KENNESAW STATE
UNIVERSITY

Module 15:

Smart Mobile Home Devices

Safety Guidelines

Dr. Maria Valero

Agenda

- Smart Home Devices Vulnerabilities
  - Thermostats
  - Home Security Systems
  - Lighting
- Best Practices in Smart Homes

Smart Home Devices Vulnerabilities (1)

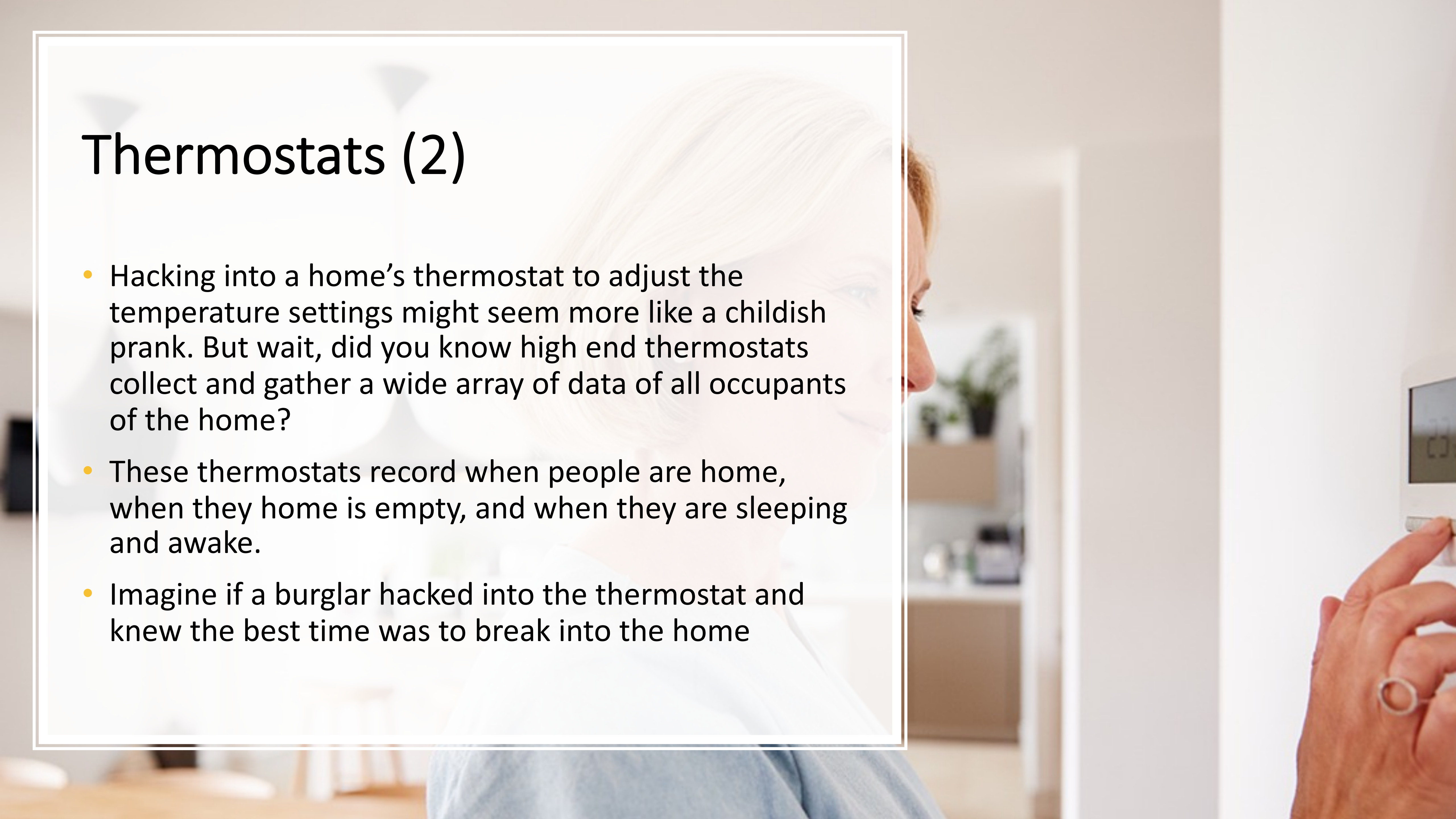
- Many smart home device manufacturers were quick to get their products to market but overlooked potential security risks once connected to a home network.
- Security has not been a top priority, but rather what features can be crammed into the devices to make it appealing for consumers

