TÜRKİYE ULUSAL AJANSI
TURKISH NATIONAL AGENCY

Co-funded by the
Erasmus+ Programme
of the European Union

MALICIOUS CONTENT, SOCIAL ENGENEERING, VULNERABILITIES IN THE INTERNET OF THINGS

2020-1-TR01-KA229-094378

Cybersecurity: Where is Our Data?

The Big Brother of Data

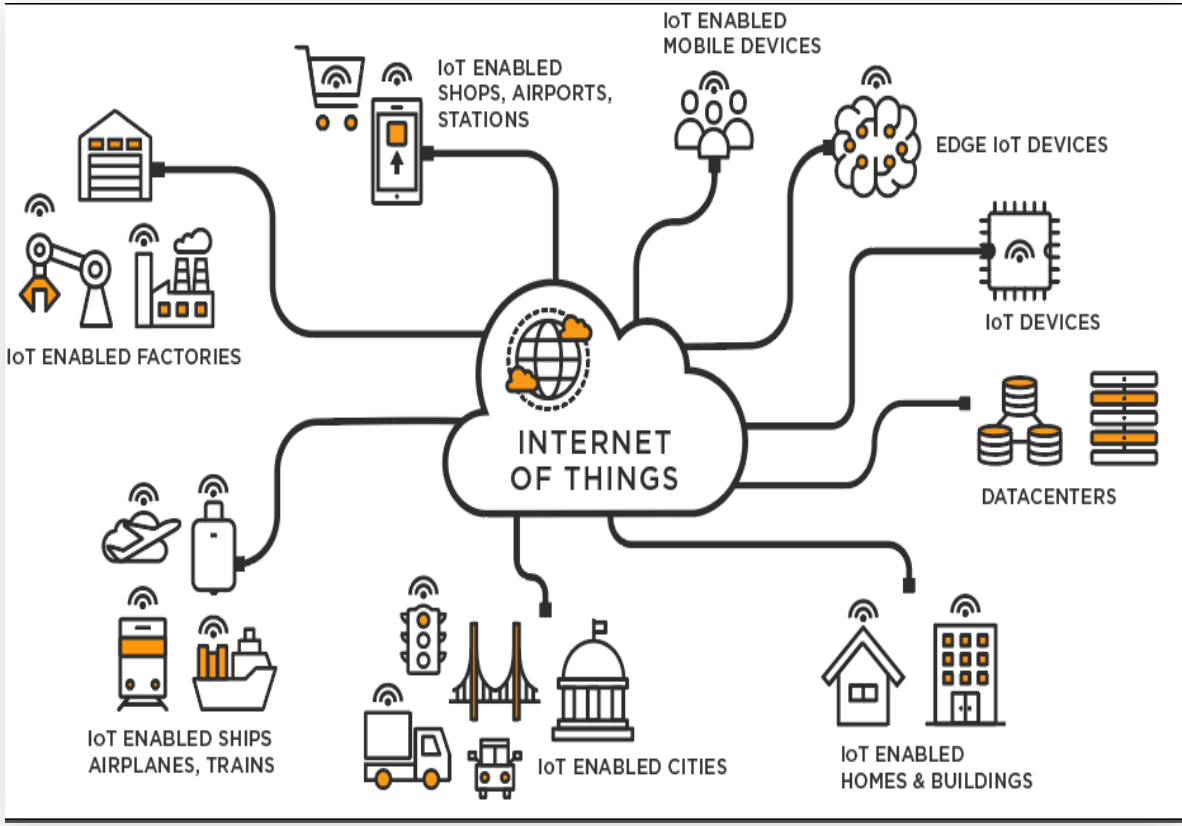
What Do We Share?

All our devices are connected to the Internet;
All of them are loaded with sensors!
Internet of Things?

Ubiquity and Things

Ubiquity:

- It is the fact of being present everywhere at the same time.
- In the context of computing, we are starting to get used to the fact that information is everywhere at the same time (eg, the same email message is on mobile phones, it is on a laptop, it is on a computer in an internet cafe).
- This is possible thanks to the *magic* of the Internet! And the technologies that are based on it.
- Things + Internet + (a pinch of) Cloud = Internet of Things (IoT).



