MPA has collected tips and actual client experiences & lessons about how to stay productive, cyber-safe, and get the fastest service from us right now.

What's Happening Right Now

- The support load continues to be heavy. Some clients did not shelter until this week and are just now requesting help. While all clients have a remote access system, some employees have never used it or have not in some time. They need extra help. We will get back to everybody.
- Video conferencing is experiencing hiccups and delaying the start of meetings, wasting precious time. (tips below).
- Slow remote access performance is being caused by improper usage (learn how not to mess up your system performance AND that of your co-worker's at the same time – tips below).
- Discoveries are being made about what tools are not available at home. (e.g. "How do I scan?" - tips below).
- LinkedIn has made available, at no cost, a library of excellent videos on productivity tips when working from home.
- Cyber/phishing/scams have spiked to take advantage of this situation. **Watch out.** Homeland Security has confirmed. We must protect ourselves. YES – SCAMS CAN HAPPEN TO YOU. (Be aware of clever new scams and read about an MPA client's CEO using his home computer who just lost $1,000 cash along with his credit card and online banking numbers. Read about a North Bay RIA firm, not an MPA client, that was compromised this morning – tips below)

Video Conferencing (Zoom, GoToMeeting, etc,)

- All the major services are experiencing full phone lines & circuits. This is compounded as cell phone services run out of circuits in your local community. This wastes the time of everyone on the call, a significant cost. We have experienced all the California Zoom conference call phone numbers to be busy at times and the only circuits available are if you use the numbers in other states. This will get worse as more workers and students around the US work from home.
- We don't know the fix for this. We have seen some success so far with a dedicated conference bridge phone number only used by your firm; though this means your firm can only have a single conference call going at any single time and anyone could call in, at the wrong time, and hear the meeting in progress. JoinMe offers this and I personally use it every day for conference calls. Other Video Conference services may offer flavors of this.
- POWER TIP: Phone and/or access your conference 5-15 minutes before the scheduled start time.
- The organizer of the call MUST set the conference to allow people to enter before the organizer does – or this TIP won't work.
- While you multi task and do something else before the appointed start time, DO NOT put your phone on hold if it has music on hold. You will drive the others nuts. Mute your phone instead or plop a pillow over it.

Keep your Remote Access As Fast as Possible for You + Your Coworkers

- **DO NOT** use the following with the web browser on the computer you are remotely controlling at the office or, for those of you who no longer use servers in your office and instead use a Private Data Center environment (PDC), the web browser in the PDC:
- Video conferencing software. Copy the URL of the conference, toggle/open up the web browser on the computer in front of you, paste the URL into the web browser, and use it from there.
- Anything that uses video: web sites with ads, "newspapers" like NYT/CNN/etc, YouTube, web sites that have embedded ads that move.
- Anything that uses sound: dictation software, streaming music, Spotify.
- Not following these basics means your experience won't be good AND you will be consuming significant bandwidth that will slow down the remote access experience of your coworkers.
- If you do not understand the difference between the two web browsers or how to toggle between them, contact a coworker or submit a service ticket and MPA's team will be happy to train you.

Are you missing important phone calls on your iPhone all of a sudden?

- It seems a recent Apple update may have changed a setting that forces calls to voicemail if the caller is not in your contacts list. This could include coworkers, prospects, the boss, your banker, or someone else whose call you don't want to miss. You may be confused as this is not the way your iPhone worked previously or the behavior of the office phone you are used to using.
- Either check your voicemail constantly or Google Search how to change the iPhone setting back so all calls ring your phone.

How Do I Scan at Home?

- For scans of a few pages like signature pages, consider the download and purchase of Adobe Scan from your cell phone App Store. You take a picture with your phone and it is converted into a PDF file you can Email to yourself. Scans of many pages are possible but cumbersome.
- We have been drop shipping scanners, while they last, to home offices. These tend to work better at scanning than printer/scanner combo systems.

