Cyber security and awareness in IoT devices

ACIT4100 - Autumn 2022

Figure 1 IoT device Security (Williams, 2022)

Table of Contents

1 Introduction

Mr. Alex has an inclination towards technology and always wants to use the latest technologies available in the market. This has led him to stay in a smart house where almost all the items are automated and connected to the internet. In his bedroom, the Lutron electric shades would automatically open to enter the shining sunlight and fresh air from the outside environment, when the alarm clock tips up at 7 in the morning. The smart wristwatch that he wears, generates a mild vibration for his wake-up process along with that it measures his heartbeat rates, anxiety levels, and oxygen levels in the blood. The automatic motion sensor triggers the lights on with recommended density along with an auto-generated message send to the thermostat and geyser for hot water. Virtual assistants (Alexa) give a reminder about the meeting scheduled for the day and play some gentle music to start the day with a refreshing coffee and healthy breakfast.

Before leaving for the office, the motion detector switches off the lights for the unused rooms. A smart security door lock system closes the doors and windows. An auto-connected car unlocks with fingerprints of Mr. Alex on its door lock. Once his smartphone and car's Wi-Fi are connected to the same network, automatically it finds the shortest route for his office and checks the condition of the tires, brakes, accelerators, and available fuels. Predefined software notification would be sent to the family members in case any accident occurs. His smart cell phone would get notifications in case of any water leakage, smoke/fire hazards, or some vandalism of his personal properties through the automatic sensors and CCTV camera.

Once he returns from his office, the garage door lock opens through the image sensor, and the main door opens with his fingerprints. Room sensors lights up the living room with enlightening colors, the smart TV is to be automatically switched-on with his preferred channel and the coffee maker has already made a refreshing coffee for him. Haven't these smart devices made the life of Mr. Alex efficient and comfortable? Mr. Alex is living like a king where the Physical devices are providing uninterrupted assistance to him.

Figure 2 Smart House (Knowles, 2022)

However, on one fine day when Mr. Alex just woke up with a strong vibration from his smart wristband, the measurement of his blood pressure was recorded as too high, and immediately some autogenerated message has sent to his doctors on basis of his suspicious medical reports. Mr. Alex could feel that all his smart devices are behaving abnormally like his windows and doors were opening automatically, and all his sensor lights are blinking at the same time along with that his smartphone, personal laptop, and other gadgets got completely encrypted with a pop-up message as "Your system has been hacked by us. Transfer 1 million USD worth of Bitcoin under the below account number else, your personal data would have compromised over public platform".

Yes, that sounds scary. Mr. Alex's smart home has become a spy home for him. All his private moments, official work details, and other sensitive information were breached. His house becomes vulnerable. No one would prefer to live in such a house where every action is being monitored with no privacy. After the police's cyber investigation, it was found that Mr. Alex has forgotten to switch off his Smart coffee machine (IoT device) which was hacked by cybercriminals using the IoT device's Bluetooth ID. The hackers used these innovative techniques to hack his coffee machine by connecting their Bluetooth device with the coffee machine. They did reverse engineering to get his home Wi-Fi user credentials with which all his smart devices have connected. After this, they were able to send their suspicious malware to all the smart devices present in that smart home.

Here the question arises, was this vulnerability happen only because of the fault of Mr. Alex or there were other factors as well that have not been considered? What about the product manufacturers who haven't made the IoT device fully secure? or the alarm sensor systems that haven't sent any alerts to Mr. Alex on an unauthorized connection to his home Wi-Fi system.

Security and IoT (Internet of things) devices are always found in the same place. Unfortunately, no device is safe until it is fully designed and tested as secure. Let's snorkel down into the ingenious inventions in technology by humans as IoT devices, their internet connectivity along with their exponential popularity among us.

2 Chronology of IoT devices

The emergence of the indigenous internet system has made the world connect with each other profoundly. Initially, the Internet was considered one of the luxury items used by professionals, executives, and big organizations for internal and external connectivity like mail access, information sharing, and virtual connectivity over some social media platforms like Facebook, and Orkut. Subsequently, with the progression of time, it became a necessity where people couldn't survive a single minute without internet connectivity. After a certain period, smartphones were able to connect internet as well as able to replace multiple electronic gadgets like calculators, high-definition cameras, radios, etc. Scientists thought similar inventions can be more helpful to technological progression. The invention of smart gadgets which can be connected through the internet has given a wide range of comfort to human beings. (Sachchidanand Singh, 2015)

Humans have five different sense organs. They use these abilities to interact with other human beings and share their experiences. When smart physical devices have added the ability to collect data, analyze, interact, and collaborate with other things connected over the internet, they are termed as Internet of things [IoT] (Hougland, 2016). The first IoT device was created by John Romkey in 1990. It was a toaster that could operate through the TCP/IP protocol with the Internet. (Vardomatski, 2018). When the count of physical machines or things connected to the internet surpassed the count of human beings connected over the internet, the term Internet of Things (IoT) draws the attention of everyone. Innovators and Researchers thought instead of humans collecting data or instructing these physical devices individually, these devices can be connected to each other through the internet where they can collect and share data, validate the collected inputs, and react as per the expected results with limited human interventions. These smart features can be a spectacular contribution to the human race moving forward. Now, a single fingertip can clean your house, switch on your lights as per your mood, provide details visualization of your child’s movement when you are not at home, prepare your coffee, and can assist you with many other activities. (Sánchez López, 2011)

IoT devices have had an enormous effect globally with quick dissemination worldwide. The Internet has provided a plethora of data across each corner of the world which has been helping users to get the obligatory information with a single click of their fingertips. These devices may be household products like (Auto Cleaning Robots, Temperature sensor, or fitness wrist watches), Assisted livings for elderly people, supply chain management systems used in the industries like (real-time data for logistics operators, sensors used for monitoring the fire alarm, or continuous supervision to elevate the production efficiency) (Legchekov, 2022) (NZ Jhanjhi, 2020)

