How to work from home: 6 Teleworking Tips

1. Have a designated work station:

Most people don’t have a lot of unused rooms in their home, so don’t feel like you have to possess a “traditional” office. However, you do want to have a designated space where you can effectively complete your work tasks. You want to make sure it is comfortable, but also functional. We all love lounging on the couch, but it’s probably best to be somewhere where you can focus on the task at hand.
2. Prioritize:

All of us working unexpectedly at home may have a number of priorities...(children). We understand this and working remotely doesn’t mean you have to ignore your kids. It does mean that you may need to set some boundaries. For instance, maybe every couple of hours of work results in a quick 5-10-minute activity with the kids. It’s important that everyone around you understands that you are “working”, but that doesn’t mean you have to completely ignore other potential responsibilities.

3. Establish a work routine with your environment in mind:

One of the most challenging aspects of working remotely is establishing a routine. We are creatures of habit as we usually get our coffee at the same time, say hi to our co-workers at the same time, take our break(s) at the same time. Try to replicate this at home as it helps you remember that you are still working. The idea is not for you to be chained to your desk, but rather to replicate the production that takes place within the workplace.

4. Make a list:

Most people don’t go shopping without a list and the same can be said for employees and their work. When you are in the office it is easy to complete a task and pick up work elsewhere. However, when you are at home that becomes more challenging. Therefore, it is helpful to map out your day and/or week. Have a list of things you want to accomplish in any given period.

5. Rest your eyes:

When you are in the office rarely are you staring at the computer screen for hours upon hours. Now you may be working on the computer, but you aren’t focusing your eyes in one place for an extended period of time. Remember the “20-20-20 Rule”, which says that for every 20 minutes spent staring at a screen you should look at something 20 feet away for 20 seconds. Following this is a great reminder to help reduce strain on your eyes.
6. Take Breaks:

Very rarely do we work throughout the day without taking a break. It is important to remember this when working at home. This might mean a walk to the mailbox or taking the dog outside. Get up and stretch your legs just as you would in a traditional office setting. Sometimes at home we tend to keep working, but your body will thank you for getting up and moving.

---

**Be more like Susan — make telework a way of life**

April 3, 2020

For Susan, not much changed on March 15 when the federal Office of Management and Budget gave the order for federal employees to maximize telework.

Susan, who asked that her last name and agency be withheld, has been a full-time teleworker for almost two decades.

On March 16 as most employees headed into work one more time to collect paperwork or laptops or whatever they needed to telework, Susan fired up her computer in her Virginia home office, walked downstairs to make coffee and let the dogs out. It was just a regular day.

“I have my own office and whole set up that makes it much easier to be successful,” Susan said in an interview. “I can close my door so the kids or the cats and dogs don’t interrupt calls. They know if the door is closed, do not to come in.”

Susan rarely goes in to the office. She only “talks” to her boss, who teleworks himself from the West Coast, and her co-workers mostly by teleconferencing, email or instant messaging applications. But now the coronavirus has turned tens of thousands of federal workers into Susans. And many are not happy to be working remotely full-time.
A Federal News Network online survey of 1,047 federal employees found 77% of all respondents say they are teleworking today because of the coronavirus pandemic.

Of those, 47% of the respondents say they did not telework regularly before the emergency, meaning there are a lot of people who aren’t used to teleworking and may not be happy about it in the least.

Alex Alonso, the chief knowledge officer at the Society for Human Resource Management (SHRM) and an industrial organization psychologist who studies telework, said roughly 40% of all workers—public and private sector — have teleworked at some point over the last 50 years.

But the coronavirus has become a forced telework situation and that is something employees need to wrap their heads around in a different way.

Full-time teleworkers will say there are some basic dos and don’ts that everyone should follow.

Susan follows a routine. She starts by logging on and getting a solid two hours of work in before taking her first short break.

“It really helps me keep my focus to take regular breaks,” she said. “When you work in a regular office there are tons of distractions that let you take a mental break. But when you are in home office, you can get siloed so it’s important to take breaks.”

Alonso agreed. Having a routine is important, especially one that allows you to stay mentally healthy and refreshed.

Susan said a recent change for her is to create a group of three or four colleagues that she keeps in touch with at least daily, if not several times a day.

“Working from home can be solitary,” she said. “Many of us have work groups in an email loop where we can fire questions back and forth to bounce ideas. It really helps to have a small group you can collaborate with and share and ask questions with because it keeps you connected and tethers you to the office. I didn’t have that at first and I would go into the office and not know anyone.”

Alonso said the need to create social interactions that are more than just an email falls more on supervisor or manager’s shoulders than anyone else.
“There needs to be a replacement for the in-person social interaction we are all used to, and not just work based interaction,” he said.

He said SHRM takes the first 15 minutes of every meeting to provide general check-in to see how everyone is doing, and then they do a specific check-in at the end of the week about how everyone is feeling.

One of the biggest problems teleworkers face is the inability to turn off work: Checking email one more time, or going back to a report at 11 p.m. once everyone else is in bed.

Susan said she makes sure her day ends, even it means flexing her time to work four hours in the morning and then four hours in the evening if she had to deal with kids when they were little or other appointments.

“It’s just too tempting to check on one more thing, which means your day never ends,” she said. “If you leave [your] computer and system up and running, it’s too tempting to check on one more email or check on one more thing. That’s not good for your family life or mental health. You have to turn everything off.”

