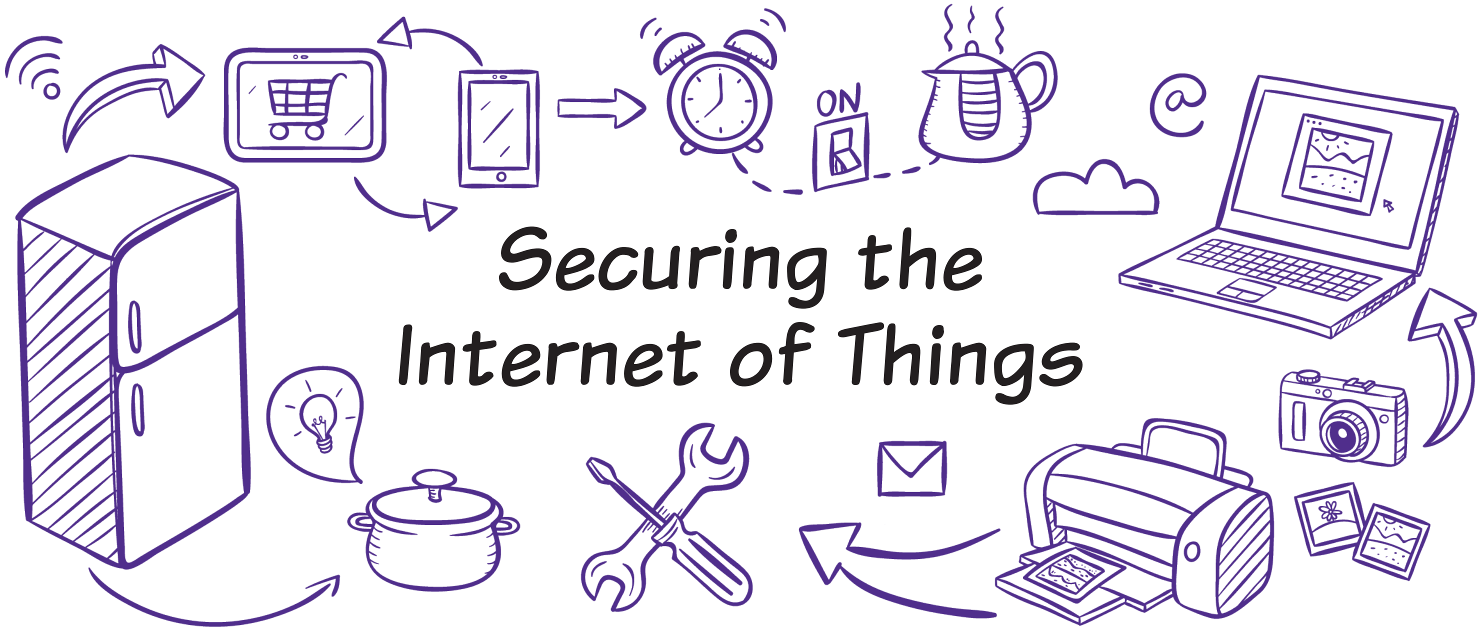
Securing the Internet of Things



The Internet of Things, or IoT, refers to the broad range of internet-connected devices that offer many different services and functionality. From consumer products, like digital assistants and remotely accessible security cameras, to smart hospitals and manufacturing plants, the potential advantages of the IoT are nearly limitless. The IoT also ushers in concerns of privacy, security, and safety.

Privacy
Smart devices collect a significant amount of data from users and their environments. If not properly secured, that data could be accessed by unauthorized parties for malicious purposes.

Security
Many devices lack adequate security features, which makes them highly susceptible to cyberattacks. They often ship with default passwords that some consumers fail to update, which makes those devices especially vulnerable.

Safety
Imagine if a cybercriminal discovered a way to take control of an internet-connected machine at a factory. It could allow them to cause physical damage or put the safety of workers at risk.

Clearly, the IoT unlocks an amazing world of potential, but it also unlocks a world of concern. The question becomes, how can we take advantage of that potential while also mitigating some of those concerns?

At work, the answer is simple: Follow policies, especially where connecting personal devices to an organization's network is concerned.

At home, research products before purchasing to learn about how they handle security and privacy. Be sure to update default passwords immediately. And consider disabling any features you won't use, where possible.

As always, security and privacy in the modern age require remaining aware of threats and being proactive to avoid them. So stay alert and stay informed when using the conveniences of the IoT.

SAC the security awareness™ COMPANY
a KnowBe4 company