Joanna Zarębska
ORCID: 0000-0002-1655-3086
j.zarebska@wez.uz.zgora.pl
Uniwersytet Zielonogórski

Natalia Howis
howisn@gmail.com
Uniwersytet Zielonogórski

https://doi.org/10.26366/PTE.ZG.2023.235

Cytowanie: Zarębska, J.; Howis N. (2023). Świadomość zagrożenia i zachowania pokolenia Z wobec cyberbezpieczeństwa oraz oszustw w życiu codziennym – studium przypadku. *Zeszyty Naukowe Polskiego Towarzystwa Ekonomicznego w Zielonej Górze*, 18, s. 41-53. DOI: 10.26366/PTE.ZG.2023.235

Świadomość zagrożenia i zachowania pokolenia Z wobec cyberbezpieczeństwa oraz oszustw w życiu codziennym – studium przypadku

Abstrakt: Dzisiejsze młode pokolenie (urodzone po 1995 roku) nazywane generacją Z, posiada umiejętności obsługi różnego rodzaju urządzeń elektronicznych i potrafi poruszać się w świecie cyberprzestrzeni. Obecni uczniowie szkół średnich i wyższych czują się w tym świecie pewnie, bezpiecznie i nie boją się nowinek technologii informatycznych. Mimo ewidentnych korzyści, świat ten niesie ze sobą także różne niebezpieczeństwa. Charakteryzuje się anonimowością i globalnym zasięgiem, co może sprzyjać zagrożeniom. Brak edukacji w tym zakresie i zbytnia pewność siebie młodych ludzi, a często pośpiech, mogą doprowadzić w życiu osobistym czy przyszłej pracy zawodowej do poważnych konsekwencji (np. kradzieży danych). W artykule zaprezentowano wyniki badania ankietowego przeprowadzonego wśród studentów Wydziału Ekonomii i Zarządzania, a dotyczącego ich świadomości na temat cyberbezpieczeństwa, zagrożeń z nim związanych, postaw wobec zagrożeń oraz sposobów uzyskiwania wiedzy na temat zabezpieczenia się przed oszustami w sieci. Wyniki badania wskazują na dużą świadomość młodego pokolenia w zakresie bezpieczeństwa technologii informatycznych, o czym świadczy wysoka popularność stosowania zabezpieczeń antywirusowych (przez 81,5% ankietowanych). Odpowiedzi studentów wskazują na potrzebę ciągłego, dalszego kształcenia w zakresie cyberbezpieczeństwa, ale również na konieczność uświadamiania szerszej grupie społeczeństwa o niebezpieczeństwie, jakie ich może spotkać ze strony oszustów, hakerów komputerowych oraz o ostrożnym korzystaniu z nowinek technologicznych.
Słowa kluczowe: edukacja; pokolenie Z; oszustwa internetowe; kompetencje cyfrowe

Awareness and behavior of Generation Z toward cyber-security and fraud in everyday life – a case study

Abstract: Today's young generation (born after 1995), referred to as Generation Z, is skilled in the use of various types of electronic devices and are able to navigate the world of cyberspace. Today's secondary and tertiary school students feel confident, safe and unafraid of new developments in this world and are not afraid of new information technologies. Despite obvious advantages, this world also entails various dangers. It is characterised by anonymity and global reach, which can foster risks. A lack of education in this area and the overconfidence of young people, often in a hurry, can lead to serious consequences in their personal lives and future professional careers (e.g. theft of data) consequences. The article presents the results of a survey of students of the Faculty of Economics and Management on their awareness of cyber security, on their awareness of cyber security, the risks associated with it, attitudes towards threats, and ways of acquiring knowledge about how to protect themselves against online fraudsters. The results of the survey indicate a high awareness among the younger generation of in terms of IT security, as evidenced by the high popularity of use of antivirus protection (by 81.5% of

respondents). Responses of students indicate the need for continuous, further education on cyber security, but also the need to make the broader public aware of the public about the dangers they may face from fraudsters, computer hackers and about the careful use of technological innovations.
Keywords: education; generation Z; online fraud; digital competence

JEL: I25, O33, P46

Wstęp

Obecnie wyróżniamy co najmniej kilka generacji, które w literaturze próbuje się scharakteryzować w bardziej lub mniej dokładny sposób. Charakterystyka ta nie jest ujednolicona, gdyż naukowcy często stosują różne nazewnictwo, okresy czasowe narodzin osób zaliczanych do poszczególnych grup i przypisują im różne lub czasami te same cechy. Charakterystyka generacji jest bardzo ważna i przydatna szczególnie dla pracodawców, którzy w swoich firmach zatrudniają osoby z różnych pokoleń, a czasami specjalnie wybierają pracowników z jednego pokolenia o szczególnych umiejętnościach lub cechach osobowościowych. W literaturze najczęściej wymieniane generacje to (Mazur-Wierzbicka, 2015, s. 307; Boruta-Gojny, Popiołek, 2014; Gadomska-Lila, 2017; Prokopowicz, 2017; Wiktorowicz, Warwas, 2016; Wasiluk, Bańkowska 2021, ss. 138-159; Karasek 2022, ss. 209-218): Radio Babies (osoby urodzone w latach 1922-1944); Baby Boomers (osoby urodzone w latach 1945-1964); X (osoby urodzone w latach 1965-1979); Y (osoby urodzone w latach 1980-1994) oraz Z (osoby urodzone po 1995 roku).