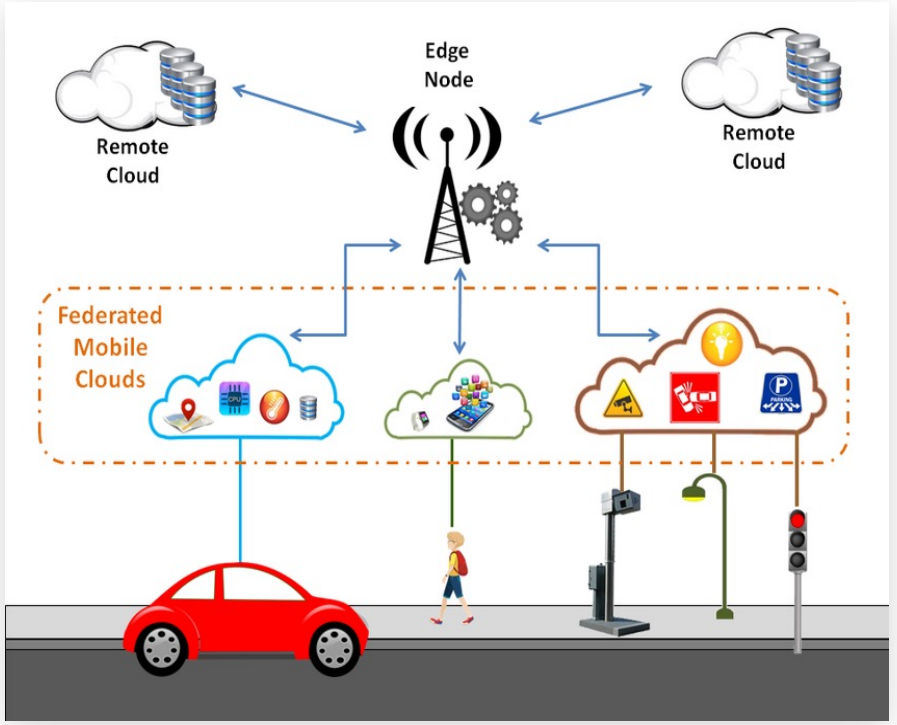
And the Security of Things?

The Internet of Things fuels some of today's most promising businesses, which causes extraordinary pressure to get to market, and things are mostly very weak in terms of IT security.

But why?

Imagine combining the Internet (and *all* the security issues associated with it) with mobile devices, sensors scattered all over the place, and... *Cloud.*

See the “salty” this is?



But what is Privacy?

Not to be confused with **Confidentiality** !!

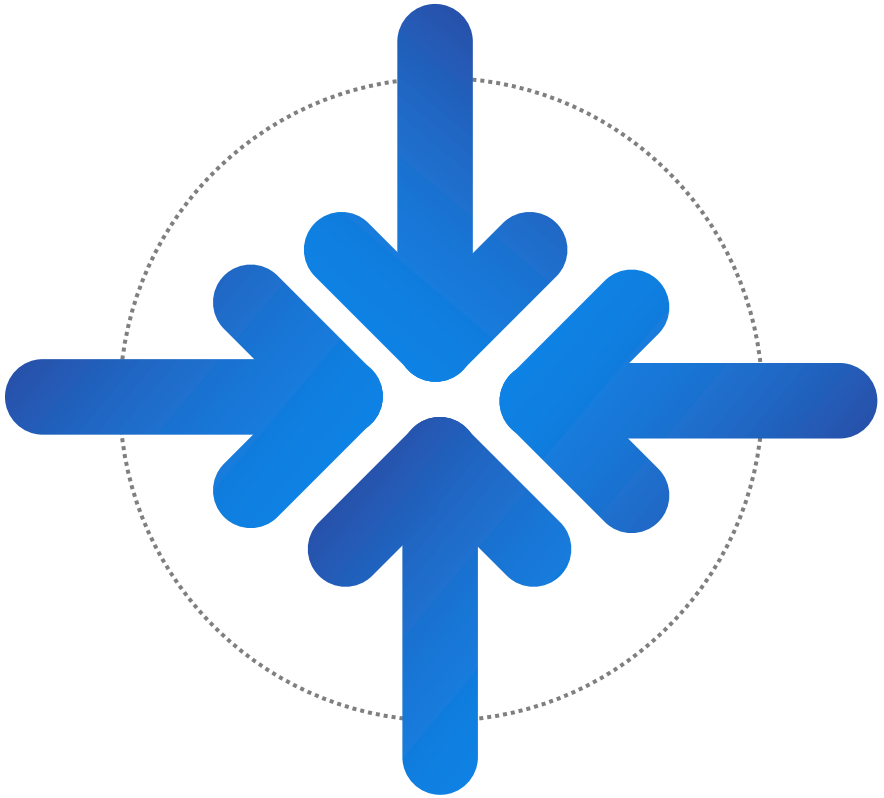
- **Privacy** refers to information relating to the person, to his intimate;
- **Confidentiality** is about secrecy.

Privacy, in the ideal digital world, means:

- **Absolute control** over the information that is processed or **inferred** ;
- **Absolute information** about what is being stored, processed or inferred about the user's private life;
- **Right to be forgotten** .

We are Social Beings!

- We love to say we want privacy, but...
- We wait our lives on social media!
- We mix privacy with security!
- And we forget how valuable our information is...



A Little Bit of Social Engineering

Social networks

Let's start by spying on them...

Gather Information

Nothing like a happy conversation where we ask mundane things...

Compilation and Exploration

Now we have a nice database of information

... *Profit* ?

Compromise of credentials, obtaining information, etc.

Social Networks and Privacy

01

We Publish Everything!

Where we went, where we were, who we were w`th, what we wore, what we ate...

02

Photos

We even pub`sh photos w`th other people... And do they know?

03

misunderstanding

We make th`ngs known about us that we don't even realize...

04

we are a mine

Our data `s the go d of the century. XX , and we g`ve them away w`thout realizing it

Some News...

The report reveals that hackers currently charge $129 to hack into popular U.S.-based email accounts such as Gmail, Hotmail, and Yahoo. They'll also go after corporate email accounts, charging $500 per mailbox. Popular Russian email accounts will cost between $65 and $103 while breaking into popular Ukrainian email accounts will cost $129. Hacking the IP address of a computer user will cost you an extra $90.