Smart Home Devices Vulnerabilities (2)

- What many people do not realize is if one device is hacked within the home, it could easily serve as a hub, or gateway for the hacker to gain access to all the home's connected smart devices
- In addition, the security of some smart home devices might seem irrelevant, but let's take a look at a few of these and discuss how they could pose risks for you and your family

Thermostats (1)

- With hydro bills surging, many people are installing smart thermostats in their home to help monitor and manage energy usage
- It is easy to connect to a thermostat using an app from your smartphone. Unfortunately, it is easy to connect to smart thermostats within homes and hack into them using the app



Thermostats (2)

- Hacking into a home’s thermostat to adjust the temperature settings might seem more like a childish prank. But wait, did you know high end thermostats collect and gather a wide array of data of all occupants of the home?
- These thermostats record when people are home, when they home is empty, and when they are sleeping and awake.
- Imagine if a burglar hacked into the thermostat and knew the best time was to break into the home

Thermostats (3)

- Furthermore, an experienced hacker could also co-op other connected devices, like your home's security system and shut it off!

Home Security Systems

- From Wi-Fi security cameras to wireless automated door locks, these smart devices have serious security flaws.
- Hackers are easily connecting to these devices and have been able to obtain camera footage and pin codes to unlock doors. They can even hack into connected automated garage door openers.

Lighting

- Again, hacking into your home’s smart lighting might seem childish and not a serious security threat
- Other than being concerned about excessive energy bills, the lack of security within the devices can provide easy access to your home’s entire network of smart devices