Dzisiejsze młode pokolenie (uczniowie szkół średnich i wyższych) – nazywane generacją Z – to osoby określane jako post-milenialsi lub pokolenie C (od ang. connect, communicate, change). Uważane jest za pierwszą generację osób dorastających w społeczeństwie w pełni scyfryzowanym, dlatego też zakłada się, że posiada ono pewien poziom obycia z nowoczesnym sprzętem komputerowym. Nie mają problemów z lękiem przed nowinkami technologii informatycznych i czują się dobrze w ich otoczeniu (wręcz nie wyobrażają sobie życia bez nich). Nie znają życia bez Internetu i social mediów. Są otwarci i twórczy, ale niełatwo przychodzi im skupienie uwagi na jednym zadaniu. Można to szczególnie zaobserwować na ulicach, w kawiarniach czy zajęciach w szkole. W literaturze wymieniane są ich główne cechy: mobilność, szybka reakcja na zmiany i realistyczne podejście do życia. Generalnie jednak ocenia się ich dość krytycznie i traktuje z dużą nieufnością (podobnie jak kiedyś tzw. „*dzieci Neostrady*"). Przypisuje się im takie cechy jak: roszczeniowość, trudność z logicznym myśleniem, brak kompetencji, pośpiech, trudność z komunikowaniem się z innymi, a czasem

nawet brak autorytetów, dyscypliny i lojalności (Wasiluk, Bańkowska 2021, ss. 138-159; Karasek 2022, ss. 209-218).

Wymienione cechy, charakteryzujące młode pokolenie, mają duże znaczenie w szkole czy w pracy – potencjalnie tym większe, im bardziej są one związane z wykorzystywaniem różnych nowinek technologii informatycznych. W dzisiejszym świecie w przedsiębiorstwach spotykają się przedstawiciele czterech pokoleń, które z uwagi na odmienne warunki dojrzewania, reprezentują różne sposoby myślenia, zachowania i podejścia do pracy.

Celem artykułu jest zaprezentowanie wyników badań ankietowych, przeprowadzonych wśród wybranej grupy studentów, a dotyczących oceny ich świadomości na temat bezpieczeństwa technologii informatycznych, zagrożeń z nią związanych oraz sposobu uzyskiwania wiedzy na jej temat. Wyniki badania mogą mieć praktyczne zastosowanie dla uczelni czy służb z zakresu cyberbezpieczeństwa, jako źródło informacji na temat ogólnej wiedzy studentów w analizowanym zakresie, co może świadczyć o brakach i/lub właściwych kierunkach edukacji w omawianym temacie.

Bezpieczeństwo a nowoczesne technologie informatyczne

Jedną z egzystencjalnych potrzeb człowieka jest potrzeba bezpieczeństwa. Według Abrahama Maslowa znajduje się ona na drugim poziomie hierarchii i odnosi się do wartości, które dotyczą bezpieczeństwa i stabilności życia człowieka, np. bezpieczeństwo zatrudnienia, stałe dochody, zdrowie, spokój, zasoby, bezpieczeństwo moralne i rodzinne oraz bezpieczeństwo własności prywatnej (Maslow, 2022).

Świat się rozwija coraz szybciej, a wraz z nim rozwija się cyfryzacja. Unowocześniany jest każdy aspekt ludzkiego życia. Według Raportu Digital Poland z 2022 roku, w Polsce występuje bardzo niski wskaźnik cyfryzacji wynoszący ok. 40% (średnia UE to 50%). Polska w 2021 roku na 27 krajów Unii Europejskiej zajmowała 24. miejsce w The Digital Economy and Society Index (DESI) uwzględniającym w zakresie cyfryzacji 4 filary: kapitał ludzki, łączność, integrację technologii cyfrowych i cyfrowe usługi publiczne, e-administrację. W ogólnym wniosku sformułowanym w raporcie, w odniesieniu do naszego kraju stwierdza się, że „Polacy nadal nie posiadają kompetencji cyfrowych, a małe i średnie firmy nie wykorzystują masowo najnowszych technologii. Podjęto szereg działań na szczeblu krajowym, jednak nadal wiele z nich nie zrealizowano" (Raport Digital Poland, 2022). Pomimo to, Polacy wykazują pozytywne nastawienie do zmian. Widzą w nich ułatwianie codziennego życia, zmniejszanie nierówności społecznych zależnych od miejsca zamieszkania i zwiększanie możliwości znalezienia lepszej pracy na rynku. Proces cyfryzacji definitywnie zmienił rynek usług –

wpłynął na wiele decyzji sektora publicznego i prywatnego (Chądrzyński i in., 2021; Załoga, 2022, s. 544).

