

Jaya Baloo - "Always check before you click!"

These are the highlights of Jaya Baloo's talk at the SingularityU South Africa 2020 Summit.



Jaya Baloo, chief information security officer at Avast Software.

Jaya Baloo, chief information security officer at Avast Software and SingularityU Faculty of cybersecurity and Quantum Computing, addressed delegates at the SingularityU South Africa Summit 2020 that was held earlier this month.

“Always check before you click!”

Baloo started her talk with breaking the misconception that while we have retreated to our homes during the pandemic, we have been under a false sense of security. In fact, working at home has a major danger – hacking. She describes it as a “veritable hackfest” due to the viruses that have been seen online.

During this time, hackers have taken advantage of people’s emotions and insecurities. Scams have targeted people’s vulnerabilities. Fake webshops have been one of the biggest culprits, claiming to sell things like discounted medical equipment, masks, gloves, fake testing kits etc. In London alone, over 500 webshops were taken down by the police in a single month. They took advantage of local and international organizations. Scammers know that attacking organizations like WHO make-believe their scams.

Corona related phishing attempts have been rife. In March 2020, there were over 1 million different types of phishing

attempts.

Not only this, people have staged phoney promotions related to news sites, such as a pandemic related survival book, which was actually available free elsewhere, sold under the brand of a news site. All of this happens because scammers know that they know they must use reputable brands to gain your trust. This is called malvertising. It is designed to get you to click on mal-ware.

Ask yourself. Is your browser up to date? When last did you do an update? Those that don't get taken advantage of. Your username, IP address and other information gets sent to attackers.

Our infrastructure eg hospitals need to protect themselves during the pandemic. Some hospitals were not able to take care of their patients as they were under cyber attacks. Phishing mails are one of the biggest attack methods. This is a moment of education for the healthcare community.

Baloo explained that at Avast, they try release tools for the security community so that they can try to understand what is happening. They also recommend you check which apps you use. They developed a tool called [AkPlab.io](https://www.akplab.io) to check your apps. This is an Intelligence-driven threat hunting platform for the security analyst Community. Since March, over 450 000 coronavirus related apps that were not what they claimed to be have been identified with this programme. They then shared the "Indicators of compromise" across the security community.

Make yourself less vulnerable. Be safe online when working from home. Do regular updates. Use a VPN when sending sensitive information. Use anti-viruses. Passwords should be as long as possible, changed often and should not be left lying around. And never, ever forget to back up both online and offline! Use secure apps and security apps. Use encryption tools like Signal for your messaging. Always check before you click! Be safe out there.

For more, visit: <https://www.bizcommunity.com>