Best Practices in Smart Homes

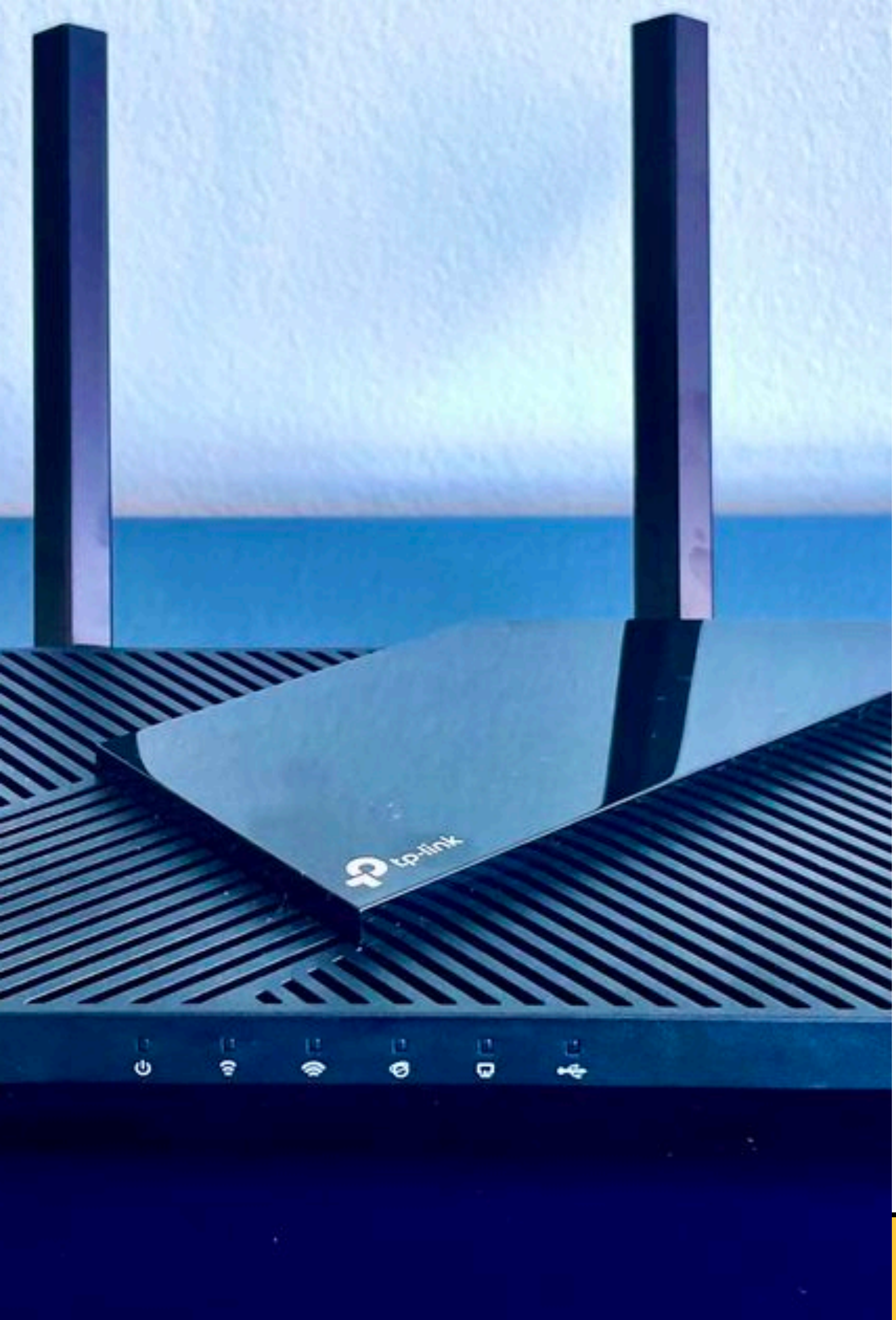
- Constantly Update your Devices
  - Unlike macOS or Windows, smart home gadgets do not automatically seek out updates and install them in the background. In many cases, they may not be connected to the Internet at all. It is a homeowner’s responsibility to check for updates, which often include patches that guard against newfound hacking techniques. They can also check the manufacturer’s website to see if the company has discovered any recent security exploits.

Best Practices in Smart Homes

- **Check all the settings on each device**
  - Whether it’s a refrigerator that knows when you are out of milk or lights you can control from your smartphones, you should explore settings on each device, so you understand everything each device can do. If a gadget doesn’t need access to the Internet, disconnect it. If the homeowner needs a password to access the device, choose one that’s difficult to guess.