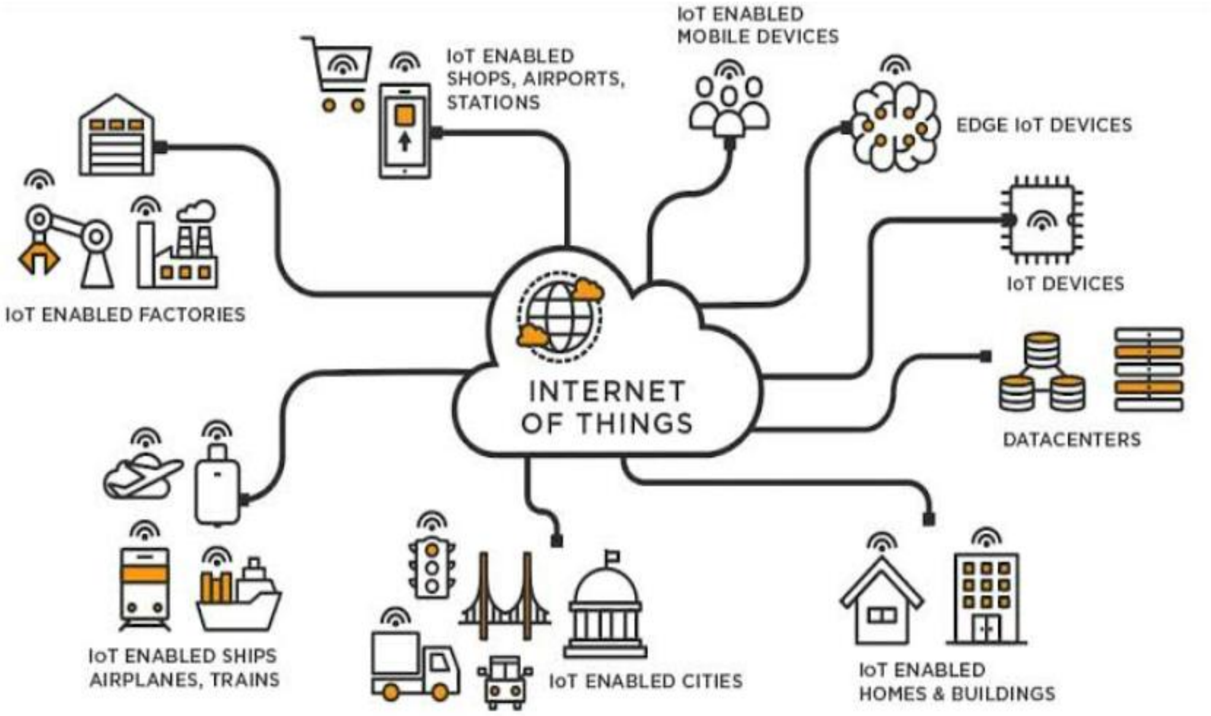
IoT ENABLED MOBILE DEVICES
IoT ENABLED SHOPS, AIRPORTS, STATIONS
EDGE IoT DEVICES
IoT ENABLED FACTORIES
IoT DEVICES
INTERNET OF THINGS
DATACENTERS
IoT ENABLED SHIPS AIRPLANES, TRAINS
IoT ENABLED CITIES
IoT ENABLED HOMES & BUILDINGS

Figure 3 IoT devices Implementations in various sectors (Securing-Internet-of-Things, 2022)

2.1 Examples of IoT devices

IoT devices are omnipresent in almost all sectors now a days. It can be at Data centres, Factories, e-commerce platforms, Transportation system etc. [refer to figure - 3]

2.1.1 IoT-enabled home & buildings

Smart home devices would turn your home into a palace with the most accurate instruction to be followed up. Vacuuming, security systems like door locks, sensors used to prevent water leakage, smoke detectors, managing the density of lights, and efficient usage of electricity and water. (Jagpreet Kaur, 2021)

2.1.2 IoT-enabled industries

Industries like supply chain management have multiple stages to get orders from end users till delivering satisfactory services. Smart IoT devices made it simple and easy. It involves collecting accurate data for the materials required for expected productions, and existing raw materials' efficient usage. Furthermore, collecting customer orders to provide them with the exact status of their deliverables as well as identifying the bottlenecks and visibility and accuracy of the warehouses. These IoT devices can be used in medical sectors (IoMT), airports, smart cites, weather forecast systems, and automobiles. (NZ Jhanjhi, 2020)

2.2 Basic design of IoT devices

In the IoT ecosystem, devices start communicating with each other by recognizing the other device's IP address. It is possible that different devices may be connected to different networks. However, they should connect to the internet so that they can send and receive the pieces of information from other IoT devices. (Sachchidanand Singh, 2015)

As per the survey (Zhang, 2017), we can divide the IoT infrastructure design into three categories as User Interaction, Delegate/Relay, and Actuator/sensor. Firstly, the user Interaction point works when the user would instruct the IoT devices, and it receives a response from them like Amazon Echo get voice instruction from the physical user and send it to other IoT device. Secondly, the delegated part will be responsible for getting the response from the user and helping them to compute the logic developed by the application designers. Finally, the actuator will act as per logic execution. For example, when the voice requests come to play Rock music, the actuator would play them for the user. We can get the pictorial view below.[figure - 4]

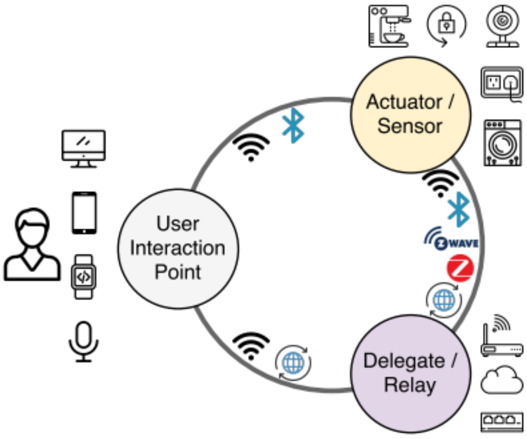

Figure 4 Infrastructure of IoT ecosystem (Zhang, 2017)

As IoT technology advances, Cloud computing provides strong support to it. After the implementation of the cloud in this field, storing, analysing, comparing, and interpreting the data collected from the IoT devices to become so easy and cheaper as compared to the previous days. This will result in billions of new IoT devices connect to the IoT ecosystem which is predicted to be 22 billion in count by 2025. (Oracle, 2022)

2.3 Popularity of IoT devices

Humanity's race has been always towards innovations and creativity. IoT devices have exponentially gained a presence in each and everyone's life. There are multiple factors that have made them available in every house [Table-1]. It is so user-friendly that, even people having physical disabilities could use them smoothly. (Sachchidanand Singh, 2015)

Features	Descriptions	Real life Implementations
Interconnectivity	IoT devices are interconnected to each other which provides a facility for people to connect, view, and instruct other IoT devices.	With a single click, we can check the webcam of our front door on our smartphone screen which would be connected to the smart web camera over the Internet. Accessibility features are also available on the devices.
Smart Sensing	Smart Sensing features would provide automatic functions without any human interference.	A smart alarm system would prompt us on any hazardous conditions like the breakage of waterpipes, fire, or any security-related outbreak.
Intelligence	IoT devices are designed with intelligence and efficiency which would make its user's life more comfortable.	The smart fitness wristwatch would monitor their sleeping cycles, running steps, calories burnt, and blood pressure metrics.
Efficient Energy Saver	One IoT device can replace multiple electronic systems with its effective design and energy efficiency.	Smartphones are replacing calculators, radios, cameras, and other electronic devices. Sensor-driven equipment would turn on and off the lights. These would save lots of energy and efficiently reduce electronic waste.
Assistance like a friend	Voice-controlled IoT devices lets you use the voice commands to search new things from internet, play music and recommend ideas like a friend.	Examples like Alexa, Siri, or Google home voice control would respond like human beings and provide all required pieces of information as requested.

