BE SAFE ON THE INTERNET

# Content Unit
# [Internet of Things]

*Project: B-SAFE*
*Number: 2018-1CZ01-KA204-048148*
*Name of author:* EDIT VALUE®
*Last processing date:* 02.09.2020

Funded by the
Erasmus+ Programme
of the European Union

*"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein."*

# Internet of Things

## First introduction

Encompassed in the fourth industrial revolution, namely Industrial 4.0, and with a more direct impact to the individual as an end user, is Internet Of Things, commonly known as IoT. The IoT is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that has an ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. The first "official" IoT device was a Coke machine on the campus of Carnegie Mellon University in Pittsburgh, Pennsylvania, in 1982. The students wanted to be able to know in advance if newly loaded cans of soda were at peak coldness, so they rigged the machine to report this information to a computer in a nearby office.

Despite of its age, IoT technology is constantly evolving, thus we are facing disruptive changes related to our habits of living, as there is a myriad of opportunities and possible applications of IoT either in industrial settings or in day-to-day life.

While it provides effective and efficient solutions too many real world problems there are significant challenges regarding security and privacy that must not be ignored.

## Practical relevance – This is what you will need the knowledge and skills for

After learning this content unit, you will know what Internet of Things is and what are the main applications of this new technology.

Additionally, you will learn about the most common issues related to security and privacy of IoT as well as how to react in case of a cyberattack to any of your smart devices.

## Overview of learning objectives and competences

In LO_Internet of Things in everyday life_O1 you will know the most important aspects that describe Internet of Things and the main applications of this technology

In LO_ Internet of Things in everyday life_O2 you will learn what are the main security and privacy risks related to Internet of Things

In LO_ Internet of Things in everyday life_O3 you will be familiarized with some technics to react to security and privacy problems that will come with Internet of Things.

| Learning objectives | Fine objectives |
|---|---|
| LO_Internet of Things in everyday life_O1 | FO_ Internet of Things in every day life_O1_O1: You will learn about the structure of IoT and how it works<br>FO_ Internet of Things in every day life_O1_O2: You will know about the applications of IoT |
| LO_ Internet of Things in everyday life_O2 | FO_ Internet of Things in every day life_O2_O1: You will have access to a brief presentation of security issues of IoT<br>FO_ Internet of Things in every day life_O2_O2: You will have access to a brief presentation of privacy issues of IoT |
| LO_ Internet of Things in everyday life_O3 | FO_ Internet of Things in every day life_O3_O1: You will have access to some recommendations to deal with security and privacy issues within IoT. |

| | |
|---|---|
| | FO_ Internet of Things in every day life_O3_O2: You will have access to a brief presentation of some methods in order to react to a cybersecurity incident. |

# 1.Build knowledge – Internet of Things in everyday life

Over the years there has been a rapid growth in the domain of Internet of Things (IoT) in terms of technology as well as market growth. The networking of computers called as "Internet" revolutionized the way we share the information. The IoT can be considered as next revolution in how we perceive and share the information (Virat, 2018). In the box below you can access a simplified definition of IoT:

Definition

**Internet of Things** is the concept of connecting any device (so long as it has an on/off switch) to the Internet and to other connected devices. The IoT is a **giant network of connected things and people - all of which collect and share data** about the way they are used and about the environment around them.

Devices and objects with built-in sensors are connected to an Internet of Things platform, which integrates data from the different devices and applies analytics to share the most valuable information with applications built to address specific needs. In the figure below you can find two good examples of a IoT technology.