Cyfryzacja znacząco ułatwia dostęp do usług medycznych, finansowych czy edukacyjnych. Przykładem mogą być portale: "pacjent.gov.pl" czy "znanylekarz.pl", dzięki którym można umówić wizytę do lekarza, mieć dostęp do historii leczenia oraz dostać e-receptę w kilku szybkich krokach. Za pomocą portalu "ePUAP" można załatwić sprawy urzędowe z każdym organem administracyjnym w Polsce, który udostępnia taką usługę. Duże banki wykorzystują aplikacje, służące do różnego rodzaju płatności internetowych (płatności BLIK, na telefon) i innych usług finansowych (Balibok, Matras, 2014). Prawidłowe korzystanie z cyfrowych rozwiązań przez szkoły czy przedszkola może skutkować lepszymi wynikami edukacyjnymi, m.in. rozwija kreatywność indywidualną oraz grupową, zapewnia holistyczny rozwój oraz zmniejsza nierówności społeczne (Plebańska, Tarkowski, 2016). W przypadku szkolnictwa dzięki cyfryzacji możliwy jest kontakt ucznia/studenta z prowadzącymi zajęcia (e-mail, rozmowa bezpośrednia na Meet), biurami obsługi studenta (BOS), biblioteką (zamawianie książek, dostęp do elektronicznych zasobów bibliotecznych) oraz bezpośredni dostęp do ocen (dziennik elektroniczny, e-indeks), itp. Dzięki cyfryzacji szkolnictwa możliwe było prowadzenie zajęć edukacyjnych w czasie trwania pandemii Covid-19.

Zachowania konsumenckie od wielu lat wspierają sprzedaż online, począwszy od zakupów spożywczych po lekarstwa, kosmetyki, meble czy ubrania (Chojnacka, Zarębska, 2022; Rudnicka, Koszewska, 2020; Morawski, 2021, ss. 241-257). Często przy zarejestrowaniu się do newslettera otrzymujemy na skrzynkę e-mailową zniżkę na zakupy w danym sklepie, nowe propozycje usług/zakupów, wiadomości o rabatach i wyprzedażach. Jest to praktyka zachęcająca do zakupów na danej platformie.

Korzystanie z technologii i systemów informatycznych to również zagrożenie. W Ustawie z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (art. 2) definiowano cyberbezpieczeństwo jako „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy" (Ustawa 2018a). W Polsce nad danymi obywateli czuwa Departament Zarządzania Systemami (2023), do którego zadań należy nadzór nad systemami teleinformatycznymi (Ustawa 2018b). Prawną opiekę nad danymi, sposobem ich zbierania jak i rozwiązaniami, w jaki sposób je można wykorzystywać zajmuje się Departament Zarządzania Danymi (2023).

W związku z rosnącym poziomem cyfryzacji w Polsce znacząco wzrosła liczba przestępstw popełnianych na odległość za pomocą systemów teleinformatycznych (w 2020

roku odnotowano 10 420 incydentów – 73% dotyczyło phishingu, a w 2021 roku odnotowano 22 575 zdarzeń – 76% dotyczyło phishingu, czyli wyłudzaniu danych i/lub pieniędzy przez podszywanie się pod wymyśloną stronę www) (Raport CERT, 2020, s. 13; Raport CERT, 2021, s. 12).

Jeszcze do niedawna jedną z popularniejszych metod oszustów był tzw. „keylogger" (Trejderowski, 2013), który w 2022 roku można by wręcz uznać za „przestarzały". Keylogger jest to typ programu lub urządzenia rejestrującego przyciski klawiszy. Dziś każdy użytkownik Internetu może bez wysiłku kupić online keylogger w formie pendrive, który tak długo jak jest podłączony do urządzenia, tak długo rejestruje działania. Program ten może w rzeczywistym czasie pokazywać, co ktoś pisze na klawiaturze (np. hasła dostępu do banku, poczty elektronicznej).

Z pewnością sukcesem jest wysoka świadomość społeczeństwa w zakresie natychmiastowej reakcji w przypadku zgubienia dokumentów (dowód osobisty, paszport i inne zawierające wrażliwe informacje jak PESEL) (Kondek, Ożarowska, 2022a). Z Raportu Związku Banków Polskich i Komendy Głównej Policji (KGP) wynika, iż zdecydowanie z każdym rokiem maleje liczba prób posługiwania się czyimś dokumentem bądź podrabiania dokumentów. Dzięki temu w 2021 roku zdołano udaremnić w Polsce wzięcie nielegalne 7885 kredytów na łączną kwotę 245,2 mln PLN (Kondek, Ożarowska, 2022b). Niestety z danych KGP wynika, iż w 2021 roku nie było województwa w Polsce, w którym nie doszłoby do oszustw metodami „na wnuczka" i „na policjanta". Co najmniej 1176 starszych osób straciło oszczędności życia w pierwszym półroczu 2021 roku, a straty wyniosły ponad 63 mln PLN (http://bip.kgp.policja.gov.pl).

Jedną z form oszustw jest podszywanie się pod pracowników zaufania publicznego. Bezpośrednio przed drzwiami mieszkania pojawiają się osoby w strojach policjantów bądź pracowników spółdzielni mieszkaniowej. Ten rodzaj oszustwa w wyniku cyfryzacji przerodził się również w phishing. (Trejderowski 2013). O wiele częściej oszuści używają negatywnego przekazu, wywołania u odbiorcy poczucia lęku co sprawi, że zamiast zastanowienia się – kliknie w podany na ekranie link. Wywołuje się te uczucie wysyłając odbiorcy informację o próbie oszustwa, niezapłaceniu za zakup, nie dotarciu przelewu. Użytkownik klika w link, który przekierowuje go do strony identycznej jak strona oryginalna, wpisuje swoje dane (np. dane bankowe) i w ten sposób robi przelew dla oszusta. Ta sama metoda jest używana telefonicznie, tj. dostajemy "telefon od banku", iż wykryto podejrzany przelew czy zablokowano nam konto, wobec czego "pracownik banku" prosi nas o podanie hasła bądź

PIN-u do karty w celu potwierdzenia tożsamości. Taka sytuacja realnie nigdy nie będzie miała miejsca – bank nigdy nie poprosi nas o podanie haseł.