Table 1 IoT device basic features (Sachchidanand Singh, 2015)

2.4 IoT device vulnerabilities

The evolution of IoT devices is a precious gift to humanity. We give all access to these IoT devices to store, transfer and share our personal data with other IoT devices. This will help us to monitor and instruct them with a single touch. However, vulnerabilities to these devices can bring misery to our life. Cybercriminals could steal all our data which is stored in these devices by hacking them. A data breach could follow any human being for the rest of his/her life. Sensitive information like driving license, passport number, home address, or past records can be used for creating fake bank accounts, applying for new credit cards, and other criminal activities. (PhillipWilliams, August 2022)

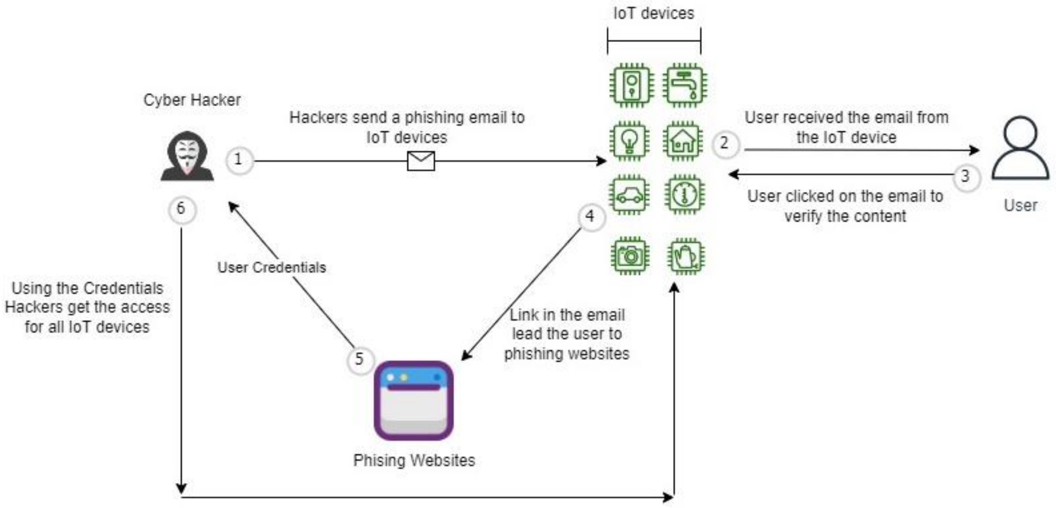
IoT devices
Cyber Hacker
Hackers send a phishing email to IoT devices
User received the email from the IoT device
User clicked on the email to verify the content
User
1
2
3
4
5
6
User Credentials
Using the Credentials Hackers get the access for all IoT devices
Link in the email lead the user to phishing websites
Phising Websites

Figure 5 Phishing Techniques (Waqas Ahmad, 2022)

Technology has given enough edge to cyber criminals to hack any device using various techniques. A simple mail, text message, or even a missed call can contain the phishing link/malware software which can hack your IoT devices in a couple of minutes [figure -5]. Free Wi-Fi connection, open Bluetooth devices can be useful options for hackers. As per research, it is estimated that IoT devices vulnerabilities, using in the industries are categorized into three different segments. Physical layer, Network layer, and application Layer. (NZ Jhanjhi, 2020)

The Graphical view will help to understand their presence(in %age) in different segments. [figure 6]

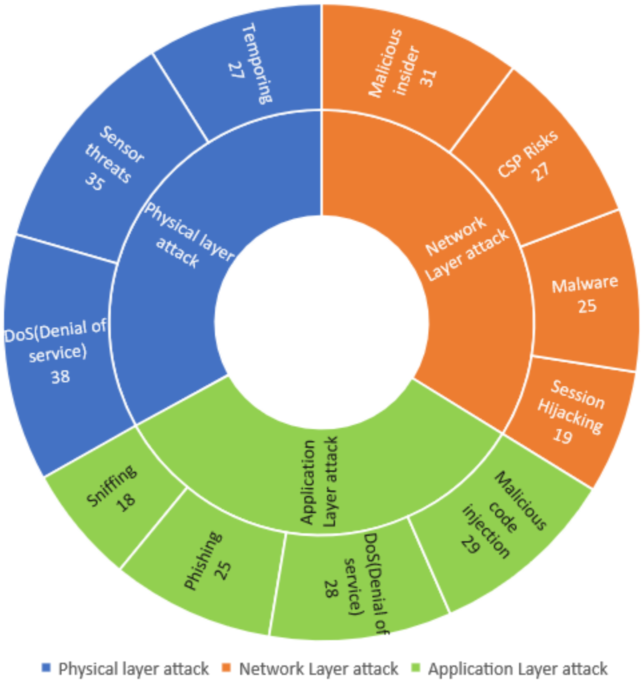

Figure 6 IIOT Cyber-attack categories in different layers %age distribution (NZ Jhanjhi, 2020)

We can save our data from being breached by following some simple set of precautionary actions like updating our devices regularly, Using VPN connections, trustworthy antivirus on our devices, and regularly changing our user credentials. (Abdur Razzaq, 2017)

We will discuss them in detail in the upcoming segments before that we will try to understand how do hackers think? how do they find their targets ? and execute the pitfalls in the systems.