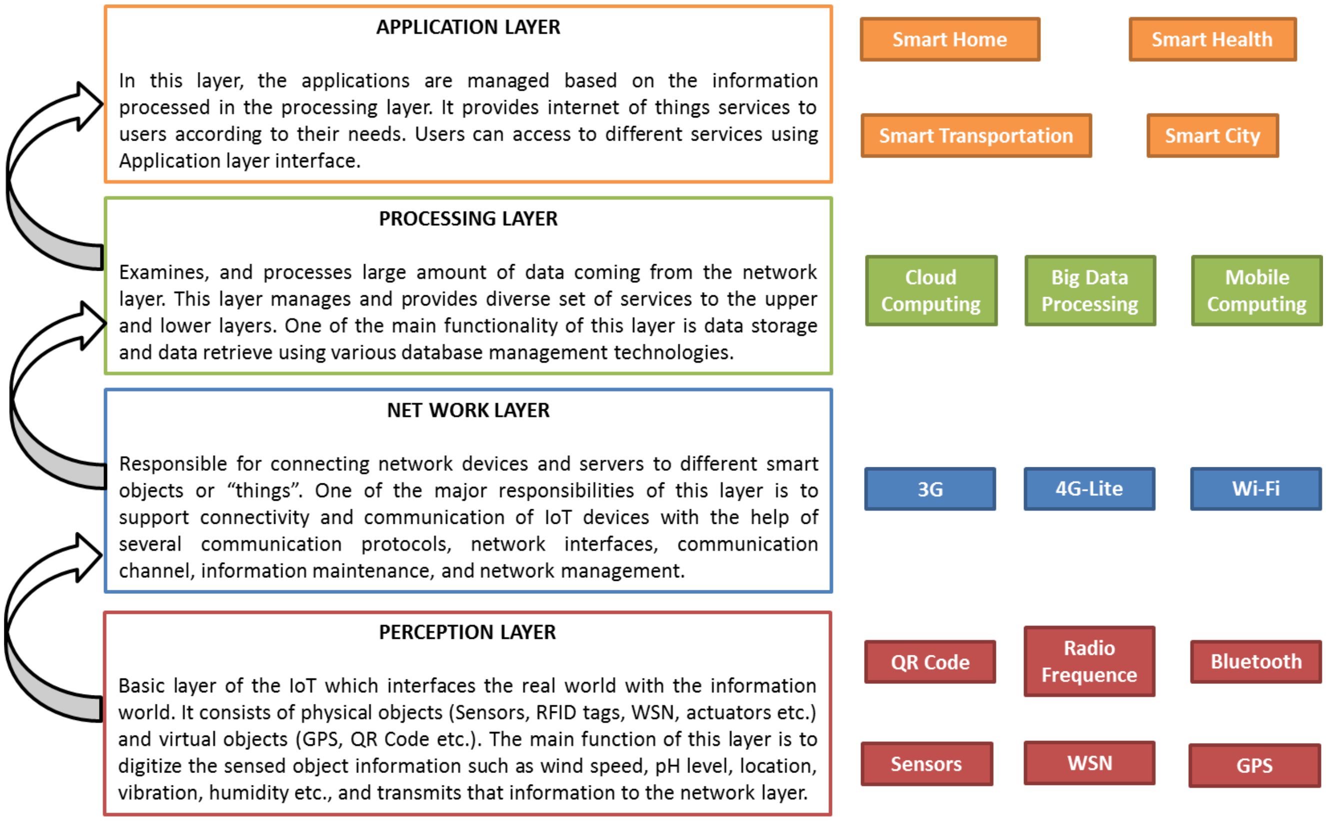
As we have seen before, the IoT is a broad term used to refer to the vast network of internet connected devices that exist today.

The Internet of Things promises to be the most important technological development for consumers since the advent of the smartphone. Experts believe that this technology will eventually generate more than $123 billion in annual revenue by 2021 and the statistics point out that there will be more than 36 billion devices connected to the internet by the end of 2020.

As a matter of fact, major companies, such as Amazon, Goole and Tesla are already working with software development services to produce cutting-edge IoT devices. The IoT is expected to make advanced smart homes a reality. More examples of IoT technologies include **self-driving cars, wearable devices that track body markers, patient adherence to behavioural changes, voice assistants (Alexa for example), intelligent heating systems, etc.**

Because of that, we can easily recognize that the overall society will be in touch with an IoT device at a certain point. Therefore, it is very **important to improve the overall behaviour** of citizens and their privacy/security.

The dynamics, intelligence and mobility of IoT make it a high demand technology but also make the IoT **vulnerable and risky under security and privacy terms**. To understand the complexity of this challenge, you need to comprehend the basic architecture of IoT, characterized by a **dynamic structure**. The number of layers that composes the architecture of IoT diverges immensely between experts, but all of them agree that IoT is composed by at least four layers: **Perception, Network, Processing and Application.**



APPLICATION LAYER

In this layer, the applications are managed based on the information processed in the processing layer. It provides internet of things services to users according to their needs. Users can access to different services using Application layer interface.

Smart Home
Smart Health
Smart Transportation
Smart City

PROCESSING LAYER

Examines, and processes large amount of data coming from the network layer. This layer manages and provides diverse set of services to the upper and lower layers. One of the main functionality of this layer is data storage and data retrieve using various database management technologies.

