BIZ NET
BUSINESS - NETWORKS

THE Tech chronicle

September 2020

Virtual Conferencing Safely and Securely

With so many of us now working from home, you are most likely finding yourself remotely connecting with your co-workers using virtual conferencing solutions like Zoom, Slack, or Microsoft Teams. Your family members - perhaps even your children – may also be using these same technologies to connect with friends or for remote learning.

Regardless of why you are connecting, here are key steps you can take to make the most of these technologies safely and securely.

Attending a Virtual Conference

If you will be attending a virtual conference, here are five key steps.

Update the Software: Make sure you are always using the latest version of the conferencing software. The more recent and updated your software, the more secure you will be. Enable automatic updating and quit your program when done, so it can check for the latest updates the next time you restart.

Configure Audio / Video Settings:
Set your preferences to mute your microphone and turn off your video when joining a meeting and enable them only when you want. Consider placing a webcam cover or tape over your computer's camera to ensure privacy when you're not actively broadcasting. Remember: if your camera is on, everyone can see what you are doing even when you are not talking.

Double-Check What's Behind You: If you want to enable your webcam, be aware of what's behind you. Ensure you do not have any personal or sensitive information visible behind

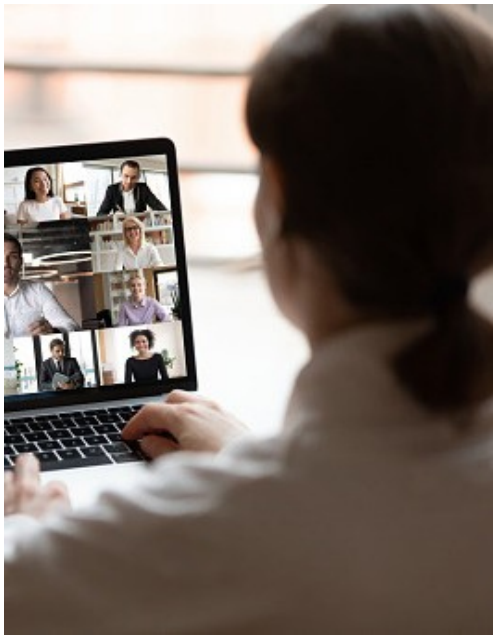
Marco's Corner

Are you working from home? Is your business data safe? With people now working at home more than ever, having a reliable home computer network is paramount. What you relied on previously to browse the web, play computer games, or read your email, probably is not sufficient to protect your critical business files. The Internet is a dangerous place and you need to take special steps so you are secure and be productive at the same time. Your son or daughter that is playing a computer game in the next room should not prevent you from having a ZOOM meeting with your boss. That same gaming computer also should not be able to infect your business computer to the point where you lose all of your important business files. The router you bought at your local computer store 5 years ago may not be sufficient to protect you from malware attacks or hackers in your new working environment. Have you changed the default password and is your router updated with the latest firmware? Concerns such as network performance, security, and privacy now become much more important than it was before. If you are using a wireless router, have you configured two separate SSID's (Service Set Identifier), one for business and one for personal use? Are you backing up your business data regularly both onsite and in the cloud? All these are considerations that you need to keep in mind when you work at home. Want more information on how to setup your home office properly and be productive secure at same time? Please call us 775-850-7700.

Biz-Net
1325 Airmotive Way Suite 208
Reno, NV 89502

This monthly publication provided courtesy of Marco Romero, President of Biz-Net, Reno NV

Our Mission: To provide the best possible service for our clients using the best tools available today. *As a business owner, I know you do not have time to waste on technical and operational issues. That's where we shine!*



you during a call. Some video conferencing software lets you blur or use a virtual background, so people cannot see what is behind you.

Don't Share Your Invite: The invite link is your personal ticket to enter the meeting. Even if a trusted co-worker needs the link, it's much better they ask the conference organizer for their own invite.

Do Not Record: Do not take screenshots of or record the conference call without permission. You could accidentally share very sensitive information if those screenshots or recordings become public.

Hosting a Virtual Conference

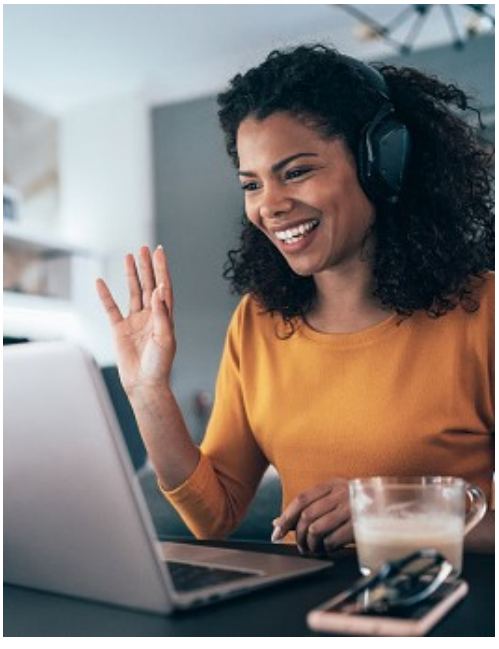
If you will be hosting a virtual conference, here are some additional steps you should take.

Require a Password: To protect the privacy and security of your conference and control who can join, protect your meeting with a password. This way only people who have the conference password can join the event.

Review Attendees: Review the people attending your event. If there is someone you do not know or cannot identify, have that person confirm their identity. If you have any concerns, or if someone is being rude or disruptive, remove them from the conference. Many solutions offer the option to lock the conference once it has begun, so no one else can join unless you let them in. Another option may be to initially place people in a virtual waiting room, so you can approve who joins the call.