Do Policji spływają bardzo często zgłoszenia oszustw „na BLIK", sms „zapłać za paczkę". Departament Cyberbezpieczeństwa w Polsce zajmuje się kreowaniem i wdrażaniem strategii ds. ochrony w cyberprzestrzeni, a także bezpośrednio nadzoruje Krajowy System Cyberbezpieczeństwa, który od 2018 roku zapewnia ochronę usług cyfrowych i nadzoruje osiągnięcie wysokiego poziomu bezpieczeństwa systemów teleinformatycznych. Na koniec 2021 roku zostało powołane Centralne Biuro Zwalczania Cyberprzestępczości. Do jego nadrzędnych zadań należy wykrywanie, zwalczanie i przeciwdziałanie przestępstwom w sieci teleinformatycznej (https://cbzc.policja.gov.pl).

Kolejnym problemem jest datafikacja, czyli codzienne umieszczanie w Internecie coraz większej ilości danych (Chądrzyński i in., 2021). Są to dane typu: od systemów informatycznych, indywidualnych, biznesowych i instytucjonalnych użytkowników, do baz danych firm prywatnych i instytucji. Warto wspomnieć, że w Internecie nic nie jest za darmo. Podając numer telefonu, nasz email, "płacimy" naszymi danymi, które są umieszczane i wykorzystywane w różnych bazach. Warto pamiętać, iż znaczącą ilość informacji umieszczamy my sami. Dzięki takim portalom jak Facebook, Linkedin, Instagram możemy dowiedzieć się np. jak przebiegała edukacja użytkownika, gdzie obecnie pracuje, jaki jest jego nr telefonu czy adres email oraz gdzie obecnie się znajduje? Złodziej już nie musi czekać na okazję pod domem, obserwować mieszkanie tygodniami by poznać plan dnia, wystarczy odwiedzić profile internetowe. Warto wspomnieć, iż sami często sprowadzamy zagrożenie na siebie całkowicie nieumyślnie (Balibok, Matras, 2014). Do takich zachowań należy przekazywanie uprawnień do dostępu innej osobie, ustawianie hasła o słabej mocy i niezmienianie go, ignorowanie zasad bezpieczeństwa, np. kontroli dostępu w budynkach. Tworzenie silnych, skomplikowanych haseł irytuje użytkowników. Największym błędem jest tworzenie hasła, które używamy do wielu stron logowania oraz tworzenie hasła łatwego z użyciem informacji, które łatwo o nas wyszukać (jak na przykład imiona dzieci, zwierząt czy data urodzenia) (Sajler-Fudro, 2022). Za pomocą tych informacji wystarczy użyć łamacza haseł (np. John The Ripper) dostępnego w Internecie za darmo.

Dzisiejsze telefony komórkowe zawierają możliwości płatnicze z użyciem aplikacji dzięki technologii NFC (near field communication) lub dzięki wbudowanej przenośnej karcie płatniczej RFID (radio frequency identification). Ciekawym, jednym ze współcześniejszych typów oszustw jest neurohakerstwo (Kotz i in., 2015). Polega ono na zdalnym zhakowaniu urządzeń niezbędnych dla pacjenta do życia, jak na przykład pompa insulinowa bądź rozrusznik

serca. Urządzenia te zbierają wrażliwe dane o pacjencie i z łatwością mogą stać się przedmiotem przestępstwa (np. wymuszenie od pacjenta danych do karty bankomatowej z zagrożeniem wyłączenia urządzenia lub podaniem wysokiej dawki insuliny zagrażającej życiu). Jednocześnie może ono być przydatne w przypadku chęci wprowadzenia instytucji Policji w błąd lub też zniszczenia dowodów w postaci wyłączenia, zablokowania dostępu do urządzenia lub też zmienienia danych w nim zapisanych.

Materiały i metodyka badań

Przeprowadzone badania składały się z trzech części. Pierwsza część badań polegała na analizie literatury przedmiotu. Systematyczny przegląd literatury przedmiotu oraz krytyczna analiza treści wybranych publikacji pozwoliły na zidentyfikowanie problemu i luki badawczej. Dodatkowym wsparciem w zidentyfikowaniu problemu i formułowaniu pytań był wywiad bezpośredni (druga część badań) z przedstawicielką Komendy Miejskiej Policji w Zielonej Górze. Jej długoletnie doświadczenie zawodowe i codzienne problemy z cyberprzestępczością były bardzo pomocne w sformułowaniu pytań i wyborze grupy badawczej.