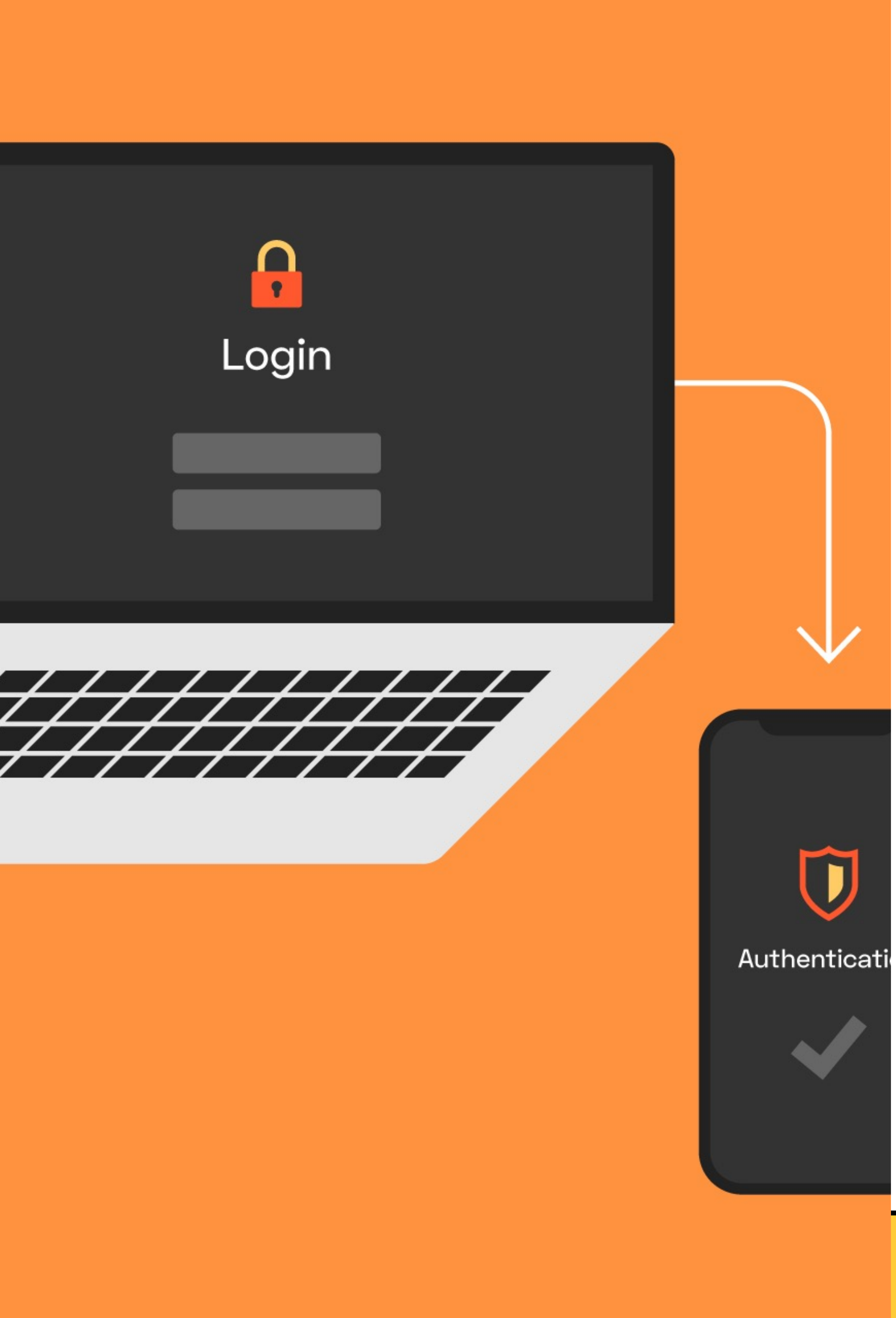
Best Practices in Smart Homes

- **Buy from reputable brands**
    - When choosing smart home devices, be wary who you buy from. Although big brands, such as LG and Samsung, aren’t impervious to hacking, they are much more likely to correct an issue with an update if a new security exploit is discovered. Before buying any new smart home gadget, research the manufacturer to make sure it has robust security measures in place.



Best Practices in Smart Homes

- **Pay special attention to routers**
  - Since the router is like a gateway to most smart home gadgets, you should try to make it as secure as possible. This means changing the default username and password to something unique. It also means ensuring that the router is running the latest firmware upgrades. You should also prevent devices from connecting to the Internet, unless they absolutely have to in order to properly function.



Best Practices in Smart Homes

- **Double up protection**
  - Encourage the homeowner to use two-factor authentication – such as a one-time code sent to a smartphone – to keep the bad actors out of their smart home accounts.

Best Practices in Smart Homes

- **Avoid public Wi-Fi**
  - You may be tempted to manage your smart home devices while sitting in a coffee shop on the other side of town. If they are using public Wi-Fi, however, you could leave your systems vulnerable to security issues. Instead, use a VPN, which offers layers of security and privacy features for both home and public Wi-Fi.