Increased internet traffic requires more security awareness

April 8 2020, by Matt Kelly

Credit: Alexandra Angelich, University Communications

Unlike the suddenly quiet city streets, there is a lot more traffic on the information superhighway these days—and not all of it has your best interests at heart.

As schools have shifted to online learning and many employees are working remotely, there is more traffic on the internet—and that's on top of people who are quarantining at home and streaming entertainment and communications across cyberspace.

The internet can handle the traffic, said Jack Davidson, a professor of computer science in the University of Virginia's School of Engineering, but he warns that not all the traffic will be smooth.

"There are likely to be slowdowns due to bottlenecks at various points where the internet infrastructure is older and has not been upgraded," he said. "Typical bottlenecks might be the point of presence that serves a particular area.

"A point of presence (PoP) is a box that is the distribution point to, say, a neighborhood or particular geographic area. If a provider has not upgraded their PoPs, service is fine when there is not much demand, but there can be slowdowns as demand increases."

Some failures may be more human in nature, as workers may not be available to replace or repair failing equipment.

"To the best of my knowledge, we have not seen that happen yet, but if large numbers of people become sick, we may see outages and slowdowns because personnel are not available to make repairs," Davidson said. "If the disruption lasts a longer time, there may not be adequate spares of critical equipment available because of supply chain problems."

He said even with failures, internet service doesn't crash, but the service does degrade.

"The underlying infrastructure of the internet, called transmission

control protocol and internet protocol, is a 'best-effort network' – it does not provide a guarantee of a particular quality of service," Davidson said.

Nor can the internet handle unlimited traffic.

"At some point, capacity at choke points or bottlenecks will be reached," he said.

The increased traffic also provides opportunities for malefactors, through various attacks—such as denial of service, distributed denial of service attacks or ransomware attacks—where data can be held hostage for money.

"Typically, these attacks target a particular service or site," Davidson said. "Maybe I decide I want to prevent people from going to some critical government site. I could certainly do that for a short period time with a DDoS attack. We have gotten pretty good about detecting these attacks and mitigating them, although there are still research challenges for sophisticated attacks, but there could be periods where the service is not available."

With more traffic on the internet, people are more vulnerable.

"Likely people will try to use services they are not familiar with because they did not need to," Davidson said. "I imagine more people are taking advantage of online banking, which provides an opportunity for cyber criminals. Similarly, people are contacting friends and family over the internet when they perhaps they did not do so before. They may be more susceptible to spear-phishing attacks. As always, one must be vigilant in making sure emails are from legitimate sources. Never give someone personal information over the phone or via the internet."

There can be a larger cybersecurity threat with more employees working

at home.

"Many employees may be using their own desktops, laptops and mobile devices," said Angela Orebaugh, director of Cybersecurity and IT Programs in UVA's School of Continuing and Professional Studies. "These devices may lack security controls, such as antivirus and host-based firewalls.

"We are already seeing an influx of malware and ransomware now being delivered through phony COVID-19-related emails and text messages. Employee-owned devices (and their potentially vulnerable users) are the low-hanging fruit for compromise. Some organizations are rolling out mobile device management software and other security software to help protect employee-owned devices. Employee-owned or not, everyone needs to be extra vigilant right now for phishing emails and texts."

The University has posted online security tips for coping with cybersecurity threats, such as gift card scams, which are email and text messaging spear phishing attempts; and malware attacks, as well as tips on working and attending school remotely, guidance on making devices more resistant to attack and tips on safe Zoom videoconferencing.

Orebaugh said with potentially unsecured devices, organizations have increased their attack surface.

"Attackers can enter the organization's network through the employees' VPN connection," Orebaugh said "Since this connection is encrypted, security staff will have a difficult chance, if any, to detect any attacks over this channel. Additionally, since many organizations did not design their virtual private network infrastructure to support a nearly 100% remote workforce, the increased load on the VPN creates its own denial of service attack with lack of availability. Some organizations are moving to shift work to address this."

Remote employees may also begin using creative solutions at work, such as third-party applications and services that may not be approved by the organization and could open new vulnerabilities in the system.

"There will be dodgy offers out there, such as for document storage and videoconferencing services that have lax security or, even worse, purposely steal and spy on information," Orebaugh said. "Employees should only use applications approved by their organizations. If an employee thinks they have been compromised for any reason, they need to call their employer's helpdesk support line first."

Orebaugh said it is very important to back up files frequently.

"If a device is compromised with ransomware, you don't want to restore from a backup that is a month old," Orebaugh said. "I have started doing my personal backups almost daily, which is a good practice anyway. I plug in an external hard drive at night while my computer is disconnected from the network and do an incremental backup and then unplug it. I also have an online service that backs up in near-real time."

She said organizations should use shared document platforms for their information.

"This document store should already be backed up every day, but right now it is even more important to make sure this is happening," Orebaugh said. "Organizations that are not using backup redundancy, different methods, stored in different locations, should implement them."

Students working from home may be vulnerable, and they may compromise their teachers as well.

"The biggest issue I am concerned with is uploaded documents from students," Orbaugh said. "I often need to download and open Word

documents to grade. This is a great way for malware to spread, especially from student computers that may not be secure and are already infected."

She said online learning systems should have a malware scanners; in the cyber-connected world, many devices are interconnected, including household devices.

"For the "Internet of Things," if a user has an IoT device at home that is compromised, he or she should assume the entire home network and all devices are compromised, or at least vulnerable," Orebaugh said. "This means that malware and attacks may use an IoT device to compromise other devices, such as a user's desktop or laptop. If that is the same system that a user uses to connect back to an organization, there could be a security incident in the works because compromised IoT devices could be used as a launch point for attacks."

And people need to be wary of potential threats.

"Social distancing doesn't work for the spread of digital viruses," Orebaugh said.

Provided by University of Virginia