JOURNAL
COMPUTER SCIENCES INSTITUTE

JCSI 23 (2022) 112–117
Received: 15 March 2022
Accepted: 5 April 2022

An Analysis of the Knowledge about the Aspects of Cybersecurity and Two-Factor Logging in the Society

Analiza wiedzy o aspektach cyberbezpieczeństwa i logowania dwuetapowego w społeczeństwie

Kamil Piłat*, Michał Tomasz Pawłowski*, Grzegorz Kozieł

Department of Computer Science, Lublin University of Technology, Nadbystrzycka 36B, 20-618 Lublin, Poland

Abstract
The article presents the course of research on the safe use of the Internet, carried out on a group of 200 respondents aged 10-60 and more. Particular attention was paid to the threat of ransomware and other threats on the Internet. Computer-aided survey research was carried out. Survey results were analyzed using a frequency analysis and a Pearson-Spearman correlation analysis. The conducted research showed an unsatisfactory level of knowledge in the field of cybersecurity for the age groups 10-15 and 60 and more, and it was sufficient for the age groups 20-24. The problem has become especially topical given the impact of the COVID-19 pandemic on teaching and remote work and remote communication in families.

Keywords: cybersecurity; two-factor login; ransomware; electronic signature

Streszczenie
W artykule przedstawiono przebieg badań dotyczących bezpiecznego korzystania z Internetu przeprowadzonych na grupie 200 respondentów w wieku 10-60 i więcej lat. Szczególną uwagę zwrócono na zagrożenie oprogramowaniem szpiegującym i inne zagrożenia w sieci Internet. Przeprowadzono badania ankietowe wspomagane komputerowo. Wyniki ankiet były analizowane z użyciem analizy częstości oraz analizy korelacji Pearsona i Spearmana. Przeprowadzone badania wykazały niezadowalający poziom wiedzy z zakresu cyberbezpieczeństwa dla grup wiekowych 10-15 oraz 60 i więcej lat oraz wystarczający dla grup wiekowych 20-24 lat. Problem stał się szczególnie aktualny, biorąc pod uwagę wpływ pandemii COVID-19 na nauczanie i pracę zdalną oraz komunikację zdalną w rodzinach.

Słowa kluczowe: cyberbezpieczeństwo; logowanie dwuetapowe; oprogramowanie szantażujące; podpis elektroniczny

*Corresponding author
Email address: kamil.pilat2@pollub.edu.pl (K. Piłat), michal.pawlowski1@pollub.edu.pl (M. T. Pawłowski)

1. Wprowadzenie

We współczesnym świecie znaczącą rolę odgrywa dostęp do sieci Internet. Wraz z każdym kolejnym rokiem dostęp do niej staje się coraz bardziej powszechny. Obecnie około 60% populacji korzysta z Internetu [1]. Ten fakt wiąże się z dostępem do różnego rodzaju stron internetowych, usług świadczonych drogą elektroniczną, ale także z rozrywką np. gry komputerowe, usługi przesyłania strumieniowego itp. Taka obfitość możliwości oferowanych społeczeństwu pozwala na realizację wielu pożytecznych celów. Warto jednak wspomnieć, że każde działanie w Internecie obarczone jest ryzykiem, które może wystąpić lub można mu zapobiec. Zarówno jedna jak i druga możliwość jest bardziej lub mniej prawdopodobna w zależności od stanu wiedzy jednostki na temat bezpiecznej obsługi komputera oraz poruszania się po sieci.

Kluczowym zagadnieniem, które powinno być bliskie każdemu użytkownikowi komputera oraz Internetu jest cyberbezpieczeństwo. Termin ten wskazuje metody oraz możliwości, jak ochronić się przed różnego rodzaju zagrożeniami takimi jak np. phishing, wirus komputerowy, kradzież tożsamości, spyware itp. W obecnych czasach świadomość czyhających niebezpieczeństw jest bardzo istotna dla każdego użytkownika - zarówno dla osób młodszych jak i starszych. Każdy człowiek może paść ofiarą internetowego przestępcy. Konsekwencje zaistniałej sytuacji mogą być różne - od wycieku danych wrażliwych, poprzez przejęcie kontroli nad sprzętem lub kontem bankowym po szantaż i zastraszanie osoby [9].

