# Q&A with Jason Hong on scams and other vulnerabilities during the COVID-19 pandemic

April 1 2020, by Daniel Tkacik

Credit: CC0 Public Domain

As the COVID-19 pandemic continues to impact countless aspects of everyday life, CyLab researchers are monitoring its effects on people's cybersecurity and privacy.

Jason Hong, a professor in Carnegie Mellon's Human-Computer Interaction Institute, thinks that right now, people need to be even more aware and cautious online.

**A lot of your research centers around online scams—anything from phishing emails to websites offering crazy deals—that result in users' machines being infected with malware. Have you seen an uptick in these sorts of scams during this coronavirus pandemic?**

Anytime there's some big issue or threat going around like right now, scams will begin to circulate preying on people's fears—that's undoubtedly going on with the coronavirus pandemic right now. And given that the stimulus bill just passed, I wouldn't be surprised if more scams started coming up. Anytime there's money involved, there's always going to be scammers who try to figure out how to make an extra buck off you. These would typically show up in the form of a phishing attack—an email that you receive that may look legitimate, but it's really just someone trying to get you to share your credentials, or to click on something that may put malware on your computer.

Given all of this, people need to be aware that these scams are going around, and they need to be extra cautious of emails they receive asking them to login to something or download an attachment. In general, people should never click on a link or download an attachment in an email if they're not sure who the sender is.

**There are reports that this sudden surge in working from home may be making businesses and organizations more vulnerable. What's the thinking behind that?**

I have no data to support this right now, but I wouldn't be surprised if malicious hackers weren't trying to take advantage of this situation where all of these office workers trying to work from home, where they may be on less secure networks than they would be at the office. If they're using their personal computers, those usually aren't as secure. If they're using it to watch videos or browse social media, they might inadvertently get malware on their computer, which could be a problem for the employer.

For larger corporations, if the IT support desk person is working from home, they might not be able to easily monitor what's going on with their internal networks. With all of the anomaly detection that's going on, now you have this major blip in how people's behaviors have changed, which will affect the machine learning models or any kind of intrusion detection, leading to difficulties in deciphering signals.

**What are your suggestions for people working from home to do so differently?**

Try to keep your computer secure. If you're using a work laptop, that'll probably be much better because it'll already be fairly secure, but if you're using a personal computer, and it has malware, that could be really bad not just for you, but also your employer. You may never have thought before to run anti-malware software on your computer, but now is the time to do that, because you're not only putting risk on yourself, but also the company that sends you a paycheck each month.

Also, make sure your kids aren't using your work laptop, because children aren't always the best when it comes to avoiding malware.

Provided by Carnegie Mellon University

Citation: Q&A with Jason Hong on scams and other vulnerabilities during the COVID-19 pandemic (2020, April 1) retrieved 23 April 2024 from https://techxplore.com/news/2020-04-qa-jason-hong-scams-vulnerabilities.html