Cloud Computing
Big Data Processing
Mobile Computing

NET WORK LAYER

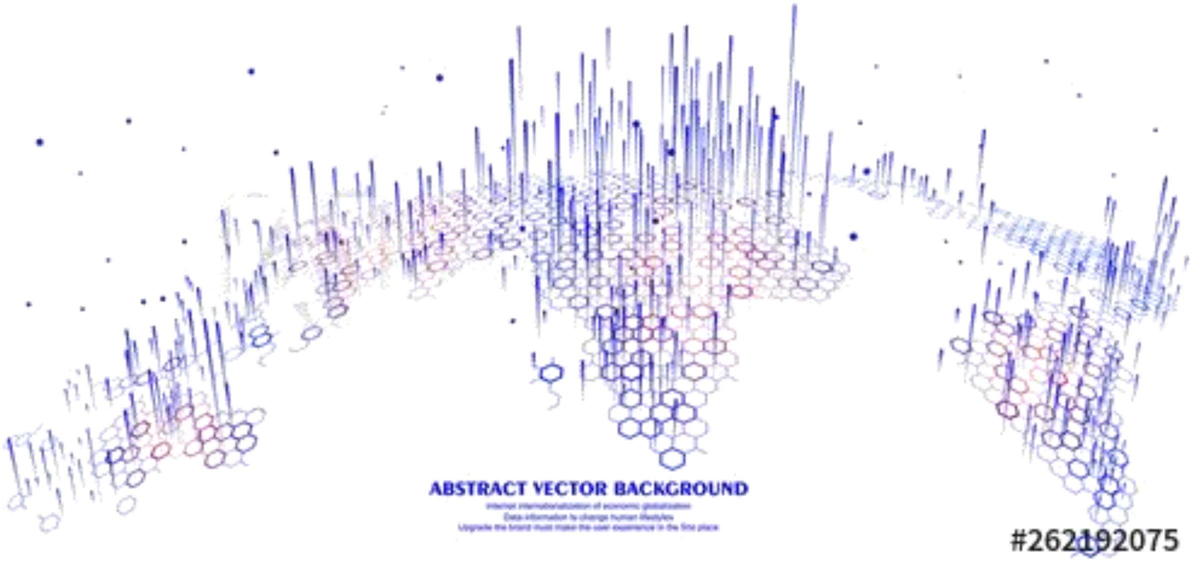
Responsible for connecting network devices and servers to different smart objects or "things". One of the major responsibilities of this layer is to support connectivity and communication of IoT devices with the help of several communication protocols, network interfaces, communication channel, information maintenance, and network management.

3G
4G-Lite
Wi-Fi

PERCEPTION LAYER

Basic layer of the IoT which interfaces the real world with the information world. It consists of physical objects (Sensors, RFID tags, WSN, actuators etc.) and virtual objects (GPS, QR Code etc.). The main function of this layer is to digitize the sensed object information such as wind speed, pH level, location, vibration, humidity etc., and transmits that information to the network layer.

QR Code
Radio Frequence
Bluetooth
Sensors
WSN
GPS



As you can notice, the Application Layer facilitates the global management of the smart applications and provides specific services to the user. In the next table the Top Applications of IoT in day-to-day life are presented:

| | |
|---|---|
| Smart Home | It is an interconnected home where all types of things interact with each other via the Internet.  For example, in a smart home you can switch on air conditioning on your way home or you can activate the washing machine while you are at work. Essentially, everything is interconnected to make your life simpler and convenient. |
| Wearables | These devices (such as Fit Bit) collect data and information about the user that is later pre-processed to extract essential insights. These small, highly efficient gadgets broadly cover fitness, health and entertainment requirements. |
| Smart/Connected Cars | A smart vehicle which is able to optimize its own operation, maintenance as well as comfort of passengers. These vehicles are being used in smart transportation – that includes waterways, railways, roadways, etc. - receiving real time information about roads, accidents, road diversions and closures, in a way that provides the maximum safety to the driver and passengers. |
| Smart Cities | It involves everything that composes a city, like surveillance, transportation, energy management systems, water distribution, urban security and environmental monitoring. For example, the government can automatically be informed about measured pollution levels or shortage of energy supplies, etc. |
| Smart Agriculture | Farmers are using meaningful insights from the data to yield better return on investment. Sensing for soil moisture and nutrients, controlling water usage for plant growth and determining custom fertilizer are some simple uses of IoT. |
| Power Management | Power grids of the future will not only be smart enough but also highly reliable. In smart power grids, the usage of smart meters, home gateways, smart plugs and connected appliances helps in conserving resources and save money for consumers, manufacturers and utility providers. |
| Smart Healthcare | A connected healthcare system and smart medical devices represents a revolution for society, as it has significant impact not just for companies, but also for the well-being of people in general. The application of IoT in healthcare domain, includes obtaining information about health parameters of an individual like blood pressure, body temperature, heart beat measurements etc through ultra-low powered, highly energy efficient and small-sized wearable devices. This information collected can be shared with the respective individuals, and health care centres for further action by doctors. |