Dell: The going rate for a hacker to break into a Gmail account is $130 (April 7, 2016)
https://www.businessinsider.com/dell-hacking-into-gmail-costs-130-2016-4

Researchers hack a pacemaker, kill a man(nequin) (September 8, 2015)
http://www.computerworld.com/article/2981527/cybercrime-hacking/researchers-hack-a-pacemaker-kill-a-man-nequin .html

Google Allo shares conversations with Google Assistant (March 16, 2017)
https://www.noticiasaominuto.com/tech/758222/app-de-mensagens-da-google-revela-mais-sobre-si-do-que-gostaria?utm_source=emv&utm_medium=email&utm_campaign=tech

While killing a simulated human via hacking is less dramatic than wirelessly murdering a real human via a keyboard, researchers said it can be done by "a student with basic information technology and computer science background;" the medical mannequin attackers had no penetration testing skills, but successfully launched brute force and denial of service attacks as well as attacks on security controls.

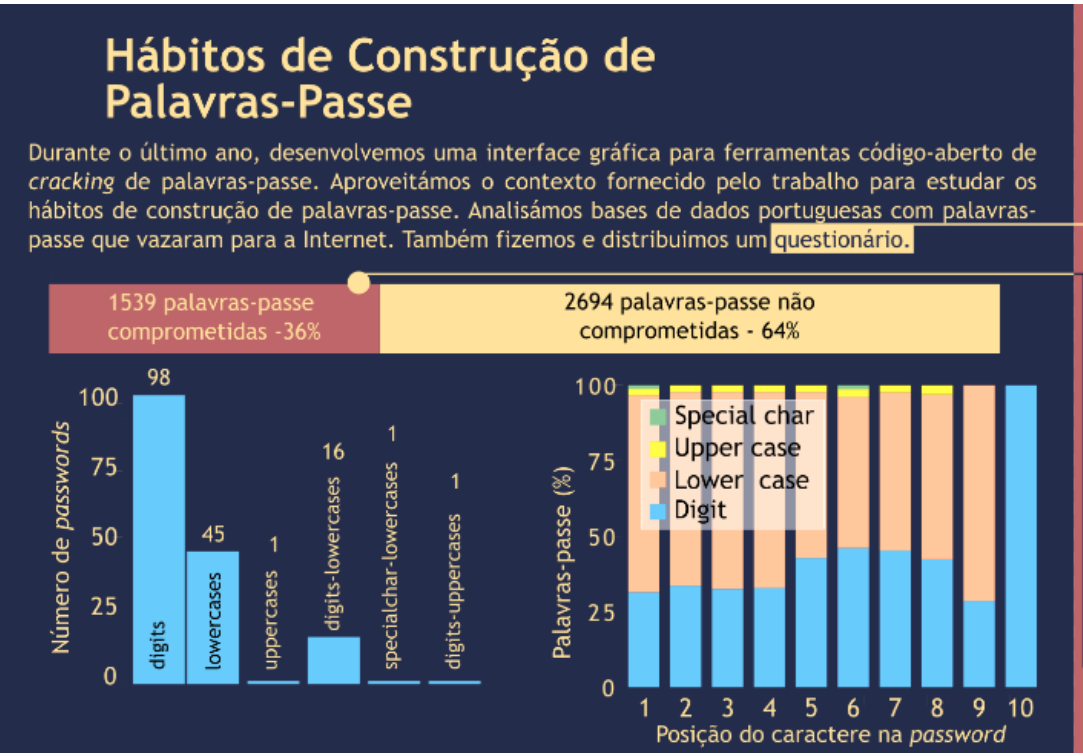
Conta o Recode que, numa conversa entre duas pessoas o Assistant apresentou resultados de pesquisa sobre um tema sem que lhe este tivesse sido pesquisado. De acordo com um dos intervenientes, esse resultado de pesquisa estava relacionado com uma busca que um dos participantes na conversa havia feito dias antes.

