



Justyna Żywiolek

Politechnika Częstochowska

Wydział Zarządzania

Katedra Inżynierii Produkcji i Bezpieczeństwa

al. Armii Krajowej 19 B, 42–200 Częstochowa

e-mail: justyna.zywiolek@wz.pcz.pl

CYBERSLACKING AND ANONYMITY IN THE NETWORK OF EMPLOYEES OF MANUFACTURING ENTERPRISES

Abstract. Computerization of companies, functioning in the information society with continuous access to the Internet is closely related to the use of the Internet by employees. A tool with such a large potential can certainly contribute to the improvement of the company's functioning, but it turns out that it also has a negative side. A factor that has a negative impact on small enterprises and large corporations is cybercrime, ie abuse of the network during business hours for private purposes. The article presents the results of a survey regarding the use of the Internet at work by employees and anonymity in the network.

Keywords: online anonymity, cyberslacking, internet usage at work.

CYBERSLACKING A ANONIMOWOŚĆ W SIECI PRACOWNIKÓW PRZEDSIĘBIORSTW PRODUKCYJNYCH

Streszczenie. Informatyzacja firm, funkcjonowanie w społeczeństwie informacyjnym z ciągłym dostępem do Internetu są ściśle związane z korzystaniem z Internetu przez pracowników. Narzędzie o tak dużym potencjale może z pewnością przyczynić się do poprawy funkcjonowania firmy, ale okazuje się, że posiada on także negatywną stronę. Czynnikiem mającym niekorzystny wpływ na małe przedsiębiorstwa i duże korporacje jest cyberprzestępstwo, tj. nadużywanie sieci w godzinach pracy do celów prywatnych. W artykule przedstawiono wyniki ankiety dotyczącej wykorzystania Internetu w pracy przez pracowników oraz anonimowości w sieci.

Słowa kluczowe: anonimowość w sieci, cyberslacking, wykorzystanie Internetu w pracy.

Introduction

The use of the Internet is noticeable in all enterprises. The size of the company and the industry is irrelevant. The network is a comprehensive information and knowledge centre that is so much needed in the company's operations. However, it turns out that most employees use the Internet for private purposes even during business hours. Abuse of the network is most often seen in areas such as visiting websites devoted to work and hobbies, searching for current information, planning holidays shopping or active participation in discussion forums and chat rooms. This phenomenon is called cyberslacking, it can be explained as the use of the Internet network by employees during work for private purposes. The problem of losing the sense of time and dropping it is not only related to the use of the Internet, but has a significant contribution to it [1]. The problem of losing valuable work time has existed for a long time, however, the dissemination of the Internet has caused a close linking of these problems. Until now, employees visibly avoided working by talking on the phone, extending coffee breaks or a cigarette. It is now easy to hide job abandonment because most employees use a computer or the Internet in their work [4]. A significant number of employers decide to purchase software to track employee activities on the Internet and even their e-mail and business mailboxes.

Cyberslacking

In order to investigate the phenomenon of using the Internet and convince employees about their anonymity in the network, a research survey was conducted, as well as an interview with senior management in 365 enterprises of various sizes (from micro to medium) in various industries located in the Silesian Voivodeship. The research was to prove where these phenomena occur commonly and how they affect the functioning of the company.

Among employees, as many as 76% of respondents have higher education, 12% average, 11% bachelor and 2% post-secondary education. The subjects have prestigious professions. In the first question, the respondents answered questions about their profession and indicated the form of their employment.

The results of the study clearly indicate that 78% of owners and presidents of companies admit that they use the Internet for private purposes. Most often those sitting on these positions feel impunity, instead of fulfilling their duties, they deal with the implementation of private goals. The second group of Internet abusers at work are IT specialists and programmers. This professional group has the owners' trust, it is they who control the remaining employees, but they themselves remain without control and supervision.

The next question concerned the identification of the industry in which the respondents are employed (Figure 2).