# 1.Apply knowledge

## Exercise SINGLE CHOICE

Associated fine objective: FO_ Internet of Things in every day life_O1_O1:

*Situation: What is the "Internet of Things"?*
*Task:* Please identify the right option following the single-choice principle: Only one answer is true.

- IoT is a network of connected servers that are accessed over the internet.
- IoT is digitalization and automation of every part of the company, as well as the manufacturing process.
- IoT is a global wide area network that connects computer systems across the world.
- **IoT is an incipient technology which focus on inter-connection between things or devices to each other and to humans or users to achieve some common goals.**

## Exercise MULTIPLE CHOICE

Associated fine objective: FO_ Internet of Things in every day life_O1_O2:

*Situation: What are the main applications of Internet of Things?*
*Task:* Pick the right options following the multiple-choice principle. None, one, more than one or all options can be true

- **Power-line monitoring and smart grid power transition.**
- **Production supply chain management in retail.**
- **Production supply chain management in transforming industry.**
- **Regulation of water in agriculture.**

# 2.Build knowledge – Internet of Things and security and privacy issues

Smart consumer devices connected to the Internet of Things are constantly collecting personal information from consumers. Therefore, one of the biggest concerns related to the implementation of Internet of Things in our daily lives is linked to the security and privacy of personal and even sensitive personal information, since the theft of personal information can cause serious harm to individuals, businesses and overall society. **IoT is a ubiquitous technology** with a complex architecture and structure. Consequently, it creates **novel security and privacy problems**, hitherto considered harmless or undefined. Those concerns are mainly related to:

1. **IoT technologies have longer lifespan** compared to smartphones and desktop computers.
2. There are **various numbers of manufacturers**, most without traditional information technology (IT) expertise, resulting in interoperability issues and poor security hygiene.
3. **This lack of IT expertise** extends to end users (who are all de facto system administrators).
4. Number of devices and global connectedness exacerbate all issues. In fact, it is estimated that there are 50 billion connected devices at this moment.

Security of data and user's privacy are different concepts but they are not mutually exclusive. Indeed, a security attack or cyberattack, automatically compromises user's privacy.
The challenges that must be overcome to resolve IoT security and privacy issues are immense. This is primarily because of the many constraints attached to the provision of security and privacy in IoT

systems. Nevertheless, in the box below a brief definition of those concepts, applied to IoT, is presented.

The type of security and privacy threats and attacks that IoT is subject to depends on its layers, since each layer has different particularities and associated technologies. In the following table a summary of the most common cyberattacks to IoT framework as well as the degree of impact to the four layers that composes IoT architecture are displayed:

| | Brief description | PERCEPTION LAYER | NETWOR LAYER | PROCESSING LAYER | APPLICATION LAYER |
|---|---|---|---|---|---|
| Malicious code | Any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system | High | High | Low | High |
| DoS attack | Cyberattack in which the perpetrator seeks to make a machine or network resource unavailable | Low | High | High | Low |
| Routing Information | Protocols that routers can use to exchange network topology information | Low | High | High | Low |
| Eavesdropping | Is the act of secretly or stealthily listening to the private conversation or communications of others without their consent | High | Medium | High | Medium |
| Identity theft | Deliberate use of someone else's identity usually as a method to gain a financial advantage or other personal information | High | Medium | High | Medium |
| Sinkhole attack | Threatens the security of WSNs at almost evert layer of their protocol stack | Medium | High | Low | Low |
| Phishing attack | Fraudulent attempt to obtain sensitive information or data typically carried out by email spoofing or instant messaging | Low | Low | Medium | High |

As you can observe, there is a **variety of possible attacks that can compromise IoT devices security and privacy with a different level of impact depending on the layer.** Thus, there are considerable challenges that must be tackles by all parties involved: **IoT manufacture or developer, government and end user.**

# 2.Apply knowledge

## Exercise MULTIPLE CHOICE

Associated fine objective: FO_ Internet of Things in every day life_O2_O1:

*Situation:* Regarding the security of IoT devices and its users, which statements are true?
*Task:* Pick the right options following the multiple-choice principle. None, one, more than one or all options can be true

- Data security is required when data are being generated and stored.