W trzeciej części badania sformułowano pytania ankietowe oraz przeprowadzono ankietę internetową (CAWI – Computer-Assisted Web Interview) wśród studentów wybranych kierunków Wydziału Ekonomii i Zarządzania Uniwersytetu Zielonogórskiego (WEZ UZ). Podstawą badania był kwestionariusz ankiety zawierający jedenaście pytań otwartych i zamkniętych jednokrotnego oraz wielokrotnego wyboru.

Kwestionariusze ankietowe rozesłano do ponad 300 studentów, którzy wypełniali je w okresie od stycznia do marca 2023 roku. Uzyskano zwrotność na poziomie 60% (180 wypełnionych ankiet). Zastosowano celowy dobór grupy. Respondenci byli słuchaczami studiów wyższych Wydziału Ekonomii i Zarządzania Uniwersytetu Zielonogórskiego (kierunki: zarządzanie pierwszego stopnia i logistyka pierwszego stopnia; słuchacze studiów stacjonarnych i niestacjonarnych) i pochodzili z różnych miast. Do badań przystąpiło 65,6% kobiet, 33,3% mężczyzn oraz 1,1%, które nie zadeklarowały swojej płci. Ponieważ badanie było przeprowadzane w krótkim czasie i większość respondentów to studenci WEZ UZ, nie należy odnosić go do całej populacji młodych Polaków, lecz do reprezentantów konkretnej grupy.

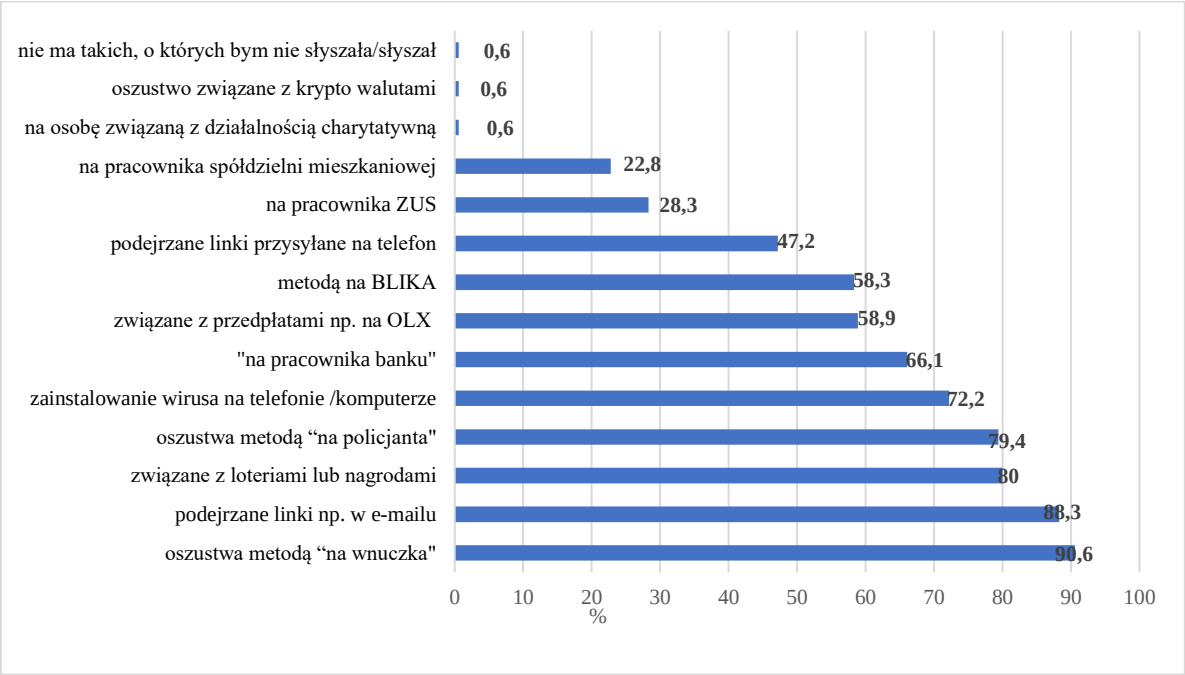
Wyniki badań

Badanie ankietowe przeprowadzone w 2023 roku wypełnili studenci pochodzący głównie z województwa lubuskiego – 122 osoby, ale byli również z województw: dolnośląskiego – 39 osób, wielkopolskiego – 10 osób, zachodniopomorskiego – 6 osób, śląskiego – 3 osoby. Wśród 180 studentów 65 było z kierunku zarządzanie, a pozostali z kierunku logistyka. Większość ankietowanych mieszka na wsi (30,0%), prawie tyle samo osób mieszka w małych miastach do 50 tys. mieszkańców (28,9%), na trzecim miejscu – 22,8% są studenci mieszkający w miastach średniej wielkości (100-500 tys. mieszkańców), 9,4% to mieszkańcy dużych miast (powyżej 500 tys. mieszkańców), a 8,9% to mieszkańcy miast o liczbie mieszkańców pomiędzy 50-100 tys. Ponad połowa ankietowanych to studenci pierwszego i drugiego roku studiów, czyli do 21 lat (43,3%), pomiędzy 22 a 25 rokiem życia było 40,6% ankietowanych, a pozostali to osoby powyżej 26 roku życia (16,1%). Osoby powyżej 26 roku życia to ankietowani ze studiów niestacjonarnych (zaliczani do pokolenia Y lub Z), którzy zostali wzięci pod uwagę w badaniu z uwagi na brak jednoznaczności w definicji pokoleń i celowy wybór grupy badawczej.

