How to make sure **connected lighting defeats potential hackers**

In this digital age, cyberattacks, malware, and ransomware are rarely out of the headlines. But it's no longer just our laptops and computer networks that are coming under close scrutiny. Now considered the backbone of the Internet of Things (IoT), connected lighting is coming increasing under the spotlight when it comes to cybersecurity fears.

Peter Duine
Global product
manager connectivity

> At Signify, we believe security is paramount **to give customers confidence in connected lighting systems.”**

20 billion reasons to worry

The reason is simple. Devices that may look harmless, like switches, sensors, and even lightbulbs, are some of the 20 billion things that are connected to the cloud and operate 24/7. But when they have their own IP address and internet connection, it makes them vulnerable to hackers. And by exploiting a weakness in your lighting system, that in turn might make it possible for hackers to infiltrate other critical devices and systems in your IP network. To spread spyware or malware, override security alarms, disable cameras or access confidential information.

How widespread is the problem?

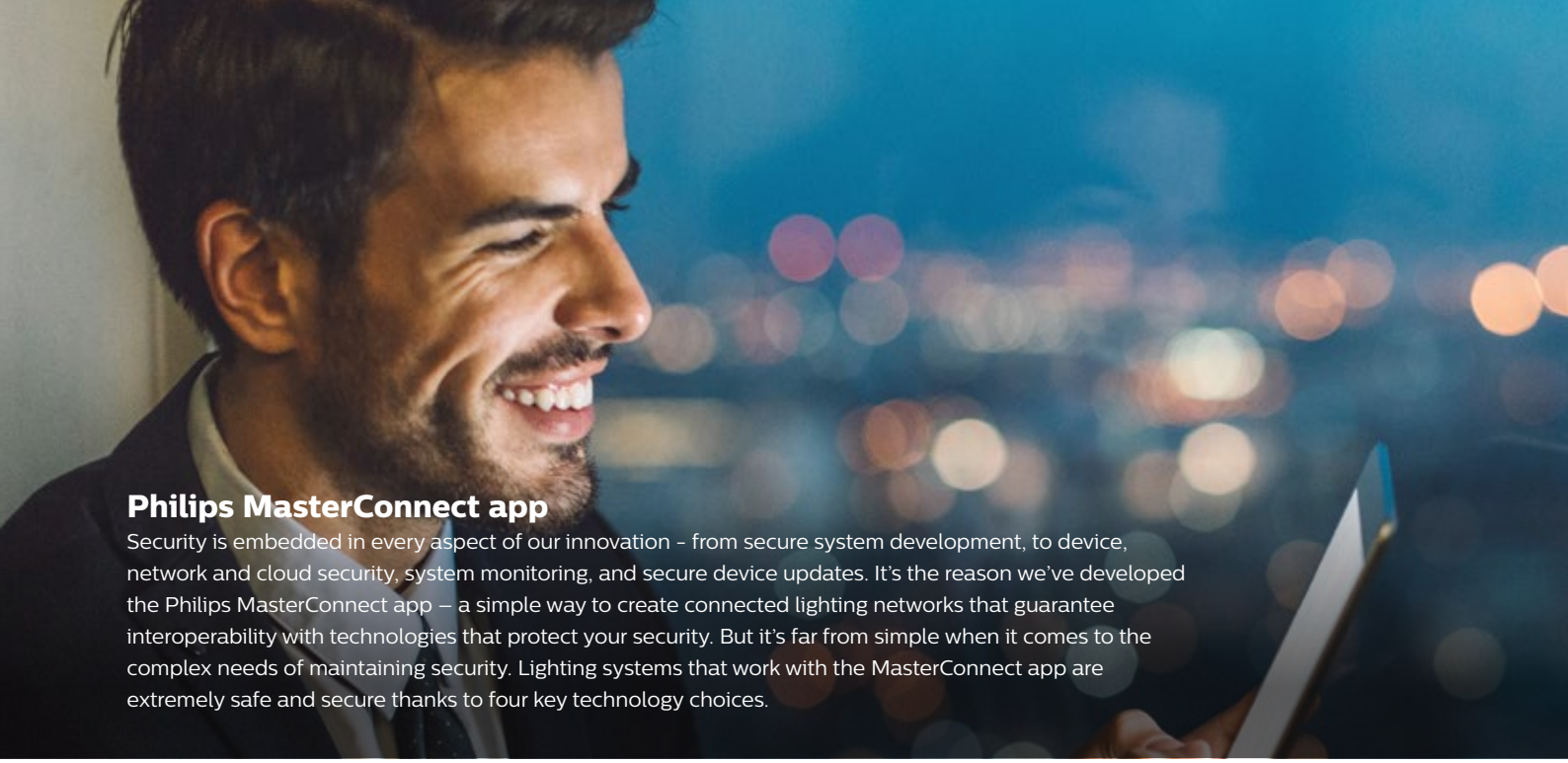
The Internet of Things (IoT) market is estimated to grow to 5.8 billion endpoints in 2022. That’s a 21% increase from 2019. And building automation, driven by connected lighting devices, is predicted to be the largest segment with a growth rate of 42% in 2020[1].