- Security requirements for IoT applications must be applied in three layers: application layer, network layer and perception layer.
- The probability of occurring a phishing attack in an IoT device it's higher is in its processing layer.
- The architecture of IoT allows malicious entities to exploit vulnerabilities intrinsic to each one of the IoT layers.
- A malicious code can affect at least three layers.

## Exercise SINGLE CHOICE

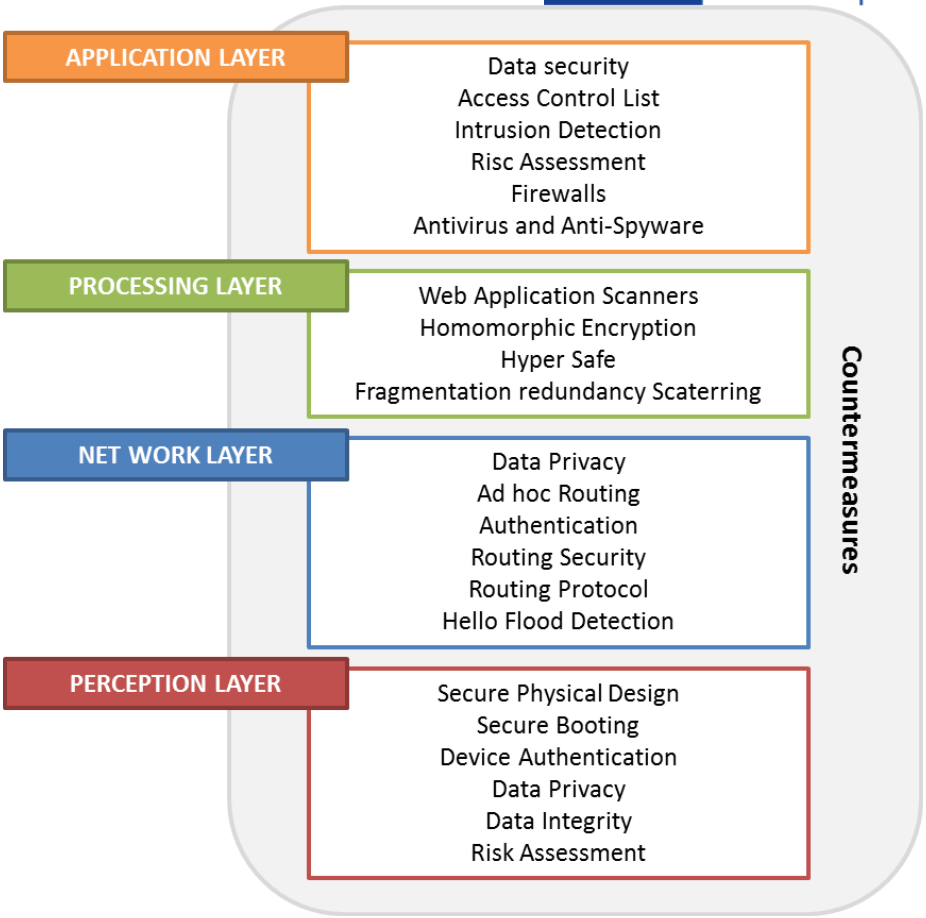
Associated fine objective: FO_ Internet of Things in every day life_O1_O2:

*Situation:* In consideration of IoT user's privacy, which statement is true?
*Task:* Please identify the right option following the single-choice principle: Only one answer is true.

- The significant growth that the IoT has shown during recent years has brought in several privacy concerns as data availability decreases, sponsored by common and usual properties of the IoT.
- Manufactures needs to guarantee the protection of users' personal information associated to their movements, habits and interactions.
- Privacy refers to how well the IoT devices defends against user data being stolen.
- Privacy is only at risk in the application layer.

# 3.Build knowledge – Internet of Things and its users protection

Early in the year of 2019, CNN managed to access a variety of camera feeds using a search engine for IoT devices Shodan. They remotely watched children playing in a middle school gym in Indonesia, a man getting ready for bed in a Moscow apartment, an Australian family coming and going from their garage and a woman feeding her cat in Japan. All of them seemed unaware of the fact they were broadcasting their lives online every second of the day. According to CNN, none of the cameras had had security checks and were open to anyone who knew the right address.
To avoid that this kind of situation happens to you, there are some **technics, procedures and behaviours** that should be **adopted both by the IoT device developer and by the smart device user.** Below you can see some measures to react and to prevent cyberattacks in all the layers that composes IoT devices.



