**Logo, company name

Description automatically generated**

**Intellectual Output 1**



**HEALTH & SAFETY AT WORKPLACE:**

**CYBERSECURITY**

**INTRODUCTION**

From this unit you will learn what cybersecurity is, how to behave online in a wise manner and what are the five laws of cybersecurity

**DISCUSSION QUESTIONS**

Do you follow the cybersecurity guidelines? Have you or anyone you know ever been attacked by hackers? Do you know what to do in case of a hacker’s attack?

**READING**

Here is what Stephane Nappo - the Chief Information Security Officer at *OVHcloud* (a global hyper-scale cloud provider and leading European cloud alternative) says about cybersecurity:

*“Technology trust is a good thing, but control is a better one.”*

*“It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it.”*

*“The five most efficient cyber defenders are: Anticipation, Education, Detection, Reaction and Resilience.”*

Match the headings to the paragraphs.

**Cybercriminals don’t discriminate!** Never think “It won’t happen to me” or “I don’t visit strange websites”. No digital user is immune to hacking and there is no vaccine. Even the Facebook account might be taken over, not to mention the savings bank account. The [University of Maryland](https://www.umd.edu/) was one of the first to quantify the near-constant rate of hacker attacks of computers with Internet access— [every 39 seconds on average](https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds), affecting one in three Americans every year**.**

### Connect wisely! It is very tempting to connect your device to any free wi-fi available but weigh the consequences, especially when handling some sensitive information, doing the online banking or logging in a company email box.

### Use a secure password! It should consist of 16 elements or more, both letters, numbers, and characters. For obvious reasons it should not contain consecutive letters and numbers or any of the personal information that can be obtained in social media e.g. your pets’ names. This piece of advice is not elegant but the common saying goes: “Passwords are like underwear: don't let people see it, change it very often, and you shouldn't share it with strangers.”

### Secure your phone too! Use strong passwords and biometric features. Turn off the Bluetooth function if you’re not using it, don’t automatically connect to any public network.

### Think before you click! Be sure to inspect links and check if they are sent by a trusted person or institution. Think twice before downloading something of the unclear origin and function.

**Apply multi-factor authentication!** It is an additional measure to ensure your identity in case a hacker can guess your password. At least two pieces of evidence from different categories have to be provided: something the digital user knows, something they have or something they are.

**Beware of phishing scams!** The statistics claims that over 3 billion fake emails are sent daily. A hacker will pretend to be someone you know or the institution you are familiar with and will try to trick you into divulging important credentials, opening a malicious link or software that will infect your system with a virus.

**Look out for social engineering**! It is not only phishing but a much broader range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information. For instance, baiting promises the victim a reward.

**Update the software!** Don’t ignore the software update notifications even if you find them annoying and it requires rebooting your device. They are often issued in cases some security flaws have been discovered.

**Follow your digital footsteps!** Keep track of the websites you left your credit card numbers for faster payments. Delete the accounts you are no longer using and change the passwords regularly.

**Back-up the data!** Remember to save a back-up copy of the important data either on a physical location or on the cloud. Hackers are not always interested in stealing your data, sometimes they simply want to encrypt or erase it. Keeping a safe copy gives you an ultimate recovery tool.

**FURTHER PRACTICE**

Watch the TED talk:

[Nick Espinosa: The five laws of cybersecurity | Nick Espinosa | TEDxFondduLac | TED Talk](https://www.ted.com/talks/nick_espinosa_the_five_laws_of_cybersecurity)

Write down the Five Laws of Cybersecurity.

Law No.1 – If there is a vulnerability, it will be exploited. No exceptions.

Law No.2 – Everything is vulnerable in some way.

Law No.3 – Humans trust even if they shouldn’t.

Law No.4 – With innovation comes opportunity for exploitation.

Law No.5 – When in doubt, see Law No.1.

What example did the speaker give to support Law No.3? Why?

He asked the audience to look under their seats to find something he left for them. In this way he explained that people follow some absurd suggestions without thinking.