Zero Trust

Jerome Z. Cunningham

Technology and Public Administration: 20:831:521:01

Dr. Lisa Mahajan-Cusack

December 11, 2022

Zero Trust means we shouldn't just trust everything we get from the AI community. We should be cautious about the information we receive daily. We get information in our email from sites we have been doing business with for years and from areas trying to obtain our business. However, how do we know what those sites do with our information? Can we trust them to protect us from cyberbullies? How is our data protected? With the world at our fingertips from utilizing online communication methods, we put ourselves at risk every day. There is no relaxing and getting comfortable with the personal information we share in cyberspace.

Sometimes, it is a second thought because most of us have not had to deal with our data being compromised. We sometimes get messages saying our data has been breached by some vendor or company with whom we have a relationship. Then, after monitoring our accounts for a few weeks for spontaneous activity, we moved on like nothing ever happened. How do we trust the government is performing its responsibility of protecting us? One of the questions we must ask ourselves is who needs access to our information and why. What tools are in place for internal and external use within the organization?

There is a constant demand now to do business on the internet, and why should we trust these sites? One reason is that our information is in so many systems from the day we apply for social security cards, apply for a job, and apply for credit. So, we begin to forget to have zero Trust.

One of the takeaways from the webinar was how so many companies switched to having staff members work from home during the pandemic. Were they ready for it? We started working from home on our personal computers. We didn't give a second thought about how more significant this issue of cyber crooks stealing our information by hacking into the systems. We didn't ask our corporations critical questions about how they would handle such an issue if that had happened. We forgot to engage the industry because we thought of the conveniences of working from home. How safe was it to use

VPN access? We didn't have zero Trust; we automatically assumed the VPN system would work so that we could perform our job duties. We trusted the flexibility of a schedule over the security of a system.

Another takeaway was how the cyber system was supposed to sustain itself, especially in smaller businesses where there would have been a capital funds issue. I didn't think of them applying for grants like the larger companies would do. Instead of companies using their capital, they were obtaining these funds through donations to combat the issues in the cyber security world. So, again, check the more prominent companies' websites to see how they handle the situation in real time.

The conclusion is to stay vigilant on what information is coming into the company, along with the lead going out. Ask questions about who needs to have your input. Purge data that is no longer useful for you and just holding space. Take advantage of government funds set aside to assist you with securing data. Finally, keep a zero-trust frame of mind, which may help you avoid pirates in the cyber security world.