Gartner estimates that by 2020, 25% of attacks in enterprises will involve the IoT, yet the IoT will account for less than 10% of IT security budgets[2]. The problem is made worse because IT staff are less vigilant about IoT devices. Yet their long lifecycles make them increasingly vulnerable when they are no longer supported by manufacturer’s security updates.

What’s the solution?

It’s clear that operating lighting remotely over the internet requires a careful choice of technologies in order to withstand potential security breaches. At Signify, we believe security is paramount to give customers confidence in connected lighting systems. So they can automate operations, measure energy use, optimize productivity and track people and assets.

[1] https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io
[2] https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf



Philips MasterConnect app

Security is embedded in every aspect of our innovation - from secure system development, to device, network and cloud security, system monitoring, and secure device updates. It's the reason we've developed the Philips MasterConnect app – a simple way to create connected lighting networks that guarantee interoperability with technologies that protect your security. But it's far from simple when it comes to the complex needs of maintaining security. Lighting systems that work with the MasterConnect app are extremely safe and secure thanks to four key technology choices.

1

Secure encryption

Encryption is the cornerstone of any secure system. If you use a Zigbee network to control your lighting, any messages are masked. That means only devices that are part of the network have the security keys to enable them to participate in the operation of the lighting system. So the hacker's prying eyes will not be able to decipher the meaning of any messages that are transmitted. Although any security key can be hacked in theory, in practice the reality is very different. Each lighting network in a building will have around 20 lights, and a unique security key. Hackers would have to make multiple attempts to break into each of these 20-light networks before a whole building could be compromised; That would be a monumental effort that is unlikely to reap the quick wins that they often seek.

Lighting systems that work with the Philips MasterConnect app use the AES128 encryption standard. This has been proved to securely operate a wide range of devices around the globe. So you can rest assured, with MasterConnect app, your lighting devices can communicate securely without fear of malicious attacks of cybersecurity threats.

The commission app is available for download under the name of **Philips field app MC.** From Q3 onwards, this app will be renamed to Philips MasterConnect app for full inclusion of the new generation of Philips MasterConnect LED lamps that are Bluetooth enabled.

2

Security certificates

The real challenge is if rogue devices become part of the network and start operating with the secure encryption key. There's an obvious weak point when a network is created and assigned a network encryption key.

It's for this reason that all Philips devices have a birth certificate with an identity from a trusted certificate authority. Any rogue device that does not have our certificate authority will not be able to generate a private key to take part in the network. Each individual device that works with the MasterConnect app will carry this unique birth certificate key, which the app will use to set up a communication. No other Bluetooth Low Energy (BLE) connection can make itself known to these devices to generate Zigbee network keys. This is how our system is protected and achieves compliance to the IEC62443v cyber security standard. high security standards.

Signify has been recognized for its efforts to strive for **high security standards**

> **The Philips MasterConnect app** – a simple way to create connected lighting networks that guarantee interoperability with technologies that protect your security."

3

A dedicated mesh network

In lighting systems that work with the Philips MasterConnect app, the luminaires don't operate on a building's Wi-Fi network. Instead, they operate on a completely separate Zigbee mesh network that is dedicated to lighting. This means the luminaires cannot receive or execute any Wi-Fi commands. In this 'standalone' model, the lights are automated by connectivity, but without having anywhere near the capability that Wi-Fi devices have. For example, their physical bandwidth is not sufficient for them to be used to steal an email. In short, the devices that are controlled by the MasterConnect app to automate the lighting are connected locally, but they cannot by hijacked to access other critical systems for more sinister purposes.

4

Optional gateways

In lighting systems that work with the Philips MasterConnect app, there's also the option to use gateways for remote operations. These effectively form a bridge between the internet and the local connectivity of the luminaires. Gateways come with additional end-user benefits: they can apply remote overrides or pull up reports. And secondly, the gateway's micro-controller offers far more connectivity capabilities, enabling it to be updated remotely with the latest security mechanisms. But gateways also come with a caveat. Facility and IT managers are advised to check regularly for software updates, just as they would with company computers or mobile phones. Factory devices start out with open interfaces for both BLE and Zigbee communication, to ensure they offer the best operability for these third-party gateways. But they must be kept up to date with the latest security updates in order to prevent hackers from exploring and exploiting old weaknesses and system vulnerabilities.

What's the bottom line?

There is no 100% guarantee when it comes to cybersecurity; unhackable is impossible. But if you encrypt and secure BLE and Zigbee devices when they are first commissioned, we're confident that they can't be accessed. When integrated into a lighting system that works with MasterConnect app, we believe the resilience of such systems is strengthened even further. So businesses can capitalize on the promises of connected lighting with confidence, while avoiding the risk of potential security threats.

To learn more, go to philips.com/technology