Wielu studentów miało do czynienia z oszustwami – jako faktyczne (26,1%) lub potencjalne (28,3%) ofiary. W sumie stanowili oni 54,4% badanych. Pozostali studenci twierdzą, że nie byli ofiarami oszustw (24,4%) lub nie pamiętają, aby ktoś usiłował ich oszukać (21,2%). Z grupy ankietowanych 180 studentów, 70,6% z nich odpowiedziało, że zna osoby, które były ofiarą oszustów (najczęściej ktoś z rodziny lub znajomych). Na uwagę zasługuje fakt, że w kolejnym pytaniu 70,6% studentów odpowiedziało, że mieli do czynienia z SMS-ami o nieopłaconej przesyłce lub z telefonami z banku dotyczącymi wzięcia kredytu. Porównując je z wcześniejszymi odpowiedziami (czy badani mieli do czynienia z oszustwami lub byli ich ofiarami) widać wyraźnie, iż pewna grupa ankietowanych usuwa zbędne sms-y, prawdopodobnie nawet nie traktując ich jako próbę oszustwa lub włamania się do danych telefonu.

Ponadto jak wynika z zestawienia na rysunku 1., większość studentów słyszała o oszustwach metodą „na wnuczka" (90,6%), „na policjanta" (79,4%), również dostawali podejrzane linki np. w e-mailu (88,3%), związane z loteriami lub nagrodami (80,0%), poprzez zainstalowanie wirusa (72,2%), podszywających się pod pracownika banku (66,1%), związane z przedpłatami np. na OLX (58,9%), metodą na BLIKA (58,3%), podejrzane linki przysyłane na telefon (47,2%), podszywających się pod pracownika ZUS (28,3%), podszywających się pod pracownika spółdzielni mieszkaniowej (22,8%), oraz pojedyncze próby wyłudzenia

danych/pieniędzy przez osobę podszywającą się pod osobę związaną z działalnością charytatywną lub związaną z krypto walutami.



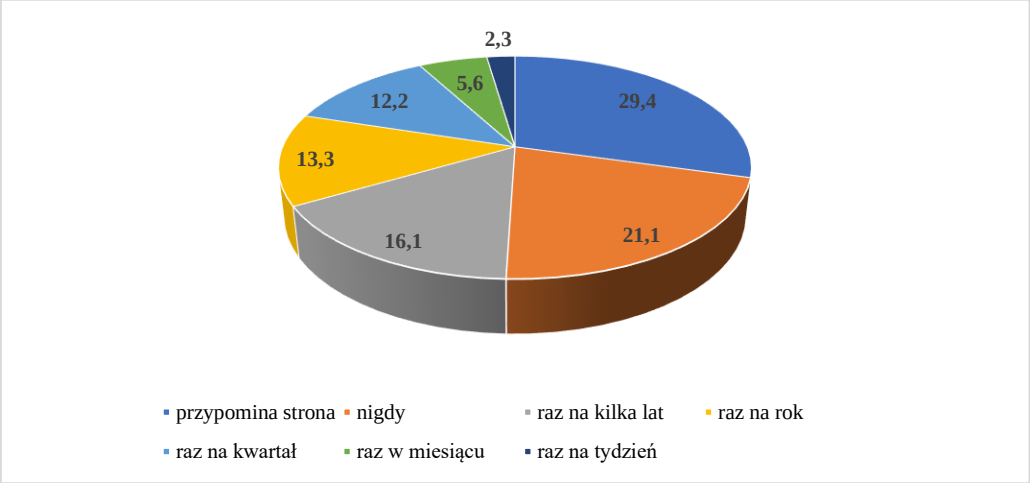
Rysunek 1. Rodzaje oszustw, o których słyszeli ankietowani studenci (n = 180)
Źródło: opracowanie własne.

Studenci pozyskują informacje na temat przeciwdziałania oszustwom najczęściej z Internetu (87,8%), od znajomych i rodziny (66,1%), z telewizji (45,6%), ze strony banku (40,6%), ze szkoły/uczelni (32,2%), ze stron urzędowych np. Policji (29,4%), z radia (28,3%), z prasy (15%).

Studenci zostali poproszeni o zaznaczenie odpowiedzi związanych z urządzeniami, do których przejawiają największe zaufanie podczas dokonywania transakcji finansowych. Największe zaufanie studenci mają do płatności za pomocą komputera/laptopa (35% osób zaznaczyło odpowiedź bardzo duże i duże poczucie bezpieczeństwa; 20% – średnie), podobne do płatności blikiem (32% – bardzo duże i duże; 21% – średnie), płatności za pomocą telefonu (analogicznie 27% i 21%), a najmniejsze zaufanie do płatności za pomocą tabletu (13% i 26%) i zegarka (11% i 19%).

Komputer/laptop budzą największe zaufanie i poczucie bezpieczeństwa wśród studentów. Wynika to z faktu, że 81,5% posiada na tych urządzeniach zainstalowany program antywirusowy. Tylko 48,7% studentów ma zainstalowany program antywirusowy na telefonie. Brak odpowiedniego zabezpieczenia przed wirusami na pewno jest przyczyną braku zaufania do dokonywania płatności innymi urządzeniami (tablet, zegarek).