3 Psychology of cyber criminals

IoT devices and smart robots are made by humans to make their lives more efficient, resilient, and convenient. Practically, we can say, what we instruct the machines they will follow the same without any failure. There is a very minimal chance that the IoT devices might be doing the wrong work that they have been designed to do. So basically, We humans are solely responsible for the activities that these devices are doing. In the era of cyberwar, smart gadgets play the role of weapons whereas, victims and hackers are targets and culprits respectively. Future battles are not only fought with machine guns or missiles but also with megabytes and malware software. It indicates that cybersecurity is neither a machinery problem nor an IT-related obstacle. Malfunctions of the IoT devices or network failure are just some excuses that portray as it a systematic issue. It is occurring continuously because of the greediness of some people. (Espinosa, 2018)

Cybersecurity is a psychological issue for people who believe they can do scams with other naive people for easy income. Lack of awareness and carelessness plays a vital role in such cases. On the other hand, people who believe there is no need to follow the rules and policies of cyber security are the easy targets for cyber hackers. In the Security triangle (Human, Machine, and Policies), Humans are considered the most fragile elements. "*More than 90% of cyber breaches are happening because of Human Error*" – said by Mark T. Hofmann. Guidelines and policies are made to provide a secure environment to human beings which would never fail, if they would be followed as predefined. (Sunil Chaudhary, 2022)

Before we move to cyber security, we must have a brief idea of cyber criminals' attitudes, behaviors, thinking perspectives, and identification of their targets. Criminals committing a crime with a perfect plan and hegemony. Whereas they still leave some clues unintentionally which later help the cops to reach out to them. Similarly, in the computational world, everyone is having their own digital footprint. When hackers do scams to their preferred targets, they leave a digital impression. This digital footprint would help us to understand the personality, attitude, and psychology of a hacker. Let us have a small deep down into those in the below paragraphs. (Mark T. Hoffmann , 2021)

When the word cyber hacker/criminal/spy is coined, what type of perception or image is created in our brain? Is that like a bunch of binary numbers on the screen entitled with a person without showing his/her face, hands on the laptop wearing a hoody? Yes, the description sounds a bit cinematic. However, the actual reality is not at all the same. Most of the cybercrimes have been executed by perfectly trained professionals under a systematic and chronological management system. They have a normal office culture, Quality management system, helpdesk facilities, and supply chain. Yes, you have read all these above correctly. It is called “CRIME AS SERVICE”. They have their own customers. For example, suppose you are owning a company that provides service for e-commerce mobile and web portal applications. Your business can grow 4 times faster if you can just make your competitor’s application blackout only for 30 minutes by paying only 200 $ USD / month to these companies. Yes, there are many options available, and big business tycoons have been using them already. “Pegasus” spyware is the best real-life example of these types of scenarios. (Mark T. Hoffmann , 2021)

Here the question arises, why do they engage in such criminal activities? Chances of getting caught might end up with them being behind the bars, their social dignity would harm, and their families might suffer these consequences. Then what motivates them to take a dive into the scamming pool?

They are hacking various technical and non-technical people as well as organizations, which shows their IQ level must be more than an average human being with specific manipulation techniques. The answers might blow our minds. These are all about their sick mentality, a psychological belief of feeling superior, easy source of income, and exploiting the lack of awareness among the victims. Cybercriminals want to prove that they are smarter than the current systems and IoT devices. Their challenge is to beat the human brain with various new techniques for continuous fun, financial gain, and espionage. Ego is considered one of the self-detrimental emotions that can damage a person internally. However, we shouldn't underestimate that in the case of cyber warfare. There is a sense of self-satisfaction after scamming people, publishing their sensitive details on public platforms or darknet websites, manipulating the images and voice using AI techniques to defame the person's social status, and making the big tech companies crumble down to their knees. (Mark T. Hoffmann , 2021)

4 Cyber vulnerabilities related to human psychology

There are plenty of methods that cybercriminals use to put their targets into their planned trap. However, we will discuss the methods which are frequently used to tackle human psychology and emotions to reach their IoT devices.

4.1 Monitoring regular activities of people

"Amateurs hack the system, professionals hack people" – Lines by Bruce Schneier

Mr. Alex was forgetting to switch off his IoT device (Coffee machine) regularly and these activities were continuously monitored by the hackers. They could see the Bluetooth-ID was always open. They knew exactly at what time Mr. Alex were leaving his house, and how much time would they get to malfunction his IoT device. That was the key factor in the hacking process.

In the cyber world, the hacker's prime motive is to play psychologically with the victims, gain their trust, put them in panic mode, and mentally manipulate them to share their user credentials or sensitive information on compromised platform. This will lead to jeopardize their own security firewall. (Mark T. Hoffmann , 2021)

4.2 Creating illusions

The human brain has the ability to think critically as well as decision-making capacity in different emotional situations. However, if someone will psychologically manipulate them then there is a possibility that hacking can be done through this manipulation process. Hackers will use the technique called "*An illusion inside another illusion*". They will use phishing techniques with their targets. For example, you will get a message over your Smart Phone that "Your bank account will be deactivated today", or "You have owned a mega lottery of Millions of dollars". To make you believe in themself, they must have done perfect homework. They will collect some of your information which you might have shared recently with the newly opened coffee shop for a free coffee, like your name, date of birth, and residential address. Then they will send phishing emails to 100 people. Maybe 90 people will ignore that however, 10 people will look into the information and 2 must click on their phishing link for attractive offers. Yes, even a 2% success rate is enough for them. (Krzysztof Cabaj, 2018)

This is what happened with Mr. Alex. He had never realized that his entire Smart house was being hacked till the hackers got all the required sensitive information from his IoT devices.

4.3 Trapping emotions

Cyber hackers know how to play with human emotions. They will use the exact logo, symbols, the same structure of writing, name of the private or government authorities to convince you that the email or SMS which you are reading is authentic. This is called clone phishing in technical terms. Victims find the *authoritarian impact* inside the fraud details sent by the cyber-criminals, and they got trapped. They could hack any IoT devices and send the infected SMS or instructions to other devices so that the complete network can be under their control. (Mark T. Hoffmann , 2021)

4.4 Gaining trust

As social animals, we do trust and believe the information that we read or listen to. Affection, Attention, Sympathy, and Love are some emotional features that give us positive vibes. There is an interesting fact that "*When we touch our tongue with our leftmost upper teeth, we can't breathe through our nose*" Yes, this is one of the biologically correct facts. (Mark T. Hoffmann , 2021) After reading this, I am sure you might be tried doing this activity. This is called TRUST.

We believe in what we read, what we see, and what we hear. But in this advanced cyber world, this might put us in trouble. Cyber hackers use this option. They will first make you fall into their trap by using your trust. You might think there is hardly a chance that there is any kind of potential threat to you. Their behavior and sympathy enforce you to share all your sensitive information of yours with them and then you will be trapped. (Mark T. Hoffmann , 2021)

4.5 Freebies hooks

There is a feeing to have cherry over the ice cream when we get some free bees from anywhere. Suppose you went to a food store for your snacks. There, while enjoying your burger, you find that the store provides free Wi-Fi service. What will strike your brain, let's watch some music videos for free or download some songs from the internet. This is where we might get trapped by hackers. Who knows if the WI-FI that we are connected to, is broadcasted by the hackers who might be near the shop using his/her router? Once the victim is connected to their network, they will get all the privileges to access their images, browsing history, notes, and passwords saved in the browsers. Cybercriminals uses *Freebies techniques* to hook their victims. (Krzysztof Cabaj, 2018)

5 Ethical point of view

We have discussed the importance of IoT devices in our daily lifestyle, and our dependency on them for current living standards. However, if these devices would get compromised, then all the sensitive data would be handed over to the wrong person or on the public platform. It is creating a dilemma. There are many questions that would pop up when we start thinking about it ethically.