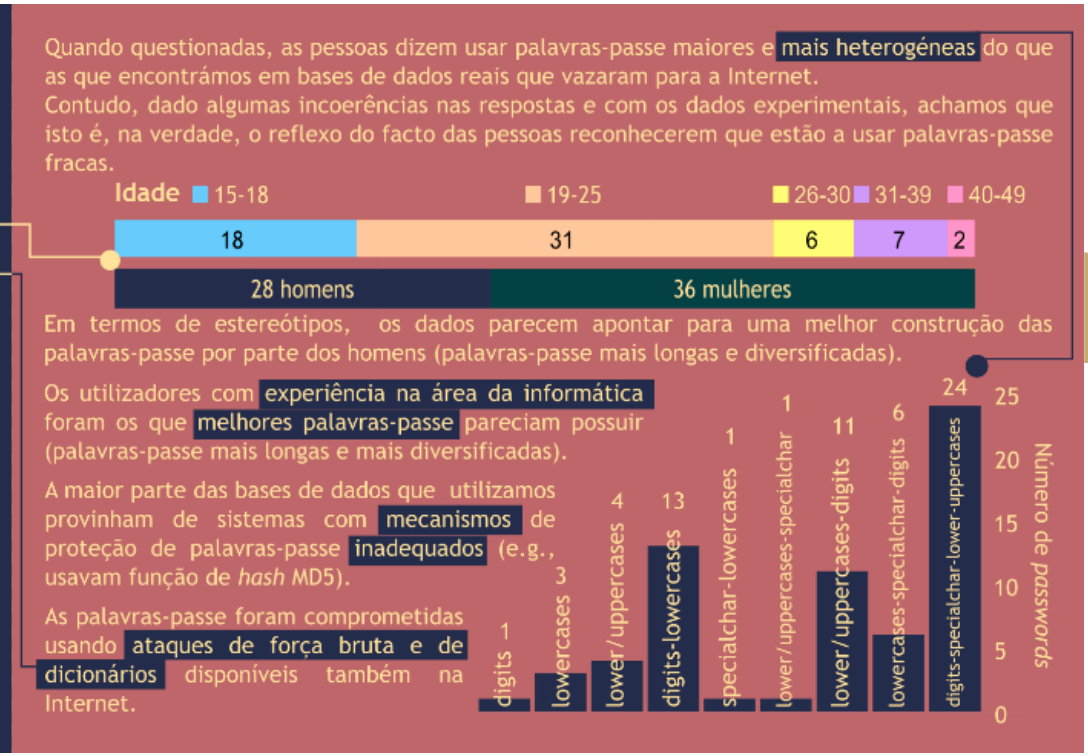
Where is the problem?

Here!!!

Mostly? Between the chair and the keyboard...

Insecure passwords **, carelessness, carelessness, lack of knowledge...**





Source

Inácio, P., Sequeiros, B; "*Onde param os nossos dados*" ; Comunicação no âmbito de um evento de ciber segurança organizado na Escola Secundária Campos Melo. Covilhã, Outubro de 2021

MAIN TYPES OF VIRUSES AND MALWARE. HOW TO PROTECT OURSELVES AGAINST THEM.

Viruses, technically known as malware, are computer codes created to infect our computers, cause problems in their operation or steal information. Although they are constantly evolving and new types appear from time to time, we are going to analyze the main viruses and the best way to protect ourselves against them.

IES ANTONIO MENÁRGUEZ COSTA

SPAIN

1

ADWARE

This software offers you unwanted or misleading advertising. These ads can appear in the browser with pop-ups or windows with great visual content, and even audio. They are reproduced automatically in order to generate economic profits for the creators.

How do we protect ourselves?

Let's avoid opening download links from unreliable pages and, when we install software, we should review the steps so that no browser, program or plug-in is installed without us noticing.

2

SPYWARE

This type of virus is responsible for fraudulently collecting information about the user's browsing, as well as personal and banking data.

How do we protect ourselves?

The first and most important step will be the installation and updating of a good antivirus system. Another way to protect ourselves is to avoid connecting unknown devices, such as USB or external hard drives.

3

COMPUTER WORMS

This virus is created with the ability to replicate between computers. It often causes network errors as a result of abnormal bandwidth consumption caused by this malware.
Cyber criminals often use flashy names on the links for this virus to be downloaded, such as the words: gift or prize.

How do we protect ourselves?

If the antivirus is up to date, it will identify and eliminate this type of threat that tries to sneak into our devices, as well as deactivating the "autorun" function of external drives (USB sticks or hard drives).

COMPUTER TROJAN

4

This type of virus presents itself as legitimate software, but by executing it, it allows the attacker to take control of the infected device. As a consequence, our personal information would be at permanent risk, at the mercy of the attacker to steal everything he wanted from our infected computers.

How do we protect ourselves?

In addition to having the operating system and antivirus updated, and analyzing the USB devices that are going to be connected to our computer, we must be very careful when we browse the Internet, since an infected file may end up being installed or when accessing fraudulent web pages.

RANSOMWARE

5

Malware that takes complete control of the device by locking or encrypting user information and then asking for money in exchange for unlocking or decrypting files on the device. This malicious software spreads on the device, just like a worm or a Trojan horse. They can arrive camouflaged in email attachments or on unreliable web pages that invite us to download a file under a harmless appearance. They also frequently take advantage of security flaws in the operating system or even applications.

How do we protect ourselves?

Be very careful with malicious emails with an attachment. Most ransomware attacks occur when the user executes an infected file. It is also recommended to make backup copies so that, in case of infection, we have a copy of our data in another storage location.

6

BOTNETS

They are networks of infected devices that cybercriminals use to launch attacks, such as mass spam mailing, denial of service or DDoS attacks, credential theft, etc. Once a device is infected, it will become part of the botnet network whose goal is to continue expanding.

How do we protect ourselves?

The main thing is to make good use of the devices when we connect to the network, having an updated system with antivirus programs installed, using strong credentials and changing passwords regularly and not entering web pages that may be unreliable. Another source of infection is malicious emails.

MALICIOUS APPS

7

When we install an app on our mobile device, it asks us to grant it a series of permissions. Sometimes these permissions are unrelated to the functionality of the app or we download an unreliable app that ends up infecting our device, taking control and stealing the information we have stored on it such as contacts, credentials, images, videos, etc.

How do we protect ourselves?