Ważnym elementem, o którym przypominają nam strony bankowe lub aplikacje jest częsta zmiana haseł o odpowiedniej liczbie skomplikowanych znaków. Jest to również ważny czynnik poczucia bezpieczeństwa w korzystaniu ze współczesnych urządzeń. Jak się okazuje 29,4% studentów zmienia hasło w momencie jak mu o tym przypomina strona, na której jest zalogowany. Niepokojący jest fakt, że 21,1% studentów wcale nie zmienia hasła, a 16,1% robi to raz na kilka lat (w sumie stanowią oni grupę 37,2% ankietowanych), 12,2% ankietowanych zmienia hasła średnio raz na kwartał, 13,3% - raz na rok, a zaledwie 5,6% – raz w miesiącu i 2,3% – raz na tydzień (porównaj rysunek 2.).



Rysunek 2. Częstotliwość zmiany hasła przez ankietowanych studentów (n = 180)
Źródło: opracowanie własne.

Wielu studentów (28,9%) bardzo często wykorzystuje to samo hasło do wielu kont, często – 33,3%, a co niektórzy nawet zawsze – 4,4% (razem 66,6%). Drugą grupę stanowią studenci, którzy rzadko wykorzystują to samo hasło do wielu kont i stanowią oni grupę 20% ankietowanych, bardzo rzadko – 6,2%, nigdy – 7,2% (razem 33,4%). Duża częstotliwość wykorzystywania tego samego hasła do wielu kont wynika z problem zapamiętywania dużej ilości haseł i dużej ilości posiadanych kont (do komputera, do portali społecznościowych, do sklepów online). Okazuje się, że 43,3% studentów nie zapisuje haseł, a 14,4% kiedyś zapisywało, a teraz tego nie robi. Pozostałe 42,3% ankietowanych zapisuje hasła w różnym stopniu, aby ich nie stracić.

Podsumowanie

Badania opisywane w niniejszym artykule to deklaracje młodych ludzi będących w większości w przedziale wiekowym pomiędzy 18 a 26 rokiem życia (pokolenie Z) i 16,1% z pokolenia Y/Z. Pokolenie to dorastało w społeczeństwie w pełni scyfryzowanym, dlatego

obsługa komputera, smartfona, tableta czy zegarka (smartwatch) nie stanowi dla nich problemu i nie budzi strachu (jak w przypadku ludzi z pokolenia X i starszych). Badani studenci posiadają wiedzę na temat różnego typu oszustw i ponad połowa spotkała się z nimi osobiście lub u kogoś z rodziny/znajomych (54,4%) lub spotkała się nieświadomie (sms-y/linki na komórce – 70,6% studentów). Ankietowani studenci największe zaufanie mają do komputerów/laptopów, które najczęściej posiadają wgrane programy ochronne przed wirusami, a najmniejsze do zegarków. Respondenci, mimo świadomości zagrożeń, nie dbają o cyberbezpieczeństwo, nie mają problemu z nowinkami technologicznymi, ale właściwie świadomie narażają się na oszustwo (18,5% nie posiada programu antywirusowego na komputerze uważanym za najbezpieczniejsze urządzenie do transakcji finansowych).

Ponieważ 26,1% studentów miała do czynienia z oszustwami jako ofiary, wyraźnie widać konieczność dalszej edukacji młodego pokolenia w zakresie cyberbezpieczeństwa. Większość badanych studentów już niedługo stanie się absolwentami studiów pierwszego stopnia i będą kontynuować naukę lub zaczną pracę. Przyszły pracodawca zapewne będzie zainteresowany pracownikiem umiejącym obsługiwać nowoczesne urządzenia informatyczne, ale również dbającym o ich bezpieczeństwo i udostępniane dane.

Bibliografia

Balibok, P., Matras, A. (2014). Bankowość mobilna jako innowacyjny kanał dostępu do usług bankowych. *Rocznik Ekonomii i Zarządzania*, 6(42)(2), 7-22.

Boruta-Gojny, B., Popiołek, K. (2014). Intermentoring pokoleniowy w organizacji. W: Sidor-Rządkowska, M. (red.), *Mentoring. Teoria, praktyka, studia przypadków* (91-105). Warszawa: Wolters Kluwer.

Centralne Biuro Zwalczania Cyberprzestępczości. Pobrano z: https://cbzc.policja.gov.pl

Chądrzyński, M., Gruziel, K., Kacperska, E., Klusek, T., Utzig, M. (2021). *Polska w dobie cyfryzacji*. Warszawa: Wydawnictwo Szkoły Głównej Gospodarstwa Wiejskiego w Warszawie.

Chojnacka, M., Zarębska, J. (2022). Analiza zachowań i preferencji zakupowych klientów mebli w dobie pandemii – studium przypadku dla miasta Zielona Góra i jej bliskich okolic. W: Majzel, A., Tankowa, E. (red.), *Rozwój organizacji w świetle współczesnych uwarunkowań społeczno-gospodarczych* (78-86). Warszawa: Wydawnictwo Naukowe IVG.