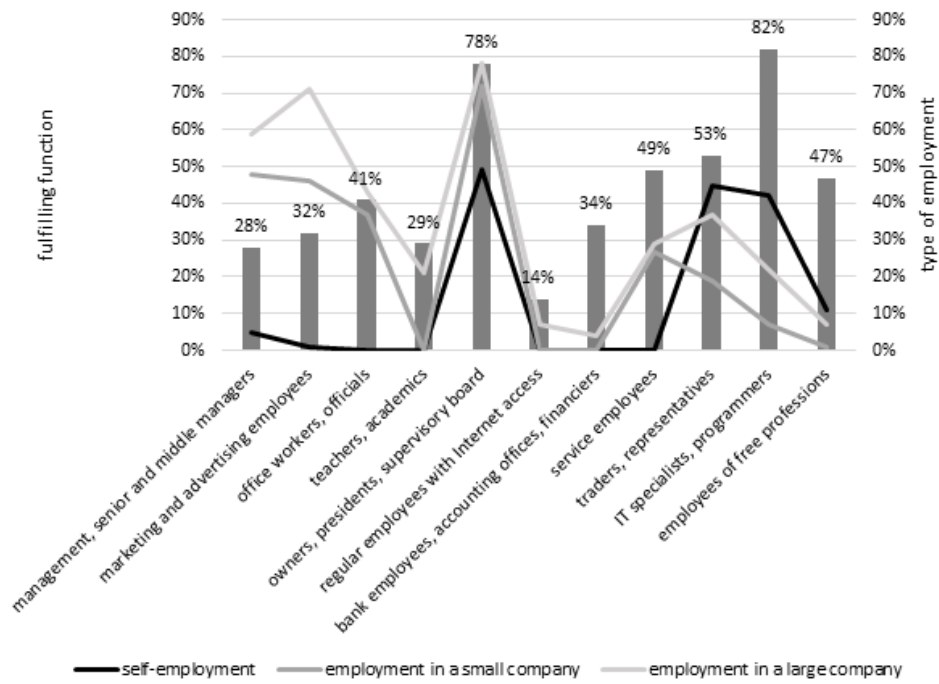


Fig. 1. Occupation and form of employment of the respondents
Source: Own study.

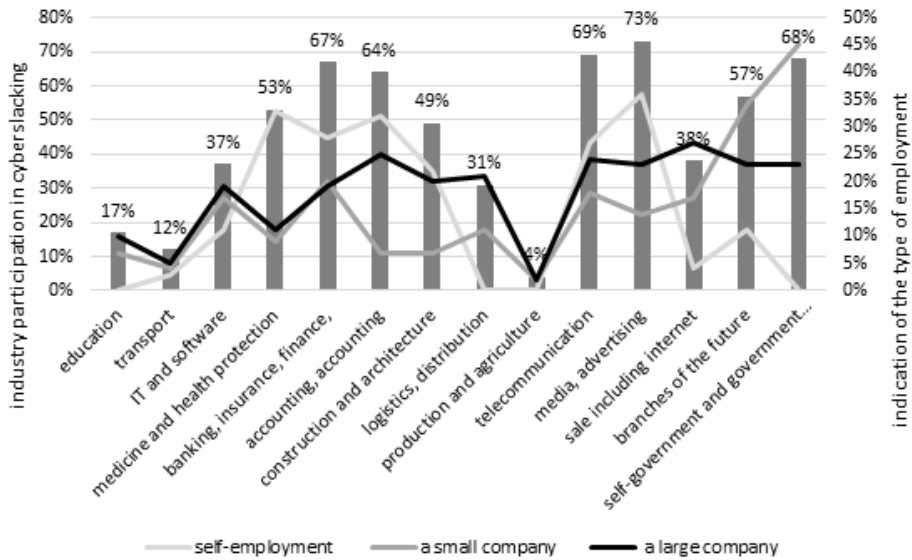


Fig. 2. Industry and form of employment of the respondents
Source: Own study.

The results of the survey indicate that the industry associated with media and advertising is particularly exposed to the phenomenon of cyberslacking, but 69% telecommunications and 68% self-governments were also ranked the highest, while the smallest rates are recorded in the production and agricultural profile.

Employees gave the information about their use of the Board for private purposes at work without much resistance. They also do not think that they do something bad, as shown in Figure 3.

