Q&A with Lujo Bauer on how the pandemic is affecting individuals' privacy and security

April 17 2020, by Daniel Tkacik

CyLab's Lujo Bauer says it's easy to spot scams under normal circumstances. But these are not normal circumstances. Credit: Carnegie Mellon University

Many Americans have been working remotely for over a month now in response to the COVID-19 pandemic, which has resulted in new paradigms in their own and their employers' cybersecurity and privacy. CyLab's Lujo Bauer, a professor in the department of Electrical and

Computer Engineering and the Institute for Software Research, has been monitoring the situation.

Many experts in the field are saying that social engineering attacks and scams have the potential to be more successful during this pandemic. What's the thinking behind that?

Things are not normal right now; routines are up-ended. It's more likely now that we get requests to do things from people we don't know or for things that we don't normally do.

It's easier to spot a scam under normal circumstances. The emails you normally receive are from people who you expect to be emailing you, and they're asking you for relatively normal things; a scam email is more likely to stand out as being unusual.

But now we're changing how we do work, who does which work, where data lives, and so on. Coping with these changes often requires us to be doing something unusual or asking someone else to be doing something unusual for us, for legitimate reasons. Unfortunately, that makes it harder for a social engineering attack to stand out, because a social engineering attack will be just one unusual thing in a sea of many unusual things as opposed to one unusual thing when everything else is normal.

Not only are scams being hidden in a sea of not-normal requests, but the speed at which we have to respond is different as well, right?

Yes, we're now more frequently forced to make important decisions, big and small, more quickly and with less deliberation. This increases the chance that we'll fail to think things through enough to recognize a social engineering attack.

We're having to re-organize how workplaces operate. In order for a hundred employees tomorrow to be able to do a certain kind of work from home, a certain kind of security measure might need to be relaxed. And it might need to be relaxed right now—we don't have time to think through whether we really want to do this because it seems like work will totally come to a stop if we don't. This kind of pressure to make decisions *now* even if we know they are decisions that deal with something risky, that again is something that plays into the hands of social engineering attackers.

How have the changes to workplace operations affected employees' privacy?

If you were considering a piece of software that had cool teleworking features, but you were worried about its [privacy](#) implications, previously you might have erred on the side of caution and said, 'No, we won't go for that software even though the features are cool.' Now, you might think, 'Well, I really need to make it as easy as possible for employees to be productive from home,' and that might sway you to the side of privacy not being as important. It's one of these situations where we need to do new things and therefore we need computer systems that offer new features. There's often a tug-of-war between more features and more privacy, and now because there's a demand for more features, privacy loses out somewhat.

There's another impact on privacy that we've thought about. Under normal circumstances, we would expect our personal and professional lives to be reasonably separate; we'd be able to keep most aspects of our personal lives private from our colleagues if we wanted to. This separation is now being eroded. For example, I might be able to see the background of the room in your home that you're working in, which maybe isn't something I would ever have seen otherwise. You could have family photos or memorabilia in the background that reveal something

about your [personal life](#), something that you might not have previously told a coworker about. In ways like this we're now sharing more information with coworkers, but what we're sharing and the consequences for our work relationships and [professional lives](#) are not necessarily well thought out.

It's also noteworthy that this kind of erosion of privacy is biased by economic circumstances, in the sense that people with more resources are more likely to have a home office, which is likely to reveal less about one's personal life, then, say, a living room or bedroom that has to do double duty as an office.

Provided by Carnegie Mellon University