Slide 2 Everyday Use

All of us use IOT devices or apps every day. Most of them aim to make something easier, give us information, or to make us feel safer like an app connected to security cameras. But what most people don’t think about is that our devices and the apps on them can be a danger to your privacy, security or even both.

Slide 5 Data Storage

Not all of the data that some apps or devices might collect is immediately sent off to an advertising agency, or to the highest bidder. Some data stored by IOT apps is kept on your device, this can be sensitive data like something as simple as “Front door open” just stored in a plain text format that could easily accessed by an attacker that knows what they’re doing.

Slide 9 Delicate Balance

You can’t always have the perfect balance of security and usability either. Sometimes it simply isn’t necessary to add a ton of security to a device that doesn’t deal with sensitive information. Something like an outdoor digital thermometer that doesn’t interact with anything else. It just has its one simple purpose. Adding security like a need for a fingerprint to see what the temperature is outside would just be annoying to most users, and wouldn’t really provide meaningful security. So it’s important to gauge how much security we really need for some devices.

Slide 10 Conclusion

In conclusion, we give IoT apps and devices access to a lot of sensitive information, sometimes without even realizing it. Its easy to just hit that accept button on that terms and conditions page and forget about it, when in reality, you just signed a 30+ page document allowing the company to do whatever they want with your device, and the information on it. so It’s important to be informed and to know where your data is going, as well as who can see it… Does anybody have any questions?