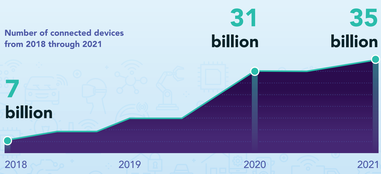
If You Connect It, Protect it

Section 1: Intro to IoT.

The Internet of Things (IoT) consists of billions of connected devices across the world that have the ability to share data.[1]

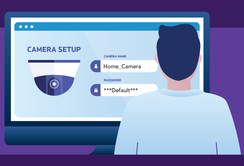
With the lines of home and work becoming blurred, bad actors can access much larger networks with less effort. Securing IoT is key to a successful remote workforce.[2]



Section 2: How can IoT be breached?

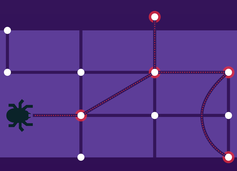
IoT devices have their own IP addresses, allowing them to transfer data over a network.

1. You set up a home security camera, but you forget to change the default password. You connect the camera to your wi-fi system.



2. A bad actor obtains the IP address of the security camera system.

3. The bad actor breaches the device and gains access to your network system.



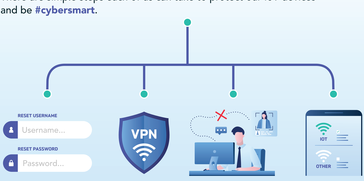
4. The bad actor can now watch you through your camera feed, compromising your physical security.

5. The bad actor can now gain access to other insecure devices, documents, and information on your network.

IoT isn't just about security cameras. IoT includes **smart home systems, refrigerators, lightbulbs, fitness trackers, printers, and more.** IoT devices are being created faster than security is being developed to protect them.[3]

Section 3: What actions can you take to prevent IoT breaches?

There are simple steps each of us can take to protect our IoT devices and be **#cybersmart.**



- Change default credentials to use strong and unique passwords
- Use a trusted VPN on your home network and at work
- Turn off social sharing settings on all of your connected devices
- If possible, use a separate network for your IoT devices

Section 4: What's the cost of no action?

IoT breaches cost more than just money. They can compromise physical security, leak sensitive data, and cause reputational damage.

One IoT breach at KrebsOnSecurity occurred through insecure security cameras causing

7 hrs of website downtime

$323k in energy consumption[4]

48% of IT leaders have experienced an IoT breach.[5]

An IoT breach

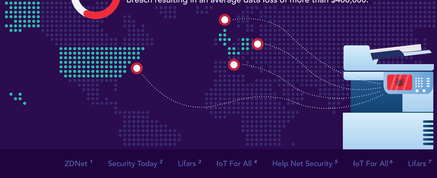
for companies **under**

$5 million in revenue could cost **13%** of annual budget

for companies **above**

$5 million in revenue could lose **10's** of millions of dollars[6]

60% of business in the US, UK, France, and Germany suffered a printer-related IoT breach resulting in an average data loss of more than $400,000.[7]



ZDNet [1] Security Today [2] Lifars [3] IoT For All [4] Help Net Security [5] IoT For All [6] Lifars [7]