Working from home because of coronavirus? Be careful what you download to keep cybersafe

March 17 2020, by Elizabeth Weise

Credit: CC0 Public Domain

So you've been told to work remotely because of the coronavirus. About the worst thing you could do right now is download a bunch of sketchy

programs for video conferencing, mobile working and the like that might carry computer viruses and make it so you can't do any work at all.

Here are some tips from cybersecurity experts to keep you safe and your computer (and boss) happy.

First, take a deep breath and re-read whatever work-from-home memo your company sent out. It should outline what programs you should be using for calls, video conferencing, file sharing and whether you need a virtual private network (VPN) to log in to your network.

If the memo doesn't outline these things, ask!

"It's OK to just wait a couple of minutes to check with someone rather than downloading something that could cause problems," said Ning Wang, CEO of Offensive Security, a cyber security company in New York.

FaceTime, Google, Slack or Teams

Chances are you've already got the programs you need on your computer and phone. You can do conference and video calls with FaceTime and Google and you might already use Zoom or Microsoft Teams or Slack for work.

If you don't, see what your work is recommending. It might take your IT department a day to figure things out, but better safe than sorry. It's amazing how much you can get done simply with emails and phone calls while they do.

If you do have to download new apps, make sure you're getting them from either the Apple App Store or Google Play. Both companies are being extra careful about apps at this point. Do not under any

circumstances use third party application sites—they're known for being malware havens.

If you do need to download a new tool or app, stick to well-known companies or ones that have been vetted and approved by your employer.

"If you see a tool you've never heard of, instead of going ahead and downloading it, ask someone at work," said Wang.

Virtual Private Networks are your friend

There are two main uses for VPNs. The first are personal consumer VPNs that create a security proxy to the internet so you can maintain your privacy on public WiFi networks.

There are also corporate VPNs, which are typically used for accessing office resources. They allow your computer to connect to your company network as if you were in the building.

Ask your IP department if you need a VPN and if so, which one they want you to use.

If you don't have an IP department, well-regarded PVN providers include Express VPN, NordVPN, CyberGhost and IPVanish, said Paul Bischoff, consumer privacy expert and editor of Comparitech.com, a security focused tech research and review site.

Note that these all cost money and that's a good thing.

"You know when it's free it also comes with a price. When it's a virus or a bot they installed so they can spy on you, it's not worth it," said Wang.

If you're working from a coffee shop with free WiFi, a VPN is a good idea because most coffee shops don't have IT departments to make sure their networks are secure. It's all too easy for a hacker to set up at the table in the corner and broadcast their own network mimicking the shop's, and harvesting everyone's information as it flies by.

Though Bischoff notes that the middle of a global pandemic is probably not the best time to be working from a cafe.

"If you're in a place where the coronavirus is bad enough that you're working from home, then maybe you should consider whether it's a good idea to work from a coffee shop in the first place," he said.

How to back up your data

Most companies do behind the scenes backups of their networks so workers never have to think about backing up. Check to see if that will still happen if you're working remotely. If it won't, ask what your company wants you to do.

For small amounts of data, you can store files on Google Drive and DropBox.

If you need something more all-encompassing and secure, popular sites include IDrive, IBackup and CrashPlan, said Bischoff.

These programs charge to securely store your data. Again, you get what you pay for, he said.

How to sign documents remotely

If you're not in the office to sign forms, DocuSign is a secure and

widespread program to get signatures on things that need signatures.

"I don't know of any other secure options that are as widespread as DocuSign, it's one I recommend," said Bischoff.

Scammers already using coronavirus

The coronavirus scams are already coming thick and fast, said Adam Meyers, vice president of intelligence at CrowdStrike, a cybersecurity firm based in Sunnyvale, California.

While it's hard to imagine, that call from someone claiming to be from your corporate IT department wanting to walk you through the work-from-home protocols could be a scam.

"It's pretty easy to get information about where somebody works. There's a lot of companies coming out and saying they're doing the right thing by having people work from home. Scammers are tracking that," said Meyers.

Scammers call claiming they're with the help desk and try to get you to download software or go to a certain webpage. They also are sending emails.

In this instance, rewrite the famous Russian proverb to, "Don't trust and verify."

If you get an email claiming to be from IT with links or documents, send a new email (so you're not using the address the possible scam came from) or even call your IT department to make sure it's legitimate.

If it's a call, tell them you need to call back to confirm before you do anything. Don't use any numbers they give you to call back on.

Scammers sometimes claim companies have set up special new call centers and the regular corporate IT phone numbers won't work. Don't buy it.

Remember that the people who do this kind of social engineering will lie or act mad to get you to do what they want. They might plead for your help, telling you they have to help a certain number of clients an hour, or act put out that you don't believe them.

Ignore them. No legitimate IT department would be anything but overjoyed that you are being cautious.

"Better off making somebody upset than being the reasons your company has been defrauded of millions of dollars or the source of a breach that caused the loss of sensitive information," Meyers said.