Here the first question comes into the picture, should we trust these IoT devices and provide all required privileges to our personal data as Mr. Alex has given? Most of the smart devices, web, and mobile applications asks for all required permissions when we start using them. Are they safe? Do they really need those details to provide us with smart services?

The next question recalls us about responsibility. When the IoT device venerability happened with Mr. Alex, is that his only responsibility to take precautions to avoid such circumstances? What about the responsibilities of manufacturers of those IoT devices? Don’t they have the responsibility to provide in-build security features in those IoT devices? The way food quality assurance is provided by the food safety authority in Finland is by a specific Evira sign [figure - 7], where the consumers only checks that particular sign over the food package with the date of expiry. These details are enough for them to trust the food quality.

Evira
Elintarviketurvallisuusvirasto
Livsmedelssäkerhetsverket
Finnish Food Safety Authority

Figure 7 Finnish food safety Authority (Evira)

Similarly in Norway, for environment-friendly products, the government has introduced a Nordic ecolabel (known as a Nordic swan) [Figure - 8]. These would help the consumers to have exact information about the products. Why can't manufactures implement the same features on IoT devices? Why can't they provide full assurance on their designed product related to security breach?

Figure 8 Sign of Nordic ecolabel (Nordic-ecolable)

When the developer of these IoT devices planned to design the product, do they really give priority to their security features? If not, then why? if they could design smart devices in large volumes then adding their security features won't take more effort for them. What is making them release the product in the market without security features? Is that the pressure from the delivery team to finish the task soon? or from the higher management who doesn't give emphasis on security traits while planning the end-to-end process? (Zhang, 2017)

Do the customers really check these security features when purchasing any IoT devices? Do they know the seriousness of their personal data breach cost? If customers would start giving priority to security features, then the competition among the manufacturers would start exponentially for providing better security features in their IoT products. This would place us in a safer environment.

Why can’t there be similar international laws made for all countries related to the data security of IoT devices? Manufacturers need to provide mandate security features that would be tested and verified by some special trustworthy agencies before it lands on the market for end-user usage. Data insurance should be given to the consumers and the consumers would be given compensation amount on the loss of their data, if the data breach happened due to a fault in the IoT device’s security features. When all the countries would start working together against cybercriminals then there won’t be any safer place for the cybercriminals.

Some businesses intentionally hire professionals to break the IoT device networks of their competitors. Do you really believe that only installing the antivirus for $150/month can save you and your IoT devices from cyber hackers? Here someone may say, as we are paying the price, so we shouldn’t worry about the security protocols and policies. However, just imagine if the user will not follow any security guidelines and expose all his/her user details to the outside world, then it would be an open invitation for the scammers to hack your smart devices. (Mark T. Hoffmann , 2021)

So, it is the responsibility of both service providers as well as service consumers of IoT devices to give importance to security protocols and awareness features. A small gaffe can lead you into a never-ending data trap which would cost you psychologically, emotionally as well as financially.

Some research papers have mentioned various recommendations for security awareness for IoT devices. Let’s just explore them in the below segments.

6 Cyber security awareness in IoT devices as per various studies

IoT devices have made our life more comfortable. However, there are always two sides to the same coin, these precious technologies have also given a perfect platform for the falsity of people to gimmick users in their cyber trap. Here the relevant question emerges why can't we aware the users of IoT devices, before they face the grim reality of cyber hacking with their beloved IoT devices? (Krzysztof Cabaj, 2018)

As per the data research, it has been found that the behaviors and responses of the users are directly linked to cybercrimes which implies that people are the weakest link in the basic triad rule of cybersecurity (People-Process-Technology). It is very straightforward to make rules of the technology and process which are strenuous to break as they are pieces of machinery. However, we need to discipline human resources regarding the modernized tricks of cyber awareness. Cyber awareness should not be just an optional process, but also mutate things into regular practice. This is a continuous process that would improvise with iterative effect and continuous improvement. Technology has been evolving so rapidly, that the cyber threat is a real jitter for every IoT consumer. To meet real expectations, it is required to review and evaluate the critical indicators like expected future planning, new technical updates, and uninterrupted brainstorming that need to be done by the cyber experts. (Sunil Chaudhary, 2022)

It has been observed that many IT firms, Banking domains, and several other industrial and non-industrial sectors that are profoundly using IoT devices. They have introduced these cyber awareness programs in their curriculums as major fundamentals. However, Is that sufficient to just attend some conferences or to give quizzes on these topics? It is not just the audience who needs to be too proactive always. It is the duty of the instructors or the employers who need to introduce regular interactive sessions, distribute innovative pamphlets, interesting games, and puzzles on these awareness assessments. These activities will make the awareness sessions interesting and relatable. They will apply them in their real-life practice. Some organizations are using simulated attacks on particular profiles to observe their immediate behaviors to overcome the situation. The practical learning exposures that they have experienced during the knowledge-sharing sessions can be very useful. (Sunil Chaudhary, 2022)

When a survey was conducted in Saudi Arabia regarding cyber awareness programs the volunteers were asked to collect data from the participants who were using various internet-based services and devices. They were asked to select the security tools that they were using with their personal and professional devices. The response to that survey showed that the security tool implementation was very low which could put them into trouble. Their graphical representations were given below [figure 9]. (F. Alotaibi, 2016)

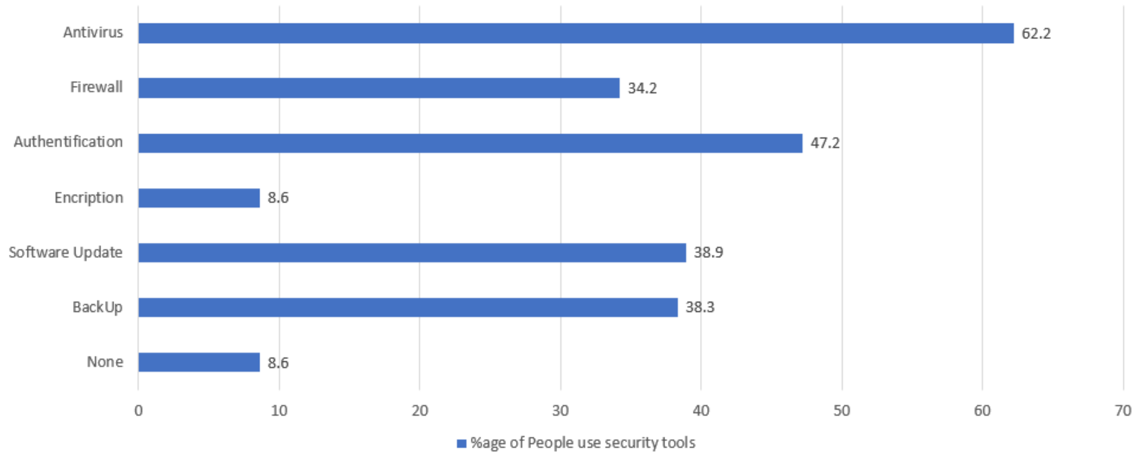

Figure 9   Security Tools used by participants in a survey (F. Alotaibi, 2016)

