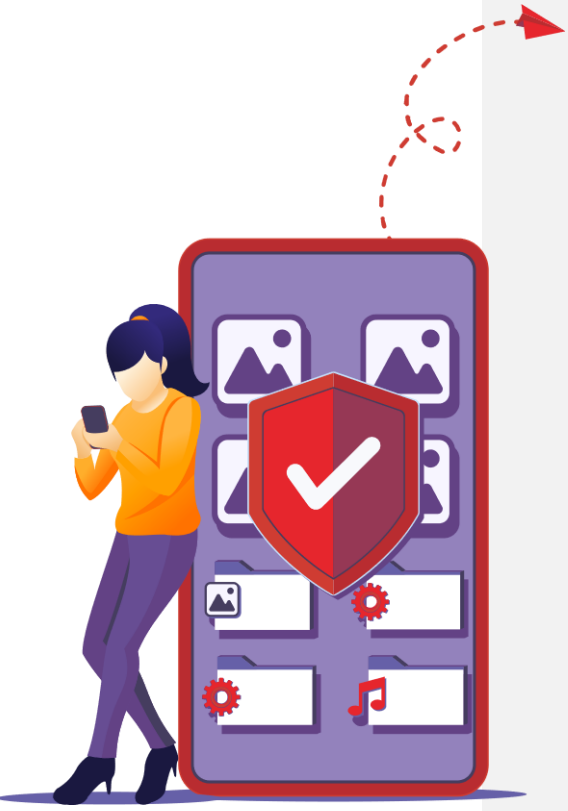
CottGroup®
Holistic Business Services

VeriSistem®
a CottGroup® company

SECURITY
OF SMART DEVICE

Could It Be That Your Work Calls Are Being Tapped?



Coronavirus (Covid-19), which has become the common agenda of everyone all over the world, also impacted the business world from various points. Most companies have shifted to remote working with consideration of both the health of their employees and to help prevent further spread of the virus. So, how well are employers and employees are aware of the risks that remote working can lead to in terms of companies' privacy, security and confidentiality processes?

Have you ever thought that your phone calls or video conferences with your stakeholders and clients, discussions about your business processes with your teammates, a psychologist who has a session with his client, a doctor who talks about the treatment, the disease with the patient could be tapped?

Due to the Wrong Detected Commands by Smart Devices, you may be Tapped

19 Times a Day, During 43 Seconds

in Average for Each

Could your conversations made via virtual assistants in your smartphones such as Siri, Google Assistant or via smart speakers be tapped to improve voice recognition features? It is an indication of this situation that these applications and devices that you need to say the command phrases in order to fulfill your instructions are always actively listening to you.

The researches show that these applications and devices can be activated with the expressions they heard wrong, apart from the command sentence established to become effective. The application, which is activated by the command "Hey Siri", can be accidentally activated by expressions such as "They very" and "Hey sorry", as well. Furthermore, there are also studies showing that these applications and devices are opened with an incorrect command, for an average duration of 43 seconds each time and 19 times a day.

Considering all this information, what needs to be done is quite simple: Smart speakers can be turned off or switched to silent mode during this period of remote working. The microphone permissions of the applications on your smartphones can be turned off.

In addition, the software used to prevent tapping of virtual meetings should be set up to establish a strong encrypted communication.

You can access our article with further information about technical issues to be considered during remote working here.

CottGroup®
Holistic Business Services

Astoria Towers
Kempinski Residences
Büyükdere Caddesi No:127
B Kule Kat:8 34394 Esentepe
Şişli / İstanbul / Türkiye

www.cottgroup.com www.verisistem.com ask@cottgroup.com +90 212 244 9222