Departament Zarządzania Danymi (2023). Pobrano z: https://www.gov.pl/web/cyfryzacja/departament-zarzadzania-danymi

Departament Zarządzania Systemami (2023). Pobrano z: https://www.gov.pl/web/cyfryzacja/biura-i-departamenty

Gadomska-Lila, K. (2017). Zarządzanie różnorodnością w kontekście tożsamości organizacyjnej – wyniki badań kultury organizacyjnej wśród kadry kierowniczej i nie

kierowniczej, *Edukacja Ekonomistów i Menedżerów: problemy, innowacje, projekty*, 3(45), 57-68. DOI: http://dx.doi.org/10.5604/01.3001.0010.6274

Karasek, A. (2022). Generation Z's expectations towards the employers. *Scientific Papers of Silesian University of Technology. Organization and Management Series*, 167, 209-218. DOI: http://dx.doi.org/10.29119/1641-3466.2022.167.15

Kondek, G., Ożarowska, E. (2022a). *Raport o dokumentach infoDOK (2 kwartał 2022*). 50 edycja. Pobrano z: https://zbp.pl/Aktualnosci/Wydarzenia/Raport-InfoDOK,-II-kw-%E2%80%93-maleje-liczba-prob-wyludzen-kredytow

Kondek, G., Ożarowska, E. (2022b). *Raport o dokumentach infoDOK (III kwartał 2022*). 51 edycja. Pobrano z: https://dokumentyzastrzezone.pl/wp-content/uploads/2022/11/infodok.2022.07-09.wydanie.51.pdf

Komenda Główna Policji. Pobrano z: http://bip.kgp.policja.gov.pl

Kotz, D., Fu, K., Gunter, C., Rubin, A. (2015). Security for mobile and cloud frontiers in healthcare. *Communications of the ACM*, 58(8), 21-23. DOI: https://doi.org/10.1145/2790830

Maslow, A.H. (2022). *Motywacja i osobowość*. Warszawa: Wydawnictwo Naukowe PWN.

Mazur-Wierzbicka, E. (2015). Kompetencje pokolenia Y-wybrane aspekty. *Studia i Prace Wydziału Nauk Ekonomicznych i Zarządzania*, 39, 307-320.

Morawski, J. (2021). Logistyka ostatniej mili – usprawnienia w obsłudze klienta. *Przedsiębiorczość i Zarządzanie*, 22(2), 241-257.

Plebańska, M., Tarkowski, A. (2016). *Cyfryzacja polskiej edukacji. Wizja i postulaty*. Pobrano z: https://centrumcyfrowe.pl/wp-content/uploads/2016/07/cyfryzacja-polskiej-edukacji_final.pdf

Prokopowicz, P. (2017). Zarządzaj ludźmi, a nie pokoleniami, *Personel i Zarządzanie*, 11, 38-42.

Raport Digital Poland (2022). *Technologia w służbie bezpieczeństwa. Czy Polacy zostaną społeczeństwem 5.0? Edycja 2022,* Pobrano z: https://digitalpoland.org/publikacje/pobierz?id=602693cf-262c-4f2a-bfa3-9f91cfaffd3c

Raport roczny CERT Polska 2020 (2021). *Krajobraz bezpieczeństwa polskiego internetu*. Warszawa: NASK PIB/CERT Polska.

Raport roczny CERT Polska 2021 (2022). *Krajobraz bezpieczeństwa polskiego internetu*. Warszawa: NASK PIB/CERT Polska.

Rudnicka, A., Koszewska, M. (2020). *Uszyte z klasą. Przemysł odzieżowy wobec wyzwań społecznych i środowiskowych*. Łódź: Wydawnictwo Uniwersytetu Łódzkiego.

Sajler-Fudro, P. (2022). Zagrożenia bezpieczeństwa w użytkowaniu systemów informatycznych – klasyfikacja i metody zapobiegania. *Nauki Ekonomiczne*, 35, 189-214. DOI: https://doi.org/10.19251/ne/2022.35(11)

Trejderowski, T. (2013). *Kradzież tożsamości. Terroryzm informatyczny*. Warszawa: Wydawnictwo Eneteia.

Ustawa (2018a). Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Tekst jednolity Dz. U. 2022, poz. 1863**.**

Ustawa (2018b). Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych. Dz. U. 2022, poz. 1863.

Wiktorowicz, J., Warwas, J. (2016). Pokolenia na rynku pracy. W: Wiktorowicz, J., Warwas, J., Kuba, M., Staszewska, E., Woszczyk, P., Stankiewicz, A., Kliombka-Jarzyna, J. (red.), *Pokolenia – co się zmienia? Kompedium zarządzania multigeneracyjnego* (19-37). Warszawa: Wydawnictwo a Wolters Kluwer.

Wasiluk, A., Bańkowska, M. (2021). Przesłanki dotyczące wyboru miejsca pracy przez pracowników pokolenia X, Y i Z. *Zeszyty Naukowe Polskiego Towarzystwa Ekonomicznego w Zielonej Górze*, 8(14), 138-159. DOI: http://dx.doi.org/10.26366/PTE.ZG.2021.197

Załoga, W. (2022). Digital competences of the information society era in the aspect of safety in cyberspace. *Scientific Papers of Silesian University of Technology. Organization and Management*, 164, 541-552. DOI: http://dx.doi.org/10.29119/1641-3466.2022.164.41