APPLICATION LAYER

Data security
Access Control List
Intrusion Detection
Risc Assessment
Firewalls
Antivirus and Anti-Spyware

PROCESSING LAYER

Web Application Scanners
Homomorphic Encryption
Hyper Safe
Fragmentation redundancy Scaterring

NET WORK LAYER

Data Privacy
Ad hoc Routing
Authentication
Routing Security
Routing Protocol
Hello Flood Detection

PERCEPTION LAYER

Secure Physical Design
Secure Booting
Device Authentication
Data Privacy
Data Integrity
Risk Assessment

Countermeasures

As you can observe most of the privacy and security mechanisms for IoT should be implemented. IoT developers should focus their efforts in the **creation of devices that are physically secured** and protected with cryptographic algorithms, hardened gateway platforms, complex encryption, anti-virus, anti-spyware, anti-adware and advanced and updated security technics. Therefore, the user is dependable of the security mechanism already integrated in the IoT devices to secure their privacy and security. Nevertheless, there are some actions that you, as an IoT consumer, must be aware to overcome various IoT security and privacy threats:

### 1st – Read the security requirements and the privacy policy for the devices

Always choose an IOT device from a trustworthy and transparent manufacturer. You are entitled to know the security technics implemented in the IoT.

As well, you should always **read the privacy policy** of the device as you must be aware of how your IoT device works and the reasons your data are being collected and used by IoT smart devices. Put simply, before using an IoT device, you should be able to know if you can:

1) Access, view and remove the data collected from you via IoT;
2) Disconnect your IoT devices when you want to do so;
3) Consent to your personal data storage on the IoT device.

### 2nd – Stop using the default password!

The first thing you should do with your IoT device is to check if it allows you to **change default passwords.** Always use a strong unique password to each and every device that you own. Don’t forget to change the passwords of your Wi-Fi router as well!

### 3rd – Deactivate remote access (WAN) to the device

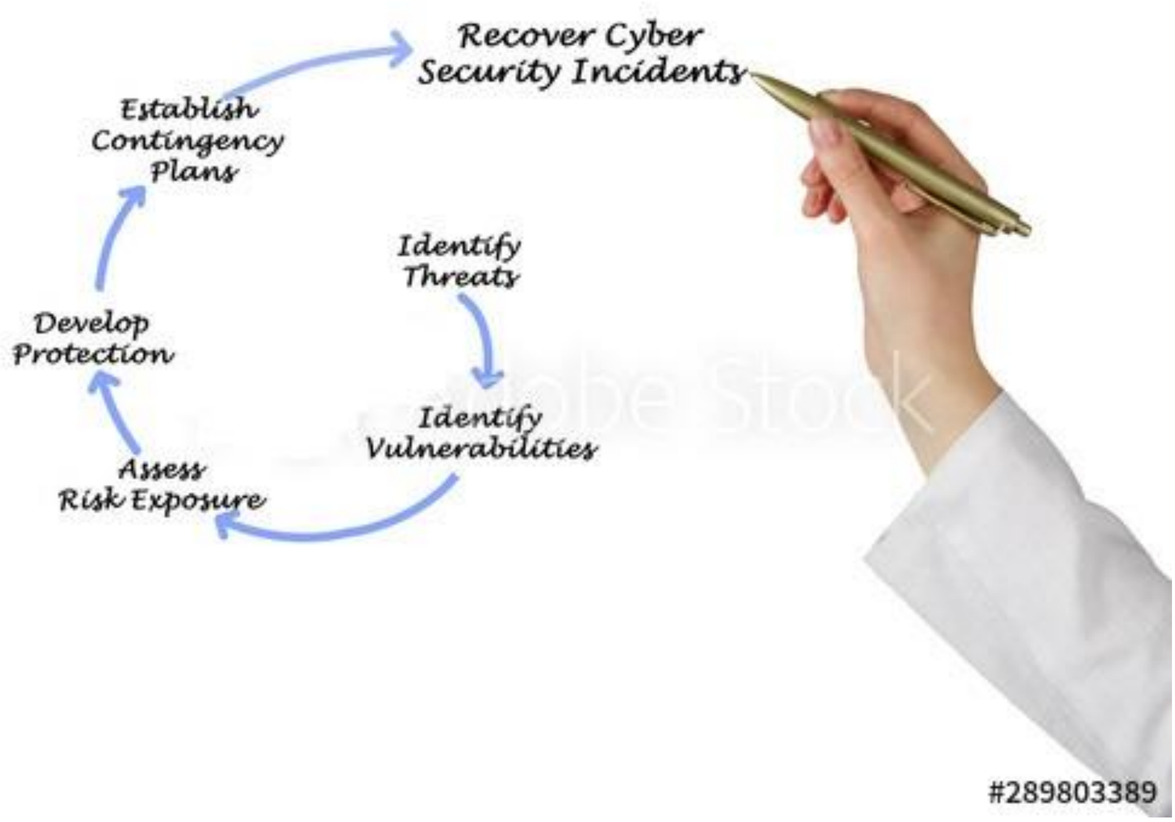
If you are at home right now, google *“what is my IP address” on your computer.* What you see there is your WAN IP address. This address is unique on the Internet at any given time. If you travel away from home, that IP address is what you can use to access your smart home devices remotely. If the devices are not secured, the IP address is all that is necessary for anybody who wants to access them. In fact, that was what CNN used to access a variety of camera feeds!

