I think we should replace milk with something more useful and safe. First, we need to understand that people are not omnivorous; it is not surprising that nature thinks that a person should eat seasonal products in raw form. In natural conditions, people would be extremely fruit-eating. Thus, the healthiest fats are found in nuts and avocados, proteins in legumes (beans, lentils, seeds), and carbohydrates in vegetables, fruits, cereals, honey. And the milk itself can be replaced with coconut, rice, almond, oatmeal, nutty, pumpkin, poppy milk. If we talk about vitamin D, then it is in fish oil, which is also useful for Omega-3 fatty acids [1].

I hope that soon the real truth about milk will be known everywhere, because a large number of the population do not even suspect that milk can be harmful. I really sorry that the people complicate everything in this world, thereby make harm to themselves. For this reason, we need to strive for healthy nutrition, because it makes our immunity strong. All diseases go pass us, and our appearance makes us happy, because a healthy person is a happy person. We are what we consume.

References

1. 8 принципов питания, которые продлевают жизнь [Електронний ресурс] - Режим доступу: https://telegra.ph/8-principov-pitaniya-kotorye-prodlevayut-zhizn-12-27
2. Молоко. Будете здоровы? [Електронний ресурс] - Режим доступу: http://livelymeal.ru/moloko.html
3. Should humans drink cow’s milk? [Електронний ресурс] - Режим доступу: https://www.theguardian.com/lifeandstyle/2016/nov/21/should-humans-drink-cows-milk

УДК 004.771=111

INTERNET OF THINGS VULNERABILITIES AND PERSONAL DATA PROTECTION

Olenich D., 31 КН **e-mail: olenichvovk@gmail.com**
Zaitseva N.V., language adviser **e-mail: nataliia.zaitseva@tsatu.edu.ua**
Tavria State Agrotechnological University

Every year, Internet of Things is becoming more and more popular and accessible. Experts report on increasing number of Internet-connected home appliances. By 2020, their number will be from 25 billion (Gartner) to 50 billion (Ericsson) [1].

This study is an attempt to analyze the vulnerability of IoT devices and make some recommendations on what needs to be done to be more secure when using IoT and not become a victim of criminals skillful at hacking and social engineering.

Smart technology is actually surrounding people. They function in everyday life, in business and in industry: teapots, television sets, door locks, photo frames connected to the network – they are just the small elements of IoT. The IoT class of devices offers users a bright future with process automation, reduced material costs and time saving, but the introduced innovations add serious security problems and are still vulnerable to hackers.

Hewlett Packard Enterprise reviewed the 10 most popular devices on the Internet of Things, and the study report reveals an alarmingly high average number of vulnerabilities in devices [2]. Vulnerabilities are ranged from service faults to weak passwords for cross-site scripting. The analysis was carried out on IoT devices from manufacturers of televisions, remote power outlets, home thermostats, scales, webcams, home alarms, hubs for controlling multiple devices, controllers and automatic garage doors. Currently, the most of devices connect to cloud services that increase security risks. In addition, IoT devices imply the presence of mobile applications that can control gadgets remotely, which opens up new attack opportunities for hackers. According to the latest research 70% of the devices surveyed do not encrypt data during transmission between themselves and the Internet or local network, and the configuration can send this data on the Internet [3]. Almost every device also collects personal information such as name, address, birth data, medical information and credit card numbers. It is important that 80% of the devices studied have problems with passwords – they did not require passwords of sufficient complexity and length. According to the researchers, most devices, cloud services and mobile applications use too simple passwords, like “1234” or “123456”.

What is the danger of hacking the Internet of things? First of all, the presence of a large number of unprotected devices of the Internet of things, even with low computational power, makes them an easy prey for intruders. By exploiting vulnerabilities or simply taking advantage of the weakness of embedded security systems, hackers create large-scale botnets and use them for malicious activity, for example, to organize DDoS attacks [4].

Infected networks consisting of millions of hacked devices become a real menacing force, not only for business, but also for private users. If a device connects to the home network, control over which the attacker has obtained, most likely, this device not just supports DDoS attacks, but also collects a huge amount of information about its owner: steals personal information, passwords and bank data. Also, the attacker will be able to intercept the transmitted traffic, that is, every user’s web activity will be in plain sight.

Therefore, here are some tips for those who are thinking about purchasing smart technology or already own such a device:

- change default passwords immediately;
- install firmware updates timely;
- protect your routers by changing your password to a more complex one;
- purchase a smart-device only from reputable manufacturers who have experience in data and network security.

Modern technologies are in many ways ahead of our own perception and understanding of digital culture. Users still do not have the habit of protecting personal data not only on phones and computers, but also on other devices connected to the network. However, in the future, with the growing popularity and usability of Internet of Things, new security problems will arise that will need to be addressed simultaneously with developing modern infrastructure and device protection standards.

References

1. The Internet of Things [Електронний ресурс]. – Режим доступу: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/ iot_201602/

2. HP Internet of Things Study - July 2014 [Електронний ресурс]. – Режим доступу: https://www.scribd.com/document/235756737/HP-Internet-of-Things-Study-July-2014

3. HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack [Електронний ресурс]. – Режим доступу: http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676

4. Security Vulnerabilities of Internet-Connected Homes [Електронний ресурс]. – Режим доступу: https://resources.infosecinstitute.com/security-vulnerabilities-of-internet-connected-homes/

УДК 378.18=111

HOW TO MAKE MONEY WHILE BEING A STUDENT IN UKRAINE

Pliasetska V., 21МК **e-mail: plyasetsckaya.vicka@gmail.com**
Kravets O.O., language adviser **e-mail: el.kravets73@gmail.com**
Tavria State Agrotechnological University

Almost, every student faces the problem of lack of funds, even if he receives a scholarship, because its size is usually not sufficient to meet most needs. Especially, if the university, where the student is studying, is in another settlement, they have to live in a social behavior, buy food