When it comes to downloading apps, the first thing to keep in mind is to use official stores. In addition, we must review the ratings and comments of other users and information from the developer. When installing it, it will ask us to accept a series of permissions, which we should not give unless it is related to the function of the app.

Co-funded by the
Erasmus+ Programme
of the European Union

KESAN
1990
KESAN TİCARET VE SANAYİ ODASI
MESLEKİ VE TEKNİK ANADOLU LİSESİ

Cyber Security
in
Schools

Vulnerabilities in the Internet of Things(IoT)

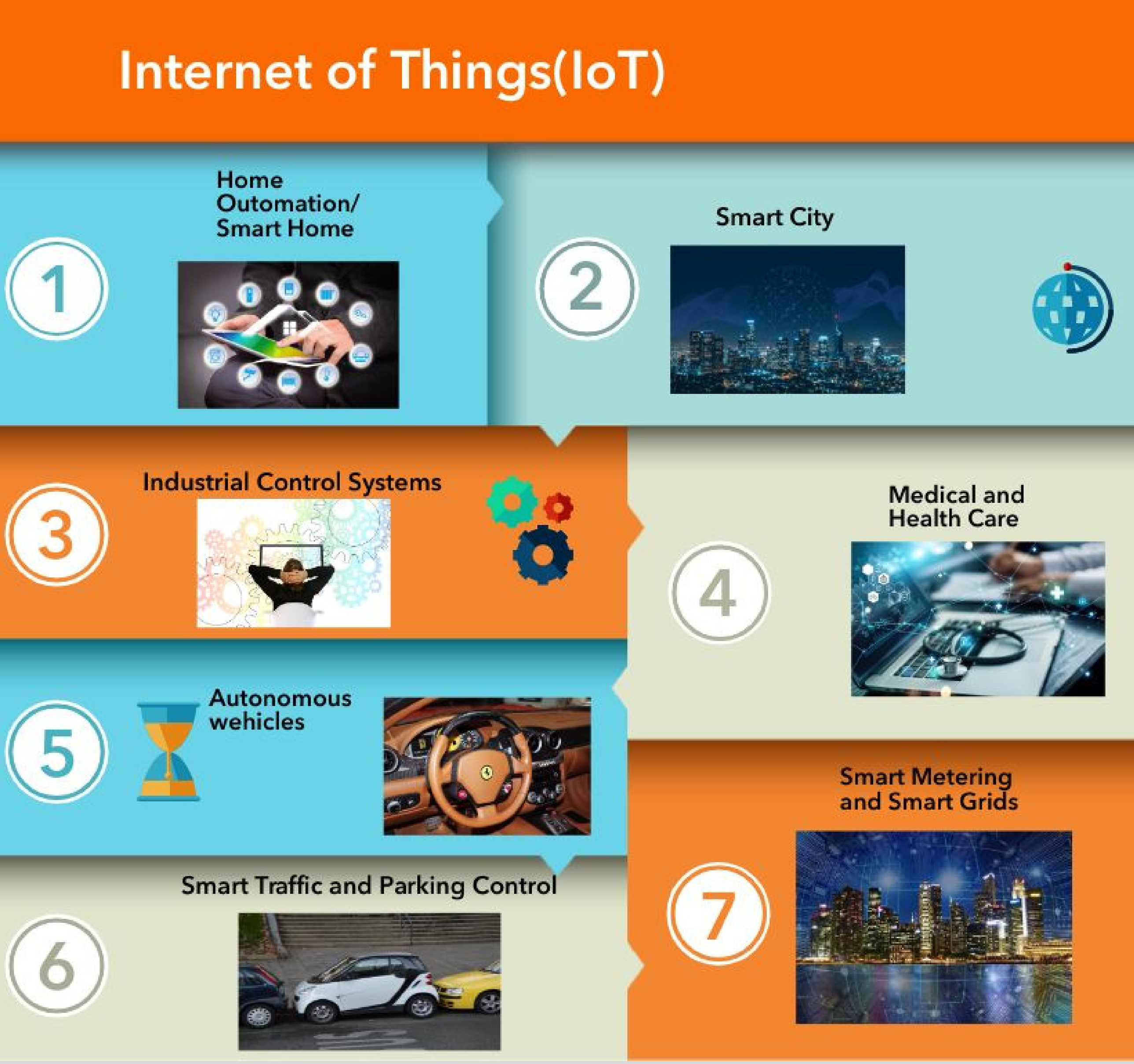
CYBER SECURITY IN SCHOOLS

What is the internet of things (IoT)?

“The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.
A thing in the internet of things can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an Internet Protocol (IP) address and is able to transfer data over a network.Increasingly, organizations in a variety of industries are using IoT to operate more efficiently, better understand customers to deliver enhanced customer service, improve decision-making and increase the value of the business.

How does IoT work?

An IoT ecosystem consists of web-enabled smart devices that use embedded systems, such as processors, sensors and communication hardware, to collect, send and act on data they acquire from their environments. IoT devices share the sensor data they collect by connecting to an IoT gateway or other edge device where data is either sent to the cloud to be analyzed or analyzed locally. Sometimes, these devices communicate with other related devices and act on the information they get from one another. The devices do most of the work without human intervention, although people can interact with the devices -- for instance, to set them up, give them instructions or access the data.” By Alexander S. Gillis, Technical Writer and Editor



The Internet of Things (IoT) is key in digital world of connected living. The futuristic appeal to make life more enjoyable in a hectic daily life routine is enticing to many. The IoT devices have a wide range of applications especially in home automation (smart homes), healthcare, smart energy solutions, autonomous connected vehicles and complicated industrial control systems.