### 4th – Disable the features that are not used

A trustworthy smart device is a device that allows you to **personalize its features**. For example, if you are not using your smart watch to collect your latest workout data, enable the Bluetooth connection; or if you don't need to record your jog path, enable the GPS and location track.

### 5th – Be a Super-Agent of Cybersecurity!

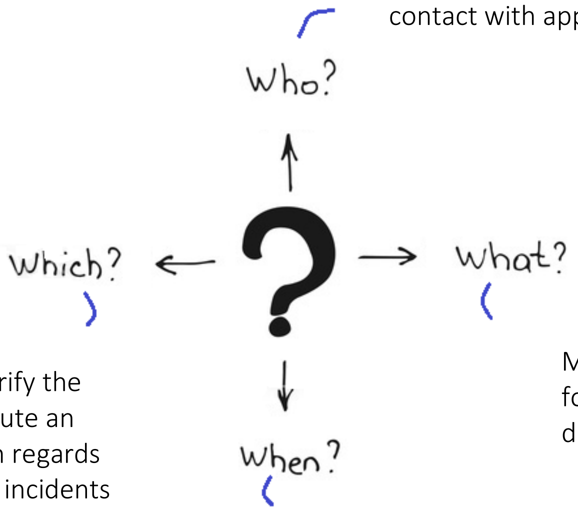
Did you know that 95% of cybersecurity breaches are due to human error? Therefore, **cybersecurity literacy** is the most important way to eliminate cyberattacks. In order to be a Super-Agent of Cybersecurity, you must master all the phases of the **cyber awareness plan:**



Whether you use Internet of Things devices in your daily life, or you are a business owner or manager that uses technology and Internet in day-to-day activities, you must **heighten the chances of catching a security or privacy attack before it is fully enacted**, minimizing damage and reducing the cost of recovery.

By now, you have all the basic knowledge to ace in the identification of threats and vulnerabilities, in the assessment of risk and in the device's protection. But what if, despite all the prevention and carefulness, you are still a victim of a cyberattack incident while using Internet of Things? The answer relies on the **4 W's: Who, What, When and Which.**

Make a list of who to call in case of an incident. It's critical that you know who will make the decision to initiate recovery procedures and who will be the primary contact with appropriate law enforcement personnel.



Your response plan should clarify the types of activities that constitute an information security incident. In regards of an organization, that includes incidents such as your website being down for more than a specified length of time or evidence of information theft.

Make sure you have a plan for what to do with your data in case of an incident. This may include shutting down and rebooting your entire IoT systems.

Determine when to alert emergency personnel, cybersecurity professionals, service providers or insurance providers.

Don't forget to involve your family, friends and/or employees in the cyber awareness plan, as cybersecurity is a responsibility of every IoT user!

# 3.Apply knowledge

## Exercise MULTIPLE CHOICE

Associated fine objective: FO_ Internet of Things in every day life_O3_O1:

*Situation:* Which security measures should you implement as to prevent cyberattacks in your IoT devices?

*Task:* Pick the right options following the multiple-choice principle. None, one, more than one or all options can be true

a) Install homomorphic encryption.
b) Install firewalls.
c) Create fragmentation redundancy scattering.
d) Change default passwords of router.
e) Disable features in my smart device that are not being used.
f) Deactivate remote access to the smart device.

## Exercise MULTIPLE CHOICE

Associated fine objective: FO_ Internet of Things in every day life_O3_O2:

*Situation:* To become a Super Agent of Cybersecurity, what should you do?

