Q&A with Lorrie Cranor on how the pandemic is affecting individuals' privacy and security

April 9 2020, by Daniel Tkacik

CyLab director Lorrie Cranor says there are number issues related to privacy and cybersecurity that people need to be aware of. Credit: Carnegie Mellon University's College of Engineering

As epidemiologists continue to work to track the spread of the novel coronavirus, millions of Americans are several weeks into a routine of working from home. CyLab researchers believe we're settling into a new paradigm for privacy and cybersecurity.

CyLab director Lorrie Cranor, a professor in Carnegie Mellon's department of Engineering and Public Policy and the Institute for Software Research, says there are number issues related to privacy and cybersecurity that people need to be aware of.

In what ways is this pandemic affecting individuals' privacy?

A lot of the privacy issues have to do with the fact that people want to be able to track the virus, which means tracking people's whereabouts to figure out with whom they've been in contact. On the one hand, people typically don't like the idea of being tracked, but on the other hand, we're already being tracked anyway for marketing purposes. If you're browsing on your phone, you're probably also sharing your location with lots of companies you didn't realize you were sharing with, and they may be sharing it with advertisers.

There are a number of research initiatives–some of which Carnegie Mellon researchers are participating in–that are aimed at using phone data to track people's contact networks, but doing so in a way in which people's privacy is still protected.

There are also privacy issues of videoconferencing from home and people seeing what your house looks like or seeing or hearing other members of your household who may not know they're on camera. Norms as to when you turn on your camera and when you don't are quickly developing.

Speaking of that, what's your advice for people using

videoconferencing apps?

Most of these videoconferencing apps have various settings, and the default setting is usually pretty open and unprotected. Depending on how you're using the app, you should use settings that require passwords or don't allow people except the speaker to share their screen.

One interesting thing with Zoom is that you have a personal Zoom number which is basically a party line that anyone can call at any time. Before this pandemic, most of us usually used that number for everything because we weren't on it that much. But now that we're on it all the time, we're starting to see meetings collide–attendees of your next meeting showing up early and hearing what's being said in an earlier meeting. There are ways around it–you just have to generate unique links and numbers for individual meetings, but it's something we haven't really had to deal with before.

In terms of working from home, I've heard from lots of people saying that if you're still using default passwords on devices like your router, now is definitely the time to change that. Can you elaborate?

Yes, and it's not just about preventing strangers walking down the street from accessing your router. When devices have default passwords, it's very easy for malware to propagate and infect them. There have been a number of different malwares that basically know all of the default passwords for different devices. Once it finds a device, it tries to enter a default password, and if it hasn't been changed, it gets in and copies itself to the device. It's possible that random people could also do that, but it's not as common as malware doing it because it's completely automated.

If you have a device that's using a default password, change it. The

password doesn't even have to be hidden—you can tape the password to your router. It's usually fine if people inside your house know the password.

What else do people need to be cognizant of regarding working from home?

A lot of people are accessing confidential company information from their homes, so they should definitely be using Virtual Private Networks (VPNs). They may also be using home equipment that may not be set up properly with the best security standards. They may also be printing stuff out on their home printer and then throwing it away in their trash can instead of shredding it. It's these kinds of issues that people need to be aware of.

Provided by Carnegie Mellon University