Vulnerabilities of IoT Applications

Weak or hardcoded passwords

Lack of an update Process

Unsecured Network Services

Unsecured data storage and transfer

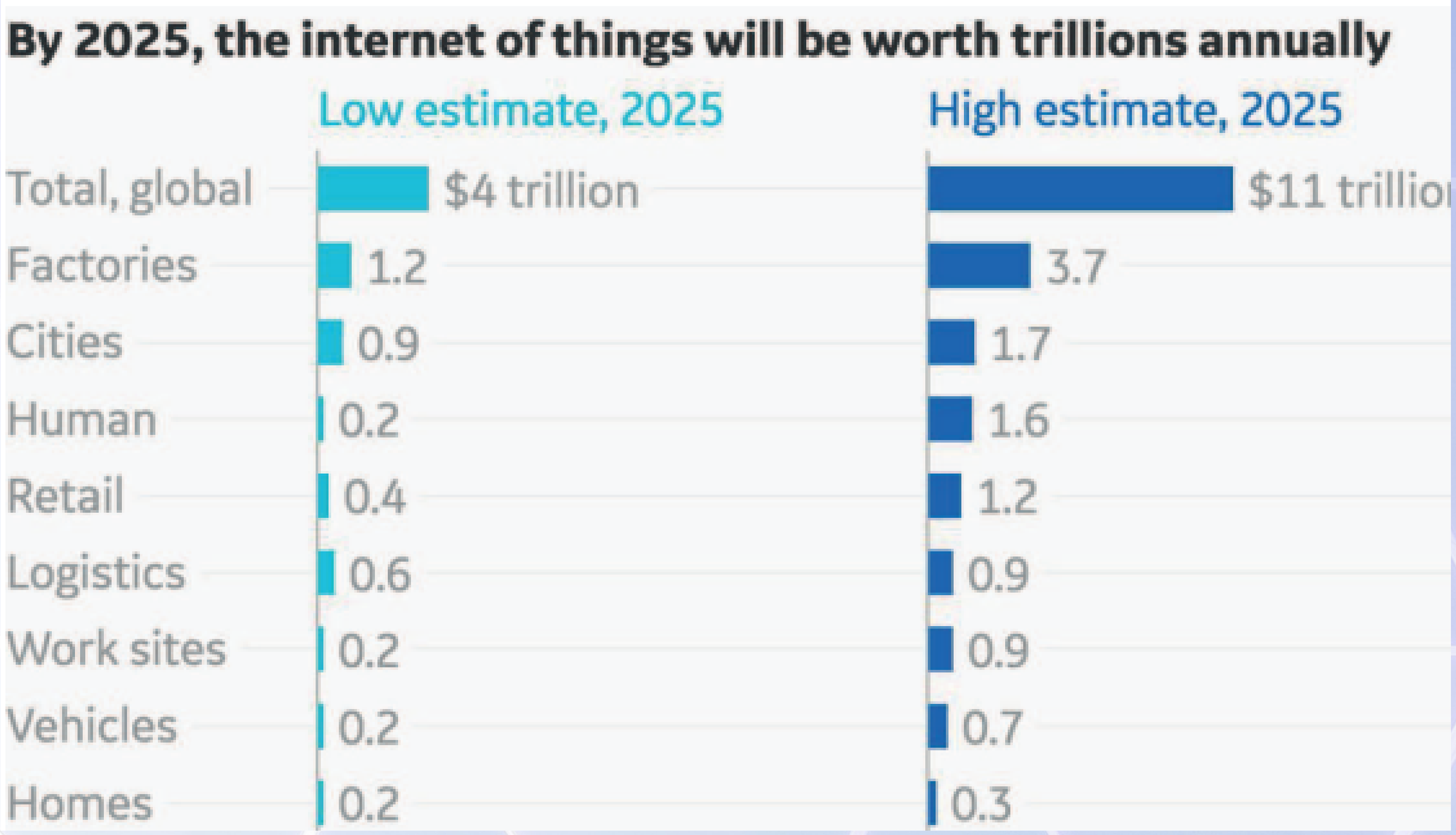
Insecure default settings

Insufficient Privacy protection

Lack of device menagement

lack of an update process

Outdated unsecured IOT App Components



The Internet has become ubiquitous and essential part of our lives. It has enable easy communication, more efficiency at work, connected enhanced living and accelerated innovation. At the same time, Internet has also increased the ease, viability and efficiency of launching a large scale DDoS attacks, especially using IoT devices

IS YOUR SMART HOME SYSTEM VULNERABLE TO ATTACKS?

Along with the convenience they bring, loT devices also offer an entry point into your home against cyber attackers. Digital assistants such as the Echo and Google Home devices have found their way into homes around the world. If you have shared sensitive information such as passwords or bank details, this information may be compromised in the event of any digital intrusion. The same is true for smart Wi-Fi thermostats, as they often have Home/Away modes; informs hackers that you are not at home. Your baby monitor may be vulnerable to hackers trying to hijack your webcam. The probability of these threats occurring is low, but not impossible.
Cyber attackers can gain access to your smart home through malware.