The one silver lining Susan, Alonso and many others in the survey hoped to come from this coronavirus pandemic is a realization that telework is more than just a nice to have during snow storms. It’s also a way of working that benefits agencies and employees alike.

“This may be a good litmus test showing managers that employees can telework,” wrote one survey respondent.

Stay Healthy, Stay Protected

By Rodney Blunt
Chief Information Security Officer | State of Kansas

The Kansas Information Security Office (KISO) is advising a more heightened sense of caution when viewing and responding to emails and when visiting websites. The KISO reports a significant increase in sophisticated phishing emails from 24,000 to 33,000 per week. Like all other national emergencies, cyber criminals are leveraging the pandemic in extremely sophisticated ways. Please stay safe, stay healthy and exercise more scrutiny in your cyber activities.
Zoom and WebEx Teleconferencing Security Tips

With the transition to work from home there is an increase of cyber-attacks against the technologies we use to communicate. One recent example of this is “ZOOM BOMBING” where malicious individuals join teleconferences uninvited and post explicit video and audio.

The State’s standard for teleconferencing is Microsoft Teams and this bulletin is not promoting Zoom or WebEx. We are aware that some vendors that you interact with leverage this technology. Also, for parents your children’s school may be using these technologies as well.

Please exercise due diligence and caution in your cybersecurity efforts. The following steps can be taken to mitigate teleconference hijacking threats if you host meetings:

**WebEx Best Practices**

1. Auto Lock Personal Room for secure meetings. This prevents all attendees in your lobby from automatically joining in the meeting. The host will see a notification when attendees are waiting in the lobby and as the host, you will authorize the attendees to join. This can be done from My WebEx > Preferences > My Personal Room on your WebEx site.

2. Set Personal Room Notifications before a Meeting to receive an email notification when attendees are waiting for a meeting to begin. You will then be able to expel any unauthorized attendees.

3. Schedule a Meeting instead of using your Personal Room. Personal Rooms web links do not change. Improve security by scheduling a meeting which includes a one-time web link.

4. Scheduled Meetings are unlisted by default by the Site Administrator for all WebEx sites. Unlisting Meetings enhances security by requiring the host to inform the meeting attendees, either by sending a link in an email invitation, or hosts can enter the meeting number using the Join Meetings page.
5. Set a password for every Meeting by creating a high-complexity, non-trivial password (strong password). A strong password should include a mix of uppercase and lowercase letters, numbers and special characters (for example, $Ta0qedOx!).

6. Do not reuse passwords for meetings. Scheduling meetings with the same passwords weakens meeting protection considerably.

7. Use Entry or Exit Tone or Announce Name Feature to prevent someone from joining the audio portion of your meeting without your knowledge. This feature is enabled by default for WebEx Meetings. For notifications, select Audio Conference Settings > Entry and exit tone > Beep or Announce Name. Otherwise, select No Tone.

8. Do not allow attendees or panelists to join before host. This setting is set by default by the Site Administrator for Meetings.

9. Assign an alternate host to start and control the meeting. This keeps meeting more secure by eliminating the possibility that the host role will be assigned to an unauthorized attendee in case you inadvertently lose your connection to the meeting. The alternate host must have a user account on your WebEx Meetings website.

10. Lock the meeting once all attendees have joined the meeting.

11. Expel Attendees at any time during a meeting. Select the name of the attendee whom you want to remove, then select Participant > Expel.

12. Share an Application instead of sharing your Screen to prevent accidental exposure of sensitive information on your screen.

13. Set password for your recordings before sharing them to keep the recording secure. Password-protected recordings require recipients to have the password in order to view them.

14. Delete recordings after they are no longer relevant.
15. Create a Host Audio PIN. Your PIN is the last level of protection for prevention of unauthorized access to your personal conferencing account. Should a person gain unauthorized access to the host access code for a Personal Conference Meeting (PCN Meeting), the conference cannot be started without the Audio PIN. Protect your Audio PIN and do not share it.

16. Do not click on emails where you don’t know the sender, email has inconsistencies with grammar and/or spelling, or contain a web link you're unfamiliar with.

**Zoom Best Practices**

1. Do not make meetings or classrooms public. In Zoom, there are two options to make a meeting private: require a meeting password or use the waiting room feature and control the admittance of guests.

2. Do not share a link to a teleconference or classroom on an unrestricted publicly available social media post. Provide the link directly to specific people.

3. Add a passcode to your meeting, then share that passcode with your guests.


5. Ensure users are using the updated version of remote access/meeting applications.

6. Do not use Facebook to sign in: It might save time, but it is a poor security practice and dramatically increases the amount of personal data Zoom has access to.

7. Use two devices during Zoom calls: If you are attending a Zoom call on your computer, use your phone to check your email or chat with other call attendees.

8. Don't use your personal meeting ID for meetings. A Zoom Personal meeting ID is the same as a Personal Room meeting in WebEx.
9. Consider turning on the “waiting room” for your meeting so that you can scan who wants to join before letting everyone in.

10. If you don't want participants to join/interact before the host enters, uncheck "Join Before Host". Set an alternate host if you need a backup host.

11. Disable "Allow Removed Participants to Rejoin".

12. Disable "File Transfer" unless you know this feature will be required.

13. Disable annotation if you don't need it.

14. Do not use recording features unless absolutely necessary.