Common questions (mentioned below) which are mostly asked in the IoT cyber awareness surveys could help us to identify why lax IoT devices used by people, become easy targets for cyber hackers. When we will start asking such questions to ourselves, we could solve maximum issues related to security . Only (approx.) 33% of the participants who have participated in the survey, felt that their data were safe. (Krzysztof Cabaj, 2018)

Question 1: Who has been installing and maintaining the software in your IoT devices?

- Yourself
- Service Provider
- Company Administrator
- IT Technician

Question 2: Are you using the latest version of your software versions in your IoT devices?

- Yes
- No

Question 3: How your IoT devices are connected to Internet?

- Common Wi-Fi
- Separate Networks

Question 4: Are you Using any firewall software, Anti-Virus software, and VPN in your IoT devices?

- Yes
- No

Question 5: Is there any Vendor security posture / Data Insurance available on your IoT devices?

- Yes
- No

Question 6: How often do you change your IoT device credentials?

- In a month
- In every 3 months
- In every 6 months
- Never / Default password

Question 7: Do your IoT devices have strong encryption technology?

- Yes
- No

6.1 Industrial awareness program

As per surveys, (Onwubiko, 2019) attractive approaches to educate the audience would always be the top priority for the institutions. Some ideas are like Surveys, which are based on issue related to technical and security policy. This would give a statistical analysis for the period-based report for the complete organizations. There should be a dedicated awareness or security week must be declared in the financial calendar in which employees should participate to make some roleplays, small storytelling sessions, Poster making competitions, and other activities to celebrate awareness week. Dedicated IT supports should be provided for cyber awareness where employees can get their doubts cleared and raise their concerns over ticket or case review. E-Learning websites would be very helpful for the employees where they can get an ample amount of knowledge with interesting games related to cyber security. Additionally, certain certifications can be rewarded to them when they will clear the exams. Interest should be shown by individuals as well as senior management organizations towards the cyber awareness program which would result in the effectiveness of the program. (Sunil Chaudhary, 2022)

It is important that the coordinator of the Cyber awareness program needs to take appropriate provisions to evaluate the effectiveness of the program with respect to its outreach among the audience else the awareness campaign can be tilled towards a complete failure. “Metrics framework” initiated by the SANS security awareness model is considered one of the best maturity models as per research which has continuous tracking progress statistics as well as a mature awareness initiative. As in every business model, the investors are usually keen to inspect the Return on Investment (ROI), here as well the research and development wings have dedicated targets to get the expected outcomes from their audience which has made this model more successful. [Table-2] (Sunil Chaudhary, 2022)

Methods	Descriptions	KPIs (Key Performance Indicators)
Process or Methods improvisations	This is calculated as per the ratio between the wealth invested in the course structure for security awareness skills with the actual outcomes from the employees regarding the necessary protocol follow-up. When the result is less than 1:1 then the experts take many important steps to improvise the ratio. New innovative methods need to be involved in the primitive learning cycle which will make it more practical and real.	▪ Cost of investments (Money spend per person with time investments)
		▪ Major security risks and technology that the learning curve encircled
		▪ Involvement of staff numbers in every learning seminar
		▪ Unbiased feedback form from the staff on the awareness curriculum
		▪ Take active counts on the security incidents that have been reported
		▪ While encountering the issue did the employee take necessary actions in an immediate basis or not, and what are the breakpoints in their action which has caused to the pop-up security breach
Outbreak Resistance	Mock cyber drills need to be addressed at regular intervals which would test the practical exposure of the staff to the potential cyber-attack on the office IoT devices	• Periodic surveys, quizzes, and interactive sessions need to be arranged to recognize the attacks
		• Cyber-attack incidents with proper cinematography would cheer the audiences, as well as experienced incidents, need to be shared with staff so that the fault chance can be avoided to repeat.
Internal Security Protocols	Every organization should have an internal IT security team who would take all the responsibilities to maintain its firewall which would make the internal systems more secure with a perfect shield	• The employees should encourage to work on the company-provided machines rather than their personal gadgets.
		• While delivering office work, there should only be accessible to secure

		websites with the usage of an internal firewall and office VPN (Virtual Private Network)
		• In case, the deliverables can be done by accessing the client's application which is a different environment then the required client and delivery manager approval should be made mandatory to get the IP addresses whitelisted.
Efficiency and Effectiveness	It measures the severity and importance of the action taken against any attacks	• Security incidents impacts (number and cost of security incidents)
		• Down-time (availability of systems after phishing)
		• Most severe incidents (Human error) represent the proportion of the total number of serious incidents that occurred due to unintentional or careless behaviors of employees

Table 2 Evaluation Metrics and measuring parameters (Sunil Chaudhary, 2022)

Knowledge, attitude, and behavior are the three key components that would motivate the employees to lead to a successful cyber awareness drive. Knowledge describes the depth of understanding of the issues, consciousness angles of the various cyber threats, priority given to the security policies which were predefined, recommended procedures, mandatory guidelines, and figuring out the fault points. Secondly, an attitude always defines the person's beliefs, opinions towards different security breakdown situations, critical thinking, or mature feelings toward security protocols. An attitude can be optimistic (For example, Reporting the security incident on an immediate basis as a priority additionally if the client's platform is also infected then inform them immediately so that future losses can be avoided) or pessimistic (for example, reporting different cyber incidents are waste of time. If the Client's platform is compromised, then it's their issue. IT security Team would be responsible for this, not me). Finally, behavior represents how the person approaches security incidents with respect to the learning that was provided in past, and how they are addressing the issues in different situations using their own presence of mind. (Abdur Razzaq, 2017)

6.2 Domestic Awareness Program

Domestic awareness plays a vital role to stop the cyber activities as domestic appliances are their easy targets. Putting all the responsibilities over manufacturers is not a genuine option. Even the technology is more advanced and the IoT devices behave smarter than most of the world's population still they need some human interventions to act accurately. Our world is full of diversity and uniqueness. We can find each corner of the world with different people and their different priorities. As per their convenience, they would use IoT devices. So, people should act smart as they want their system to be smart enough. They should follow some basic security principles. (PhillipWilliams, August 2022)