IN CASES WHERE IT IS NOT TAKEN FROM SMART HOME SYSTEMS IN LIEE WITH THE INTERNET OF THINGS, MAJOR SECURITY GAPS OCCUR.

3 STEPS TO STRONGLY SECURING IOT

• KEEP YOUR NETWORK NAME MYSTERIOUS

Showing your modem's default name is often enough for a hacker to identify the make and model of the modem; from this point on it is easy to access your devices. Name your network in such a way that it does not give anyone the slightest clue.

• BUILD A GUEST NETWORK

This is a simple security measure worth implementing. No guest needs to have full access to your network. Also, if your kids have guests they've brought home, how do you know if they're really friends with your kids or if they're not just casual acquaintances? Guest networks are easy to set up and provide basic internet privileges without compromising anything sensitive.

• CHANGE DEFAULT NAME AND PASSWORD INFORMATION

Most devices come with standard usernames and passwords, and it wouldn't be difficult for a hacker to use this information to their advantage. Use numbers and symbols to turn them into strong passwords against attackers, and avoid using a password you use elsewhere.

SOCIAL ENGINEERING PHISHING

1ο GEL Agiou Dimitriou

CONTENTS

WHAT IS SOCIAL ENGINEERING?

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime, these “human hacking” scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems.Attacks can happen online, in-person, and via other interactions.

Scams based on social engineering are built around how people think and act. As such, social engineering attacks are especially useful for manipulating a user’s behavior. Once an attacker understands what motivates a user’s actions, they can deceive and manipulate the user effectively.In addition, hackers try to exploit a user's lack of knowledge.Users may not realize the full value of personal data, like their phone number. As a result, many users are unsure how to best protect themselves and their information.

SOCIAL ENGINEERING-PHISHING ATTACK TECHNIQUES

Phishing

One of the most popular types of social engineering attacks is phishing scams.

Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. The goal is to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

The information is then used to access important accounts and can result in identity theft and financial loss. Attacks using phishing are targeted in one of two ways:

1.**Spam phishing, or mass phishing**, is a widespread attack aimed at many users. These attacks are non-personalized and try to catch any unsuspecting person.

2.**Spear phishing** and by extension, whaling , use personalized info to target particular users. Whaling attacks specifically aim at high-value targets like celebrities, upper management, and high government officials.

There are actually plenty of phishing methods, however, these are the most common used.

Voice phishing (vishing) phone calls may be automated message systems recording all your inputs. Sometimes, a live person might speak with you .

Email phishing is the most traditional means of phishing, using an email urging you to reply or follow-up by other means. Web links, phone numbers, or malware attachments can be used.

SMS phishing (smishing) texts or mobile app messages might include a web link or a prompt to follow-up via a fraudulent email or phone number.

REAL LIFE EXAMPLES OF PHISHING

Example of spare phishing

Armorblox reported a spear phishing attack in September 2019 against an executive of a company that was named as one of the top 50 innovative companies in the world. The email contained an attachment that appeared to be an internal financial report, which led the executive to a fake Microsoft Office 365 login page. The fake login page already had the executive's username pre-registered on the page, adding further to its cover. fraudulent website.

Example of vishing

In September 2020, the Spectrum Health System reported a vishing attack involving patients receiving phone calls from people disguised as employees. The attackers aimed to extract personal data from patients and members of Spectrum Health, including member IDs and other personal health data related to their accounts. Spectrum Health reported that the attackers used measures such as flattery or even threats to force the victims to hand over their data, money or access to their personal devices.

Example of email phishing

The Daily Swig reported a phishing attack in December 2020 on US healthcare provider Elara Caring following an unauthorized computer intrusion targeting two employees. The attacker gained access to employees' email accounts, revealing the personal details of more than 100,000 elderly patients, including names, dates of birth, financial and banking details, social security numbers, driver's license numbers and insurance details. The attacker maintained unauthorized access for an entire week before Elara Caring could completely curb the data breach.

Scareware

Scareware is the bombardment of victims with false alarms and fictitious threats. Users are deceived into thinking that their system is infected with malware, prompting them to install software that has no real benefit. Scareware is also referred to as rogue scanner software or fraudware. A common example of scareware is the legitimate pop-up banners that appear in your browser while surfing, displaying such text as "Your computer may be infected by malicious spyware." It either offers to install the necessary tool for you (often infected with malware) or it will direct you to a malicious site where your computer will be infected.

Pretexting

Pretexting is form of social engineering in which an attacker tries to convince a victim to give up valuable information or access to a service or system. The distinguishing feature of this kind of attack is that the scam artists comes up with a story — or pretext — in order to fool the victim. The pretext generally casts the attacker in the role of someone in authority who has the right to access the information being sought, or who can use the information to help the victim. For instance, the pretexter may impersonate colleagues, police officers, bank officials, or other people with legitimate authority.