Inform if Recording: If you intend to record the event (and have permission to record), be sure to inform everyone on the conference ahead of time.

Sharing Your Screen: If you will be sharing your computer screen at any point, be sure to first close all other applications and remove any sensitive files from your computer's desktop. Also disable any pop-up notifications. This helps ensure you don't accidentally share sensitive or embarrassing information while sharing your computer screen. Another option is to consider sharing just the program you want to show instead of sharing your entire computer screen.

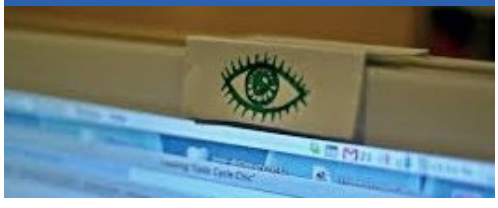


These technologies are a fantastic tool and, in many ways, represent the future of how we will work, collaborate, and communicate with others. These simple steps will go a long way to ensure you safely and securely make the most of them.

Cover or Unplug Your Webcam When You're Not Using It

If you're using an external webcam – that is, one that plugs into your computer's USB port – only connect it when you need it. Yes, it can be a pain to remember to plug it in whenever you want to video chat with someone, but at least you'll know 100% you aren't been spied on if there's no camera connected.

If you're using a device with a built in camera, consider covering it (don't put something with sticky residue on the camera lens or it can ruin it).



Remote Workers Are Getting Hit By Ransomware

According to the 2020 Vulnerability and Treat Trends Report, the number of new samples of ransomware increased by a staggering 72 percent during the first half of this year.

Hackers around the world have come to increasingly view it as their go-to attack option.

As with a great many things in recent months, this trend can be traced back to the COVID-19 pandemic. In response to the virus, untold millions of employees began working from home, which allowed them to stay productive, but at a terrible cost to network security. Few companies can afford to provide the same level of security and protection to their remote employees as they can when everyone is in the office.

Unfortunately, the moment a remote employee is infected and connects to the corporate network, the malware in question spreads like wildfire. Worse, since IT staffs are running thin these days and many security professionals themselves working from home, they're relatively less able to deal with the rising threat.

The biggest and best way to protect against a ransomware attack now and at some point in the future, when the pandemic has finally run its course, comes down to visibility. Specially, the IT security people who have watching your network need full visibility and the means of analyzing how critical network assets could potentially be accessed by an agent moving laterally within the network, with or without proper credentials.

Additionally, this full and transparent view of things gives your security professionals the means of telling, at a glance if VPN's, firewalls and related systems are properly configured and have all the latest security patches installed.

While that certainly doesn't provide bullet-proof protection, that kind of visibility goes a long way toward minimizing your risk. If you don't have something very like that in place right now, you need it as soon as possibly.

Keep Your Personal Life Off Your Work Machine

While you're working from home, you may be tempted to work on your personal computer or to use your work equipment for personal activities, like checking your social media accounts and streaming TV. However, as much as you can, you should avoid mixing your personal life with business applications on any of your devices.

Cyber Security Tips for Avoiding Malware While Working From Home

Hackers are interested in exploiting new vulnerabilities as employees disperse. A March 2020 survey of the CNBC Technology Council found that 36% of respondents at that time already saw an increase in cyber threats as employees transitioned to remote work.

Since cyber security issues change daily, it's important to always stay on your guard against potential security issues, including malware. This is the best way to keep yourself safe.

Look out for COVID-19 scams
Phishing attacks and phony apps may exploit current crises as part of their social engineering techniques. In order to influence you to download malware from an attachment or click through to a website where you could be subjected to a drive-by attack, hackers may try to trick you into thinking you've received a critical communication about public health.

Look out for suspicious links in emails, especially if they're sent from an unknown address or if it seems out of character for the sender. If you're uncertain, don't click the link. Flag it with your security team for review or simply delete it.

Adhere to company security policies
Your employer likely has a very specific set of regulations governing work-from-home policies, including cyber security measures. If you're unclear about any of the guidelines, ask for help. It's better to resolve the issue now than leave your system vulnerable to infiltration.

Your company may have a mandated antivirus application. Make sure that it's installed correctly on your machine. It should be set up to scan your system frequently and update automatically or according to your employer's desired schedule. Keep tabs on whether it noticeably slows down your device's performance, though.

Keep your home wireless network secure
Once you're out of the office, you lose access to the company's secure on-site network. There are several steps you can take to make sure your home Wi-Fi network is more secure.

First of all, make sure your network uses the Wi-Fi Protected Access 2 (WPA2) or WPA3 protocol, not the outdated Wired Equivalent Privacy (WEP) standard.

Secondly, you should verify that your home network is set up using a secure password. If you haven't already done so, update it from the default password, and make sure to use something that is hard to crack. It should have a mixture of capital and lowercase letters, as well as numerals and special characters. The password should not include complete words or something that's easy to guess based on your personal information, like your date of birth or wedding anniversary.

Use a virtual private network
If possible, you should consider setting up separate wireless networks through your home router. You can reduce risk to your work devices by keeping them logged onto a separate network from the one used for personal devices in your household.

As with antivirus software, your employer may mandate the use of a virtual private network (VPN) for work-related activity. If so, use their preferred VPN, and make sure it's enabled while you're working. A VPN can also provide added security if you do have to use public Wi-Fi temporarily for any reason.