We can put reminder to change our passwords in every month. It must be complex and shouldn't contain any easy guessing words like our name, date of birth, month name. Adding special characters with alphanumeric letters would be best options. Always update the software that we are using in our systems. Data back-up should be taken in regular interval. We can discuss facts and preventions of cyber-attacks during our family conversations. Before using the IoT devices, we can read the safety parameters as well as security parameters and make sure all our family members are aware of the same. Making all the security measures implement in daily activities can reduce the cyber-attack threat. In the era of zero trust, we can't trust what we see, hear, and read. It is better to confirm the sources from secure trusted websites then only we can proceed with the actions. (Krzysztof Cabaj, 2018)

If someone would say hey! I have experienced cyber-attacks on my IoT devices then we need to dig into the depth of the situation and understand what security components are missing in the puzzle. Let's discuss with some research papers, how they have done analysis and get the appropriate prerequisites to avoid such situations in the future.

7 Precautionary approaches

Let us start with some practical examples which would help us to grasp the actual understanding behind the attacks and their approaches towards IoT devices mentioned in various research papers. Multiple access control over IoT devices can cause security breakage smoothly. As the IoT device has instructions to follow from multiple inputs so any inputs which carry the virus/malware can infect the IoT device easily. The owner of the IoT devices shouldn't share his/her device's user credentials with other people that they don't trust. In the case of the organization level, authorized employees should have access to the company's IoT devices after sufficient background verifications. Maybe Mr. Alex has shared some of his IoT device credentials with other persons who have been carrying the malware which later infected the Coffee maker IoT device and spread it all over his smart home. (Jagpreet Kaur, 2021)

When the smart devices start communicating with each other through normal text, then there might be a chance of spying on those communications using the techniques of man-in-the-middle (MitM), Active and Passive attacks. Here the attacks would take a position in between the data sender and receiver IoT devices. They might only view their exchanging of information or modify the information and get the required access to the IoT devices. A strong encryption technique can break such attacks. It is recommended to use encryption while storing the data inside the IoT devices and sending it to other devices as well. (PhillipWilliams, August 2022)

IoT devices are always connected over the Internet, so it is recommended that if they use updated software then the chances of getting hacked are tough. Updated versions of software have minimal changes of vulnerability (PhillipWilliams, August 2022). Additionally, it is recommended to use the firewall and VPN in IoT devices. There are other attacks as well which are mentioned below [Table - 3] as per their severity with respect to some precautionary measures. Smart IoT devices used for Children's safety, tracking, (Sa Murugan, 2019) and education can be hacked and data can be misused to manipulate children easily. It can be protected by making those IoT devices encrypted communication and strong authentication features. Voice-activated assistance like (Alexa and Siri) can be hacked physically as well as remotely which we need to ensure with multifactor authentication methods such as WAP2 or WAP3 (PhillipWilliams, August 2022)

Spoofing is also considered as one of the techniques used by hackers to get the required data from the IoT devices. [figure -10]

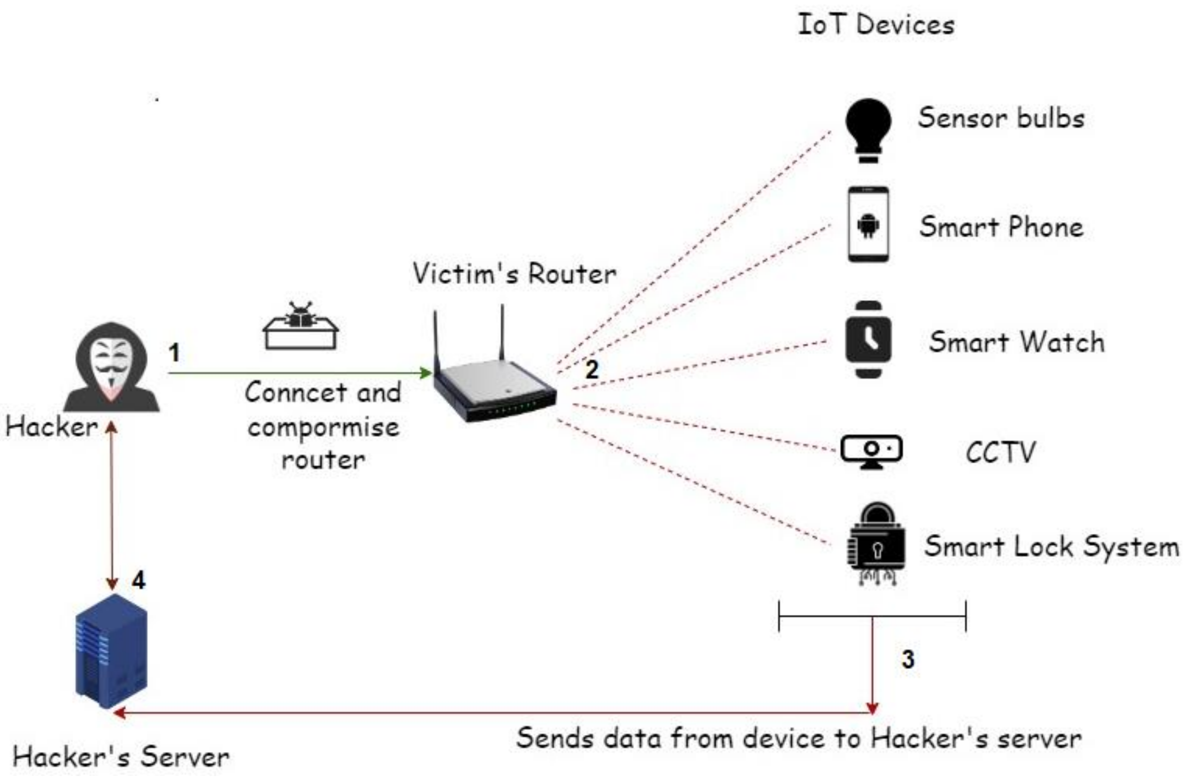

Figure 10 Spoofing example (PhillipWilliams, August 2022)

