**Botnets**

Cybercriminals can bring together huge numbers of infected devices into [networks called botnets](https://www.avast.com/c-botnet). These botnets can be used for a variety of things, but they are best known for their use in [DDoS](https://www.avast.com/c-ddos) attacks.

DDoS (Distributed Denial of Service) attacks send out a targeted stream of network requests from infected devices to the server, computer, or network that the bad actor wishes to bring down. As there are too many network requests for the target to handle, it crashes, and becomes unavailable for real users. In 2016, [a botnet brought down some of the biggest sites](https://blog.avast.com/ddos-attack-on-dyn-took-down-the-bulk-of-the-internet-on-friday), including Twitter and Netflix, using a DDoS attack.

### 4) Lack Of Physical Hardening

The lack of physical hardening can also cause IoT security issues. Although some IoT devices should be able to operate autonomously without any intervention from a user, they need to be physically secured from outer threats. Sometimes, these devices can be located in remote locations for long stretches of time, and they could be physically tampered with, for example using a USB flash drive with Malware.

Ensuring the physical security of an IoT device begins from the manufacturer. But building secure sensors and transmitters in the already low-cost devices is a challenging task for manufacturers nonetheless.

Users are also responsible for keeping IoT devices physically secured. A smart motion sensor or a video camera that sits outside a house could be tampered with if not properly protected.

### Knowledge Gap

While all of the technical vulnerabilities of IoT devices are important to note, it should also be remembered that all of them can be made worse [when users are unaware of them](https://www.vxchnge.com/blog/reducing-human-error-crucial-to-it). Since one of the great appeals of IoT devices is their convenience, people often don’t stop to think about how something as simple as connecting their tablet to the office WiFi could pose a security risk. Even if an organization doesn’t make extensive use of IoT devices, its employees likely will be using them in their own homes. [Making sure they understand](https://www.vxchnge.com/blog/effective-information-security-policy) why doing things like connecting a work computer to their home stereo over Bluetooth could potentially compromise data is a vital step in building a strong security policy that guards against data breaches.

The IoT revolution is already well underway, but many organizations are still struggling to [implement the security policies needed](https://www.vxchnge.com/blog/iot-challenges-and-solutions) to protect themselves from the risks associated with these smart devices. By identifying specific vulnerabilities that pose a threat to their networks and educating employees on practicing good habits when it comes to their connected devices, companies can take the first steps toward creating systems that are highly resilient and reduce the risks of data breaches and unauthorized access.