

Q&A with Vyas Sekar on the COVID-19 pandemic's impact on cybersecurity

6 April 2020, by Daniel Tkacik



Credit: CC0 Public Domain

The COVID-19 pandemic has impacted countless aspects of everyday life, and our cybersecurity is no exception, according to [CyLab](#) researchers.

[Vyas Sekar](#), a professor in Carnegie Mellon's Electrical and Computer Engineering Department whose work focuses on [network security](#), thinks that enterprises need to be thinking very critically about the security of their networks—maybe more now than ever.

During this pandemic, millions of people have been told to work from home if they're able to. How might this new paradigm affect our own—and our employers'—cybersecurity?

The things that have typically been on-site and on the premises have gone remote and onto the public Internet. Security and privacy properties that you previously took for granted inside your [enterprise](#) or your closed [network](#) now are on the public Internet. We have to use the public network to get to our campus network, so there's a lot more reason to be careful about using things like Virtual Private Networks (VPNs) and encryption. That safety you had in the office is much different at

your home.

I think the second-biggest problem relates to this issue that people have dealt with for a long time: BYOD, or Bring-Your-Own-Device. Enterprises were always worried about people bringing their own devices—their own laptops or their phones that might be carrying malware and could infect the enterprise's network. It's the opposite problem now—you've brought your enterprise network into your home. People have already been talking about how the lines are blurring between what is home, what is [device](#), and what is enterprise. It's even more true now.

What's your advice for people working from home?

Using enterprise VPNs is even more critical right now, just to make sure work-related information cannot leak onto public networks. If people are able to do so, they should avoid using personal devices to conduct the work, just because company-issued devices are typically much more protected. If people must use their own devices for their remote work, they should run anti-malware software to ensure that their computers are clean. People should be doing that anyway, but with remote work, if they're using their own devices, they're passing that risk onto their employers.

Health and Human Services (HHS) got hit with a failed distributed denial-of-service (DDoS) attack a few weeks ago. What kinds of precautions do people and businesses need to take to protect themselves from this kind of attack?

It's tough, because some protections require going into the office and reworking some of the network's plumbing, and you can't do that if you're remote. You should be using some DDoS-protecting service, but going in and retro-fitting your network is probably not an option, and there's probably no on-

premise IT staff to do this. Also, if you're buying some new hardware online, it may be seen as "non-essential" and might take three weeks for it to be delivered to you. The whole supply chain has been diverted to other things.

I saw that a hospital in the Czech Republic was attacked with ransomware, and also that some ransomware groups have agreed to stop targeting hospitals during this pandemic. What's your take on all of that?

It's always a problem, but now it's much more of a problem because you are much more critically tied to your company equipment and so on. If you fall victim to a ransomware attack and your computer is locked up, it's great if people have a backup—not just of their computers but of their data—but that's not the case for everyone right now. And in regards to the ransomware groups saying they've agreed to stop attacking hospitals: they're probably worried that they may get sick. They're humans, too.

Companies should be training their employees on what's good cyber hygiene when working from [home](#). Some companies have already been doing this, but right now it's even more important to do so.

Provided by Carnegie Mellon University

APA citation: Q&A with Vyas Sekar on the COVID-19 pandemic's impact on cybersecurity (2020, April 6) retrieved 21 September 2020 from <https://techxplore.com/news/2020-04-qa-vyas-sekar-covid-pandemic.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.