*Task:* Pick the right options following the multiple-choice principle. None, one, more than one or all options can be true

g) Learn how to program in order to encrypt IoT devices.

h) Establish a contingent plan following the 4 W's: "What is being generated?", "Where are data stored?", "When are data used?", and "With whom are data shared?"

**i) Establish a contingent plan following the 4 W's: "Who to call?" "What is my course of action?", "When to alert others?", and "Which activities are incidents?"**

**j) Involve all my family, peers and employees in the cybersecurity awareness.**

k) Develop the incidence response plan only after suffering a security breech, as is the only way to know the right actions for the incidents still to come.

# Sources

Analytics Vidhya (August 26, 2016). *10 Real World Applications of Internet of Things (IoT) – Explained in Videos.* Retrievd from https://www.analyticsvidhya.com/blog/2016/08/10-youtube-videos-explaining-the-real-world-applications-of-internet-of-things-iot/

Clark, J. (November 17, 2016*). What is the Internet of Things (IoT)?* Retrieved from https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/

Evans, D. (2011). *The internet of things how the next evolution of the internet is changing everything.* Cisco White Paper, 1–11. Retrieved from

https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Griffiths, J. (February 2, 2019). *'Internet of things' or 'vulnerability of everything'? Japan will hack its own citizens to find out.* Retrived from https://edition.cnn.com/2019/02/01/asia/japan-hacking-cybersecurity-iot-intl

Kelbert, J. (September 24, 2019). *5 Interesting Facts About the IoT.* Retrieved from https://blog.flexis.com/5-interesting-facts-about-the-internet-of-things-iot

Mena, D. M., Papapanagiotou, I. and Yang, B. (2018) *Internet of things: Survey on security.* Information Security Journal: A Global Perspective, 27:3, 162-182, DOI: 10.1080/19393555.2018.1458258

Finance Monthly (September 5, 2019). *The Worst And Weirdest IoT Hacks Of All Times.* Retrived from https://www.finance-monthly.com/2019/09/the-worst-and-weirdest-iot-hacks-of-all-times/

Ngo, D. (December 22, 2015). *Home networking explained, part 9: Access your home computer remotely.* Retrieved from https://www.cnet.com/how-to/home-networking-explained-part-9-access-your-home-computer-remotely/

Oorschot, P. C and Smoth, S. W. (2019). *The Internet of Things: Security Challenges.* IEEE Security and Privacy Magazine, 17(5):7-9. DOI: 10.1109/MSEC.2019.2925918

Spencer, T. (August 8, 2019). *How to Respond to a Cyber Attack.* Retrived from https://www.industryweek.com/sponsored/article/22028042/how-to-respond-to-a-cyber-attack

Viriat, M. S. et al. (2018). *Security and Privacy Challenges in Internet ofn Things*. Proceedings of the 2nd International Conference on Trends in Electronics and Informatics. IEEE Conference Record: # 42666; IEEE Xplore ISBN:978-1-5386-3570-4

Images

https://innovationatwork.ieee.org/low-power-low-latency-healthcare-iot/
https://messinaconstruction.com/smart-homes/smart-home-technology

# Save Knowledge

**Internet of Things**, or simply IoT, is a *buzzword* these days. The IoT will undoubtedly change the way that individuals interact with the world and technology around them. This **network of internet-connected devices** will have many positive impacts.

IoT represents a revolution in the way we interact with each other. As a matter of fact, IoT created new kinds of interaction, as it is a **technology that allows the connection between things, processes, people, animals and almost everything that we see around, by using Internet.**

Despite being a simple concept, IoT needs an **elaborate architecture** to properly function. IoT architecture is made at least of **four layers**, namely, perception layer, network layer, processing layer and application layer. It is in this last layer that we have the perception of utility of IoT, as it represents smart applications and smart devices that could be used in many fields, making them "smarter": smart homes, smart agriculture, smart cities, smart healthcare, and many others.

The dynamics, intelligence, and mobility of IoT make it a high-demand technology but also makes the **IoT vulnerable and risky under security and privacy terms**. All the layers of IoT are subjected to different cyberattacks. Therefore, **smart devices designers must actively participate in the development of effective security and privacy measures**, thus making IoT more robust in terms of security.

Nonetheless, the leading cause of IoT vulnerability is the **lack of security awareness**. People, businesses and society overall must **engage in the enhancement of cybersecurity literacy** in order to eliminate the number one cause of cybersecurity breaches: human error.

**Always remember, be a Super Agent of Cybersecurity!**