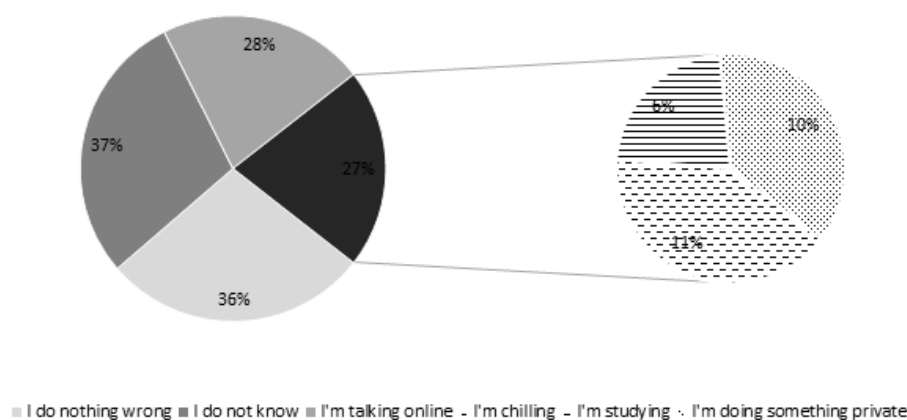


Fig. 3. Declaration of respondents on using the Internet
Source: Own study.

The respondents indicate that they are aware of carrying out activities against the employer. However, in most cases, they describe it as a temporary relaxation, training as reading information on internet portals. Employees believe that their activities are anonymous in the network.

Anonymity in the network

Anonymity is treated as the impossibility of identification in the network [5]. The word anonymity derives from the Greek word "anonymia", which was translated as "namelessness" [9]. Currently, this concept is defined as the inability to identify a given person's identity among other members of a given community [3]. Anonymity can be understood in many different aspects, also in terms of the web. The Internet, that is the generally available, global computer network is treated by many of its users as a tool ensuring some anonymity. The mechanisms of the Internet seem simple, especially for people who are unaware of the complexity of the network and are unaware of its threats [6]. The assump-

tion that the Internet gives a sense of anonymity is wrong, because every action taken, for example, browsing the pages, sending various information, setting up e-mail accounts everyone leaves a "trace" [8]. Left 'traces' make identification easier because each computer has an IP address (Eng. Internet Protocol).

There are more and more reasons why people want to remain anonymous on the Internet. By hiding IP, computer users try to avoid [2]:

- the blockade established by a given web server that reserves the right to use and access its resources to specific people,
- recognizing the sender of the message or email,
- tracing people in the network that use the computer for illegal purposes.

Employees take actions on their own, which they think help with remaining anonymous on the Internet (Figure 4).

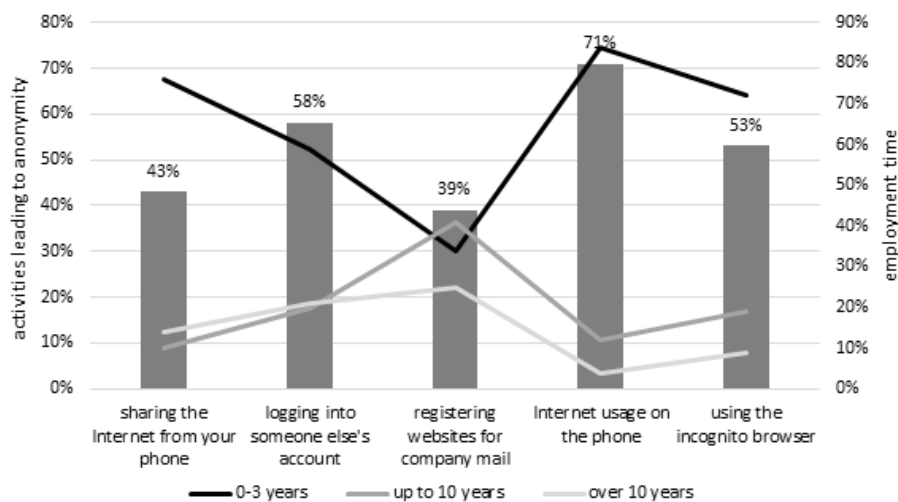


Fig. 4. Actions taken by employees to ensure their anonymity on the Internet, taking into account the time of employment

Source: Own study.

