GUARDSIGHT

https://www.guardsight.com

Cybersecurity Tips For Remote Workers - Location Services

1. LIMITING LOCATION DATA EXPOSURE

Mobile devices inherently trust cellular providers, and cellular providers receive real-time location information from a mobile device every time it connects to the network. It is an open secret that providers sell data, including near real-time location data, to third-parties. Location data from a mobile device can be obtained even without provider cooperation through the use of a rogue base station with a stronger signal than the authentic cell tower. Additionally, location data is stored on the mobile device through browser cookies, WiFi logs, and Bluetooth sensors.

Be in the know on facts related to location services and learn about ways you can minimize your footprint.

2. IN-THE-KNOW

LOCATION SERVICES ≠ GPS	Users can disable location services in the settings of a device, but this *does not turn off GPS*. Disabling location services only limits access to GPS and location data by apps. It does not prevent the operating system from using location data or communicating that data to the network. GPS is not the same as location services. Even if GPS and cellular data are unavailable, or turned off, a mobile device will calculate location using Wi-Fi and/or BlueTooth. Apps and websites can also use other data (that does not require user permission) to obtain or infer location information.
LOCATION CAN BE DETERMINED EVEN IF DEVICE IS TURNED OFF	Even if all wireless features are disabled, numerous sensors on the device provide sufficient data to calculate location. When communication is restored, saved information may be transmitted.
THE RISK ISN'T LIMITED TO MOBILE DEVICES	Anything that sends and receives wireless signals has location risks similar to mobile devices. This includes, but is not limited to, fitness trackers, smart watches, smart medical devices, IoT devices, built-in vehicle communications, household smart devices (light bulbs, cookware, thermostats, home security). Most of these devices have no way to turn off wireless features, and little, if any, security built in. These security and privacy issues could result in data being freely leaked. Yes, your light bulb could be telling on you.
APPS AND SOCIAL MEDIA	Many apps request permission for location and other resources that are not needed for the app to function. Users should be careful about sharing information on social media. For example, pictures posted on social media may have location data stored in hidden metadata. Even without explicit location data, pictures may reveal location information through picture content.

3. MITIGATIONS

- Disable BlueTooth and turn off Wi-Fi if not needed
- Use Airplane Mode when the device is not in use
- Set an app's locations services permission to either "not allow" or "only allow when app is in use"
- Disable advertising permissions to the greatest extent possible
- Use a VPN to help obscure location

For additional advice or to learn more contact us: info@guardsight.com