W innych publikacjach można spotkać się z analizami wskazującymi na wykluczenie cyfrowe osób starszych, szczególnie żyjących na wsi [2], jak również skrajność tego zjawiska – cyfrowe dzieciństwo osób młodych lub dzieci, które nie wyobrażają sobie funkcjonowania we współczesnym świecie bez dostępu do Internetu [3]. Chcąc zweryfikować obie te skrajności jak również stany pośrednie czy występują w społeczeństwie postanowiono przeprowadzić badanie. Jego celem było zbadanie obecnego stanu wiedzy Polaków w zakresie bezpiecznego korzystania z sieci Internet oraz świadomości zagrożeń, jakie występują.

Na potrzeby badań postawiono następujące tezy badawcze:

T1: Świadomość i podatność na zagrożenia wynikające z korzystania z Internetu jest najmniejsza dla skrajnych grup wiekowych (najmłodsi i najstarsi użytkownicy)

T2: Osoby młodsze (wiek 18-29) mieszkające w mieście mają wyższy poziom wiedzy z zakresu cyberbezpieczeństwa niż osoby starsze (40+) mieszkające zarówno w mieście jak i na wsi. Wyniki w identycznych przedziałach wiekowych są zbliżone.

2. Przegląd literatury

Portal internetowy dobreprogramy.pl udostępnił wyniki badań ankiety dotyczącej cyberbezpieczeństwa w społeczeństwie. Na jej podstawie można wykonać analizę porównawczą danych z jednego jak i z drugiego badania. Po wstępnym porównaniu wyników można stwierdzić, że przeprowadzony scenariusz eksperymentu w ramach pracy magisterskiej nie odbiega znacząco od badania przeprowadzonego przez dobreprogramy.pl.[12]

Strona internetowa controlengineering.pl przeprowadziła ankietę na temat cyberbezpieczeństwa w systemach sterowania w 2016 roku. We wnioskach można przeczytać, że według 37% respondentów największym zagrożeniem jest złośliwe oprogramowanie, 21% badanych osób martwi się możliwością ataku przez hakerów. Co więcej sześciu na dziesięciu respondentów doświadczyło w ciągu ostatnich 24 miesięcy zarejestrowanych incydentów związanych ze złośliwymi cyberatakami [13].

O tym jak bardzo istotna jest ochrona informacji w sieci można było przekonać się na przykładzie służb wojskowych. W związku z wyciekiem danych z Wojska Polskiego przez aplikację Pegasus, można było zdobyć dane o stanach magazynowych polskiej armii [14].

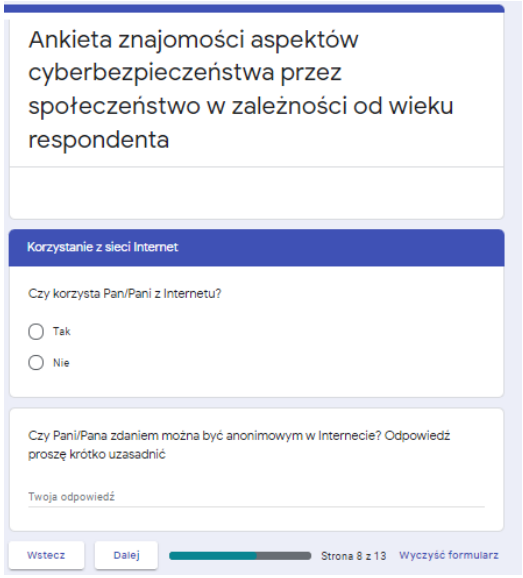
Sprawdzono również jakie skutki może spowodować wyciek danych. Może być to utrata zaufania i wizerunku przez instytucję, duże kary finansowe. Takie wycieki danych mogą powodować kilkuset milionowe straty tak jak to było w przypadku spółki Heartland Payment Systems w 2009 roku i wycieku danych kart płatniczych jej klientów. Straty zostały oszacowane na ponad 100 milionów dolarów [15].