Employees of the surveyed companies believe that using the Internet on the phone or logging in to a coworker's account is the best way to anonymity on the Internet. Providing passwords is widespread, it causes difficulties in verifying the actions taken by employees. Employees employed in the company for up to three years also practice registering shopping websites for corporate e-mail. Private shopping takes up a lot of time at work, registration of shopping websites is to eliminate verification of logins to private mail, which, according to employees, gives them anonymity of activities on the Internet [7]. Newly employed people use the Internet with smartphones. Employees working for

more than 10 years rarely use smartphones, but they are happy to register shopping portals on a formal mailbox.

Employees should apply certain activities to remain anonymous, by creating certain behaviours among employees, a certain level of anonymity can be maintained, which provides the enterprise and its employees with security against industrial espionage, presented in Figure 5.

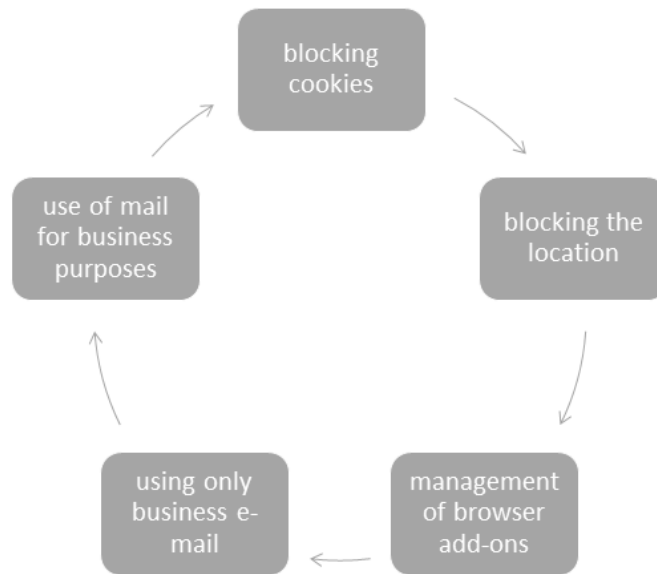


Fig. 5. Activities aimed at maintaining "healthy" anonymity on the Internet
Source: Own study.

Keeping the "healthy" anonymity on the Internet by following the rules described in Figure 5 will ensure the security of the company and its employees, but also reduces the emerging phenomenon of cyberslacking in the company.

Summary

The aim of the article was to show the threats arising with the development of technology enabling the use of the Internet at work. The dynamic development of these tools has facilitated illegal activity on the web. However, it is worth remembering that these methods were not intended to be used for illegal activities, but for the safety of users and enterprises on the Internet. The article is only preliminary research, showing in which industries and professions the phenomenon of cyber-caching threatens the functioning of the enterprise. The phenomenon of using the Internet at work is so common that employers try

to protect themselves from it using, for example, programs tracking employees' activities on the Internet. The methods of preventing the phenomenon of cyberslacking constitute the next stage of research.

Literature

- [1] Nowak M., Cybernetyczne przestępstwa – definicje i przepisy prawne, <http://www.ebib.pl/2010/113/a.php?nowak> (14.04.2018)
- [2] Podraza, P. Potakowski, K. Wiak, Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna, Difin, Warszawa, 2013, s. 278 r.
- [3] Weber R. H., Heinrich U. I., Anonymization, Springer, 2012, s. 1, books.google.com/books?isbn=1447140664 (10.04.2018)
- [4] <https://www.hacking.pl/prosty-sposob-na-anonimowosc-w-internecie/>
- [5] Mitnick K., Vamosi R., Niewidzialny w sieci. Sztuka zacierania śladów, Wydawnictwo Pascal, Warszawa, 2017.
- [6] Sokół R., Jak pozostać anonimowym w sieci, Helion, Gliwice, 2015.
- [7] Żywiołek J. Międzyorganizacyjna wymiana informacji jako element zagrożenia bezpieczeństwa informacji [in:] Systemy bezpieczeństwa w podmiotach gospodarczych, Oficyna Wydawnicza Stowarzyszenia Menedżerów Jakości i Produkcji, Częstochowa, 2016, p. 78.
- [8] Żywiołek J., Zarządzanie wiedzą o systemie bezpieczeństwa i higieny pracy w przedsiębiorstwie, [in:] Światowy Dzień Bezpieczeństwa i Ochrony Zdrowia w Pracy 2017, Częstochowa, 2017, p. 114.
- [9] Liderman K., Bezpieczeństwo informacyjne, PWN, Warszawa, 2012, p. 163.