TikTok and Cybersecurity - Just The Facts
Flash Briefing Questions

ProCircular's Director of Incident Response, Nic Stevens, answered the following audience questions from our "TikTok and Cybersecurity - Just The Facts" Flash Briefing:

- Does the TikTok application have to be open in order for the risks to be operable?
  No, the application does not have to be open to provide access to your data and activity.

- Is it recommended to set all permissions to "Not Allowed" under the phone's app settings?
  Possibly, but access to your data and activity, and potential influence campaigns is still a risk.

- If our employees use TikTok on a personal phone via their cellular connection, could TikTok be potentially hearing and recording those conversations our employees have with customers and other employees?
  Yes, if the end user has provided the app permission to access the camera and microphone.

- Can you speak on the difference in the TikTok federal legislation introduced and passed by Senate in terms of government device policy vs. the civilian policy?
  I believe that the legislation passed by the senate is designed to block TikTok on federal government devices only, but the risk is the same for all US citizens.

- Which social media platform, if any, would be the safest for business use?
  I think any platform not owned by enemies of the US would be safest for business use.

- As far as the keylogger goes, if I have typed a password on my phone and have the TikTok app installed, should I consider that password compromised?
  No, but if you typed a password in a 3rd party website, using the TikTok in-app browser, you should be concerned.

- When using Microsoft's Conditional Access, users can access company data via enlightened apps on their personal phones, which are not being managed by an MDM or Intune. Are Microsoft's enlightened apps secure enough to protect from TikTok accessing them?
  I'm not sure if this is a catch all for data being accessed by untrusted applications installed on your mobile device.

- Is the TikTok version you run as a webapp, in any web browser, safe or safer? (As long as you don't install the app?)
  Yes, because the webapp does not have the same over-reaching permissions and access to your data and device.

- Should you block TikTok on business networks?
  Yes, it is recommended to block all TikTok traffic on corporate networks. While the risk is the permissions and access to your device, data, activity, etc., blocking TikTok traffic on corporate networks provides multiple layers of protection in addition to blocking the app installs.

- Do you think the microphone and camera are active all the time?
  Yes, they are accessible to applications that have been granted permission to be available all the time.

- How do you suggest managing employees that have TikTok on their personal devices?
  It's recommended to uninstall TikTok from all devices. I think employee education is key to "managing" personal devices. If your employees are aware of the risks, they may be willing to protect themselves and the organization in combination to corporate managed devices.

- In general, if a firm allows access to corporate email, OneDrive, etc. on personal devices, is there is reason to believe that TikTok does or might eventually gain access to those data points?
  It's a valid concern, and why we recommend uninstalling TikTok from all devices, both corporate and personal.

- How securely protected is the data that TikTok collects?
  The risk is the access to your data and activity, and potential influence campaigns, however, I'm not sure I can speak to how securely they protect your data.