Protect Yourself: Commercial Surveillance Tools

Companies and individuals have been selling commercial surveillance tools to governments and other entities that have used them for malicious purposes. Journalists, dissidents, and other persons around the world have been targeted and tracked using these tools, which allow malign actors to infect mobile and internet-connected devices with malware over both WiFi and cellular data connections. In some cases, malign actors can infect a targeted device with no action from the device owner. In others, they can use an infected link to gain access to a device.

These surveillance tools can:

- Record audio, including phone calls.
- Track phone's location.
- Access and retrieve virtually all content on a phone, including text messages, files, chats, commercial messaging app content, contacts, and browsing history.

Below are common cybersecurity practices that may mitigate some risks:

- Regularly update device operating systems and mobile applications.
- Be suspicious of content from unfamiliar senders, especially those which contain links or attachments.
- Don't click on suspicious links or suspicious emails and attachments.
- Check URLs before clicking links, or go to websites directly.
- Regularly restart mobile devices, which may help damage or remove malware implants.
- Encrypt and password protect your device.
- Maintain physical control of your device when possible.
- Use trusted Virtual Private Networks.
- Disable geo-location options and cover camera on devices.
- While these steps mitigate risks, they don't eliminate them. It's always safest to behave as if the device is compromised, so be mindful of sensitive content.

For additional information on NCSC awareness materials or publications, visit our Website: www.NCSC.gov