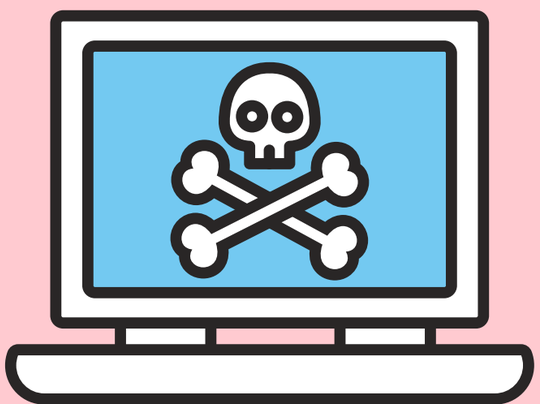
Pretexting has a fairly long history in the U.K., where it's also known as blagging, it's a tool tabloid journalists have used for years to get access to salacious dirt on celebrities and politicians.

Baiting

As its name suggests, Baiting attacks use a false promise to pique the victim's curiosity. They lure users into a trap that steals their personal information or infects their systems with malware.

The most dangerous form of Baiting uses natural means to distribute malware. For example, attackers send the bait (flash drivers with infected software) to exposed areas, where potential victims are sure to see it (eg bathrooms, elevators, parking lot of a targeting company). The bait will have something that usually catches the attention of the victims, such as a label that says "company payroll".

Of course, baiting scams do not have to be done only in physical space. There are also online baiting forms that consist of enticing ads that lead to malicious websites or encourage users to download an application that has been infected with malware.



HOW TO SPOT THESE ATTACKS

Defending against social engineering-phishing requires you to practice self-awareness. Always slow down and think before doing anything or responding.

Attackers expect you to take action before considering the risks, which means you should do the opposite. To help you, here are some questions to ask yourself if you suspect an attack:

→ **Are my emotions heightened?**

→ **Does this offer sound too good to be true?**

→ **Can this person prove their identity?**

→ **Attachments or links suspicious?**

→ **Did my friend actually send this message to me?**

→ **Does the website I'm on have odd details?**

→ **Did this message come from a legitimate sender?**

HOW TO PREVENT PHISHING ATTACKS

Beyond spotting an attack, you can also be proactive about your privacy and security. Knowing how to prevent social engineering attacks is incredibly important for all mobile and computer users.

Here are some important ways to protect against all types of cyberattacks:

Never click on links in any emails or messages

Use multi-factor authentication.

Use strong passwords (and a password manager)

Avoid sharing names of your schools, pets, place of birth, or other personal details

Never let strangers connect to your primary Wi-Fi network

Keep all network-connected devices and services secure

Use a VPN

SOURCES

- https://www.secnews.gr/180321/ti-einai-to-social-engineering-poies-oi-technikes-tou-kai-pos-na-prostatefteite/
- https://www.csoonline.com/article/3546299/what-is-pretexting-definition-examples-and-prevention.html
- https://www.phishing.org/what-is-phishing
- https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering

HOW TO IMPROVE YOUR PASSWORD

I.P.S.E.O.A.
"Gallo"

INTRODUCTION

The students of the school **I.P.S.E.O.A GALLO** decided to make this e-book to give you some advice in managing your passwords. We would like to give you some technical and practical advice.

in this e-book we will give you 3 tools, to improve your security, these 3 tools are:
- 2-factor authentication
-how to create a password
-how to check if your password is safe.

I.I.S.S.
"GALLO"
AGRIGENTO

Two-Factor Authentication (2FA)

Given how easily password and username combinations can be stolen by hackers, and when they do, two-factor authentication is the best way to protect your data from theft.

Two-Factor Authentication (2FA) works by adding an additional layer of security to your online accounts. It requires an additional login credential – beyond just the username and password – to gain account access, and getting that second credential requires access to something that belongs to you.

Two-Factor Authentication (2FA)

Without this additional access method, it’s impossible to enter the account, which in turn makes it impossible for hackers to access your account using only stolen password and login information.

the best 2FA app according to our research is **Google authenticator**

GOOGLE AUTHENTICATOR

HOW TO CREATE YOUR OWN PASSWORD

Nothing is more frustrating than creating new passwords.

To create a strong password, putting together 12 or more characters, numbers and letters often becomes a challenge.

A strong password generator helps create strong passwords to be used on various services, avoiding the risk of brute force attacks that are impossible to guess for any attackers and cybercriminals.

The password must not be linked to personal information and words in an Italian, English or other language dictionary must never be used.

HOW TO CREATE YOUR OWN PASSWORD

Using a password generator can help provide strong, random passwords while minimizing risks.

Our school recommend using as a site to generate passwords we think this is the best around: **LASTPASS.COM**

https://www.lastpass.com/it/features/password-generator

HOW TO CHECK YOUR PASSWORD

With **kaspersky.com** password verification you can quickly find out how secure your password is. This tool calculates the average time it takes a computer to crack your password. Furthermore, it can check whether the password in question has been made public in the past due to a data leak or a hacker attack.

useful and service links

useful links:

https://password.kaspersky.com/it/

https://www.lastpass.com/it/features/password-generator

source of the links:

https://www.merchantfraudjournal.com/two-factor-authentication-work

https://www.aranzulla.it/computer/sicurezza-informatica

photos used in this e-book
https://blog.mistercredit.it/media/evabd4nk/cybersecurity-ransomware.jpg