LinkedIn Videos – Excellent and Free - on Home Office Working and Balance

- LinkedIn has made an excellent library of these available free (16 courses) on topics related to working remotely, managing change and staying productive.
- Cut/paste this phrase into your web browser: **LinkedIN Remote Working: Setting Yourself and Your Teams up for Success** (Notice how I included the name not the link to get you used to being cyber-safe)

Cyber Attacks - - WATCH OUT – especially now.

We're seeing three principal challenges.

- Cyber-attacks have spiked to take advantage of Coronavirus. Homeland Security has issued warnings. MPA peers in the Bay Area have report increased incidents in our community. Ransomware. Scams. Theft of data.
- Home networks and home computers are not as well protected as office networks and office computers.
- Face it, we are all a bit distracted right now, emotions may be high (do you have kids at home?), and our guard is down. Furthermore, we're reading stuff sent by family, friends, and "trusted authorities" via clicking on links or opening attachments with less caution than we normally would.

Cyber Safety Tips for Right Now

- Don't believe anyone asking for money. Watch out for Coronavirus charities, the "Red Cross," (how do you know for sure it's the Red Cross?), scammers pretending to be Microsoft or Apple, someone who "knows" a friend of yours who has the virus and urgently needs money for an ambulance. The Government does not ask for money via phone or email so don't fall for that one.
- **True Story:** Last week, the CEO of an MPA client received a call at home from "Apple." He was told his home Mac had a situation that urgently needed fixing. The CEO gave the "Apple" guy $1,000. Then he gave the guy remote access to his computer. The crook took over the computer, loaded who-knows-what malware software, and transferred data. Then the crook said everything was fixed now and to leave the computer turned off for a while, likely to buy time to use the stolen information. We're guessing the crook harvested the passwords/credentials stored in the client's web browser. The client subsequently had to cancel all his credit cards, home banking, and any systems that used the passwords. Who knows what the downstream results of this might be.
- TIP: THIS CAN HAPPEN TO ANYONE.
- TIP: DON'T STORE YOUR CREDENTIALS IN YOUR WEB BROWSER.
- TIP: It may be safer to use one web browser on your home computer for work and another one for personal use. It may be safer to use one computer at home for work and another for personal matters. It may be safer to not save work credentials on a personal device.
- **True Story:** Last week, multiple employees of a client received extremely clever phishing messages. Here is a description by MPA's William Gandolph and what you can do right now to protect yourself:
    - The client saw a wave of a phishing attacks affecting multiple employees. Emails appeared to be coming from "Office 365 Microsoft" and alerted each person about email prevented from delivery. The message directed the reader to click a link to login to O365, review the emails, and confirm if they were SPAM. Everything about this email looked legitimate. Even the web page it takes you to when you click the link looks like the Microsoft O365 sign-in page. Unfortunately, sometimes it may look so real it may fool the tech you reach for support.

- POWER TIP: For a good review of what phishing is and why it is not easy to spot, review this brief website: cut/paste this into Google and search: vadesecure.com/en/phishing-awareness-training-8-things-employees-understand/
- While most MPA clients have Mimecast to try and stop these emails, Mimecast is only as good as the last wave of attacks. Meaning, the bad guys know you're using a filter and they constantly try new tricks to get past the filter – and your suspicions.
- **This morning,** an RIA (Registered Investment Advisor) firm in Marin (not an MPA client), had their email system compromised. An email was sent out from the "Named Partner" to all clients & contacts he had ever sent email to with a request to click on a suspicious link regarding a proposal. A phishing attack like the one described above may have caused this to occur by inadvertently giving hackers his email credentials.
- It is important to not only recognize email that may be an attack but also to report it. In Outlook, select the suspected email. Click on Mimecast in the Toolbar. Select Report Spam and Select Report Spam or Report Phishing. Mimecast engineers review the reported emails to determine how to spot and filter new forms of attack. That is why it is important to report suspected spam / phishing because the prevention is better when they get feedback they from the users. **We're in this together.**

Best of regards to all of you,
Michael

Michael Price, Founder & CEO
MPA Networks, Inc.
Voice: (650) 566-8800 x106