conferencing because it allows organizations to keep their fingers on the pulse and have a visual connection with their employees and customers, all while still adhering to the social distancing requirements that are crucial at this time. However, security on these platforms have been a hot topic.

Alarmingly, some of the platforms do not have end to end encryption, a security feature that secures communication so that it can only be read by the users involved in the video conference. There is also a shocking permission gap which allows unauthorized users to gain permission to join in on a video conference call. In addition, privacy issues are raising concern.

Continued 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

Whatever service you decide to use for your video conferencing needs, there are security measures that should be put in place.

1. Have a Video Conferencing Policy in place. Set clear boundaries and expectations for users. The policy should include rules that take into account those who will be connecting remotely.

2.Always use the latest version of the software. Security vulnerabilities are likely to be exploited more often on older software versions.

3. Secure networks or devices. Transmitting sensitive information and data across the internet is always risky. Encryption and network security are a must to protect crucial data. Encryption is one of the ways to ensure a video conferencing solution is safe and not susceptible to security breaches.

4. Use Meeting Lock for enhanced privacy. The meeting lock feature allows any new participants trying to enter a meeting to be held at a waiting screen and can only be allowed in by the host.

5. Make sure password protection is enabled. Make sure that your service uses both a meeting ID number and a separate password or PIN.

6. Don't allow participants to screen share by default. Once a meeting has begun, the host can allow specific participants to share when appropriate.

7. Keep tabs on attendees and remove unknown participants. If you see the name of someone you do not recognize, you have the ability to remove them from a session by dismissing them.

8. Consider using a virtual background. Virtual background features prevent any accidental mishaps and enable team members to stay focused even in the presence of distracting background activities.

These are just a few of the best practices that will make this critical communication tool safer and more private for employees and their employers. Organizations will need to do extensive research on these platforms and decide what works best for their work environment.

Sources:
https://www.computerworld.com/article/3535924/do-s-and-don-ts-of-videoconferencing-security.html
https://highfive.com/blog/5-steps-for-secure-video-conferencing
https://searchsecurity.techtarget.com/tip/8-tips-to-ensure-enterprise-video-conferencing-security-and-privacy

COVID-19 Phishing Scams

Phishing has widely proclaimed to be one of the greatest dangers and most consequential cyber security threats of our time. It has proven to be extremely successful and profitable for cybercriminals. At a time where much is unknown, cybercriminals are taking advantage of the COVID-19 pandemic and are sparing no one. They have launched new phishing campaigns and are relentless in their attempts. By using emails, phone calls, text messages, fake websites and even written correspondence that appear to be legitimate about COVID-19, they trick you into divulging information such as bank accounts numbers, credit card account information, social security numbers, logins and passwords. Clicking links that come from unreliable sources could unknowingly download malware that infects your computer.

Now, more than ever, everyone must remain digitally vigilant and scrutinize every email, phone call or text message that is received from an unknown source or even a known source. It is not beyond hackers to use the name of legitimate well-known organizations in their schemes. There have been reports of cybercriminals sending out correspondence using official government department names and the World Health Organization on official looking letterhead in hopes they can trick someone into calling a fake number or emailing them with the information they seek. The Centers for Disease Control and Prevention (CDC) is sounding the alarm on these "government impersonation fraud" tactics and are urging everyone to not fall prey to these nefarious acts.

As of the end of March, COVID-19 scams have cost Americans 13.4 million dollars in losses according to the Federal Trade Commission. Many expect that number to grow until the crisis is over.

It is extremely important to practice good security measures for your own protection and to help reduce the chances of you becoming a victim of these scams. Here are a few things you need to keep in mind:

- The government will never call to ask for money or your personal information like Social Security number, bank account or credit card numbers.
- Don't open unsolicited email from people you don't know.
- Be wary of third-party sources spreading information about COVID-19. Refer to the official CDC.gov website for updates on COVID-19.
- Hover your mouse over links to see where they lead. But be sure to not click on the link!
- Do not click links in emails. If you think the address is correct, retype it in a browser window.
- Be wary of attachments in any email.
- Do not supply any personal information, especially passwords, to anyone via email.
- Don't respond to texts, emails or calls about checks from the government.
- Hang up on robocalls. Scammers are using illegal robocalls to claim they are representatives of the government with important information.
- Watch for emails claiming to be from the Centers for Disease Control and Prevention (CDC) or The World Health Organization (WHO).

The reality is we will see more of these types of scams. Taking advantage of people when they are at their most vulnerable state is a goldmine for hackers. Although the pandemic has brought out the best of us, unfortunately it has also opened the doors to some of the worst online criminals. Users need to be extra cautious and pay close attention to every email, text and phone call received.

Sources:
https://www.forbes.com/sites/thomasbrewster/2020/03/12/coronavirus-scam-alert-watch-out-for-these-risky-covid-19-websites-and-emails/#73d7385c1099
https://www.pcmag.com/news/phishing-attacks-increase-350-percent-amid-covid-19-quarantine
https://www.cdc.gov/
https://www.consumer.ftc.gov/blog/2020/04/scammers-are-using-covid-19-messages-scam-people