Type of attacks	Severity Level	Behavior	Precautions
Phishing	low	Fraud emails and messages are sent by hackers to IoT devices when the user would click on the links then the respective device would get hacked by cybercriminals.	Check the source of the information before proceeding with any link. It is recommended to block suspicious emails. Don't connect all IoT devices to the same WIFI network.
Man in the middle	Low to medium	Hostile may view as well as manipulate the transmitted data between IoT devices.	Data confidentiality should be given priority. Regularly change the user credentials, avoid using sensitive information over public networks.
Large attack surface	Medium	When IoT devices get multiple options to offer service Internet, then the attack surface area becomes wider. Each connection can be an opportunity for hackers to manipulate the device.	Enable only the necessary services through IoT devices. Device access should be handled by the owner and his/her known contacts. Avoid connecting multiple connections to IoT devices.
Malware	High	Malware attacks are the most famous attacks where infected software like Trojan Horse, Ransomware, Spyware, and Maria Malware would infect the IoT devices completely without users' recognition. These can be sent via SMS, email attachment, or other methods.	Avoid unknown SMS, Emails. Update IoT device software regularly and follow all security measures. Admin privilege should be protected with multiple authentications.
Dos (Denial of service)	Extremely high	Sending floods of requests to the IoT devices to increase processing time and halt the system. The user won't get the response from the IoT devices resulting in a denial of service.	Whitelist only the ports which should connect to the IoT devices. Use a firewall and avoid IP spoofing. EDR (Endpoint detection and response) agents should deploy to monitor and analyze the threat detection.
Blocking	Extremely high	Huge amounts of data/Malware attacks can lead to network jamming and blocking. Infected viruses would completely block the IoT device to respond.	Usage of updated anti-virus, Firewalls, and anti-jamming programs which could save IoT devices from blocking threats.

Table 3 Types of cyber-attack on IoT devices (Abdur Razzaq, 2017)

8 Conclusion

We have discussed how innovative technologies have strengthened mankind with flying colors. IoT devices are extending their wings all over the world with their smartness and compatibility bondage with humans. However, the vulnerability associated with these devices can’t be ignored. The solution to this problem can be settled when we will get to the root cause of the issue. Making awareness in regular practice with ethical approach will reduce the cyber-attacks on IoT devices.

The endless fight between hackers and survivors in this modern world will continue. However, the responsibility to give some extra edge to the survivors is reliant on the design and policies of the IoT device manufacturers, Government bodies, network service providers, and finally on the consumers themselves. Any pitfalls can be an opportunity for hackers to break through our system. The famous quote “Survival of the fittest” – by Charles Darwin is also applicable to this scenario. The persons who care about their security will follow the security policies and rules which would help them to salvage from cyber espionage. On the other hand, there would be plenty of easy targets waiting in a queue for black hat hackers. So, it depends on the user on which side he/she wants to be on.

In the end, the solution to this problem can be handled properly. Change begins with us. When we start following the required measures and explain their importance to our family, friends, and children that would collectively create a shield of human awareness against cyber scammers. This would help us to protect ourselves as well as to enjoy the sip of the ingenious invention of scientists as IoT devices. What has happened with Mr. Alex can be a lesson learned for himself as well as for us. In future, the repetition of such cases can be avoided with preventions.

9 References

(n.d.). Retrieved from Nordic-ecolable: https://www.nordic-ecolabel.org/

(n.d.). Retrieved from aphaea: https://www.aphaea.eu/partners/evira

Abdur Razzaq, M. a. (2017). Security Issues in the Internet of Things (IoT): A Comprehensive Study. *International Journal of Advanced Computer Science and Applications*.

aphaea. (n.d.). *aphaea.eu*. Retrieved from aphaea: https://www.aphaea.eu/partners/evira

Espinosa, N. (7 September, 2018). The Five Laws of Cybersecurity.

F. Alotaibi, S. F. (2016). A survey of cyber-security awareness in Saudi Arabia. *11th International Conference for Internet Technology and Secured Transactions (ICITST).* IEEE.

Hougland, B. (22 August, 2016). *What is Internet of things*. Retrieved from Enfellowship: https://www.enfellowship.org/what-is-the-internet-of-things-benson-hougland/

Jagpreet Kaur, K. .. (2021). The recent trends in cyber security. *Journal of King Saud University - Computer and Information Sciences*, 5767- 5777.

Katzan, H. (2016). Contemporary Issues in Cybersecurity. *Journal of Cybersecurity Research*.

Knowles, C. (13 Jan, 2022). *ecommercenews*. Retrieved from ecommercenews.co.nz: https://ecommercenews.co.nz/story/smart-home-market-continues-to-grow-driven-by-changing-tech-and-demographics

Krzysztof Cabaj, Z. K. (2018). Cybersecurity: trends, issues, and challenges. *EURASIP Journal on Information Security*.

Legchekov, S. (1 August, 2022). *IoT for Smarter Supply Chain Management and Logistics*. Retrieved from ScienceSoft: https://www.scnsoft.com/blog/iot-scm-and-logistics

Mark T. Hoffmann . (28 June, 2021). *Profiling hackers The psycology of Cybercrime.* TEDxHHL, Germany.

NZ Jhanjhi, M. H. (20 December, 2020). Cyber Security and Privacy Issues in Industrial Internet of Things. pp. 361-376.

Onwubiko, C. O. (2019). Cyber KPI for Return on Security Investment. *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*.

Oracle. (9 May, 2022). *what is IoT ?* Retrieved from Oracle.com: https://www.oracle.com/internet-of-things/what-is-iot/

PhillipWilliams, I. K. (August 2022). A survey on security in internet of things with a focus on the. *Internet of things*.

Sa Murugan, N. P. (2019). Smart IOT Device for Child Safety and Tracking. *Security and privacy analyses of internet of things Children's toys, IEEE Internet Things*, 978-985.

Sachchidanand Singh, N. S. (2015). Internet of Things(IoT): Security Challenges, . *International Conference on Green Computing and Internet of Things (ICGCIoT)* (pp. 1577-1580). Noida: IEEE.

Sánchez López, T. R. (2011). Adding sense to the Internet of Things . *An architecture framework for Smart Object systems*.

Securing-Internet-of-Things. (06 January, 2022). Retrieved from drishtiias: https://www.drishtiias.com/daily-news-analysis/securing-internet-of-things

Sunil Chaudhary, V. G. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness program. *Journal of Cybersecurity*.

Vardomatski, S. (12 July, 2018). *HQ software*. Retrieved from hqsoftwarelab: https://hqsoftwarelab.com/blog/the-history-of-iot-a-comprehensive-timeline-of-major-events-infographic/

Waqas Ahmad, A. R. (2022). Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey . *Electronics 2022*.

Williams, S. (26 August, 2022). *SecurityBreif*. Retrieved from https://securitybrief.co.nz/story/internet-of-things-vulnerability-disclosures-grew-57

Zhang, N. S.-H. (2017). Understanding IoT Security Through the Data Crystal Ball : Where We Are Now and Where We Are Going to Be. *ArXiv*.