U.S. AIR FORCE
CHIEF INFORMATION SECURITY OFFICE (CISO)

The office of the Chief Information Security Officer enables the US Air Force core missions – to fly, fight, and win – by ensuring the cybersecurity and resiliency of systems, information, and staff.

What is the Internet of Things (IoT)?

The IoT refers to the ability of everyday objects to connect to the Internet and to send and receive data.*

IoT devices connect to the Internet via Wi-Fi, Bluetooth, or cellular data.

IoT devices include fitness bands, heart monitors, crockpots with Wi-Fi capabilities, virtual assistants, etc.

The average American interacts with **6** IoT devices per day.*

How might my IoT device pose a threat?

- Collects, transmits, stores and/or shares vast amounts of consumer data; some of which could be highly personal
- Having limited security settings makes your device(s) vulnerable
- Difficult to protect - once deployed, devices run in "default mode" with limited security settings

Questions to Ask Yourself

1. Is this device connected to a network? If so, how?
2. Can I secure my IoT?
3. Should I disable connectivity before I come to work or even bring my device in at all?

Know the security capabilities of your IoT device

- Find out if you can install anti-spyware and anti-virus software; be sure to update regularly
- Lock via passcode, when possible
- Research the device's data collection and storage capability – avoid discussing sensitive data for good measure

Changing your security mindset could help protect you from an incident!

Stop attacks in their tracks before they impact the Air Force and your personal life.

*FTC Staff Report 2017