3. Materiały i metody

Eksperyment zrealizowano za pomocą badań ilościowych. W omawianym przypadku zastosowano technikę badań ankietowych wspomaganych komputerowo (CAPI) na grupie 200 respondentów w różnych grupach wiekowych. Aby właściwie przeprowadzić eksperyment przygotowano kwestionariusz ankiety sporządzony w Google Forms. Badanie było anonimowe i zostało przeprowadzone jednorazowo – istotny w tym badaniu jest stan obecny wiedzy respondentów, bez porównywania w okresie czasowym. Poniżej zaprezentowano scenariusz badawczy:

1. Udostępnienie linku do ankiety elektronicznej
2. Respondent otwiera link – otwiera się ankieta
3. Respondent zapoznaje się z opisem na stronie tytułowej, następnie klika przycisk „Dalej”
4. Prezentowana jest ankieta właściwa z pytaniami:
   a) Metryczka (płeć, przedział wiekowy, zawód, wielkość miejsca zamieszkania)
   b) Sekcje:
      - Poziom znajomości informatyki;
      - Korzystanie z sieci Internet;
      - Zagrożenia w sieci;
      - Płatności elektroniczne;
      - Bankowość elektroniczna;
      - Usługi zdrowotne w czasach pandemii;
      - Bezpieczeństwo informacji.
5. Respondent kończy ankietę klikając na przycisk „Wyślij”

Oprócz zaprezentowanego scenariusza, z racji ograniczeń niektórych respondentów wzięto pod uwagę scenariusz alternatywny, który umożliwiał dodatkowo skorzystanie ze wsparcia asystenta – docelowo przeznaczony dla osób z grupy wiekowej 60+. Na Rysunku 1 przedstawiono wybrane pytania z ankiety badawczej:



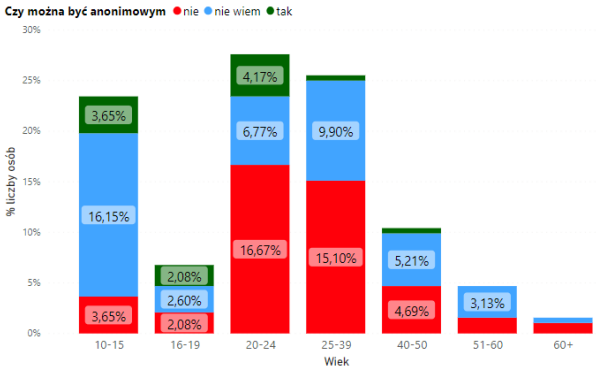
Rysunek 1: Pytanie dotyczące anonimowości w Internecie.

4. Rezultaty i dyskusja

W wyniku przeprowadzonych badań, które poddano analizie uzyskano następujące rezultaty:

4.1. Wykresy

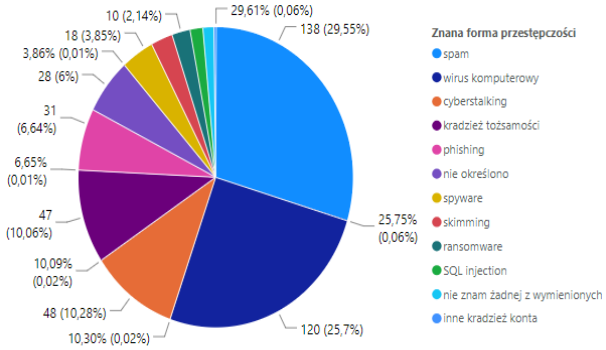
Na wykresie przedstawionym na Rysunku 2 zaprezentowano zależność odpowiedzi na pytanie „Czy można być anonimowym w Internecie?” względem badanych grup wiekowych



Rysunek 2: Wykres zależności wiedzy o anonimowości względem wieku.

Z przeprowadzonych badań wynika że największy procent osób uważa że nie można być anonimowym w Internecie – szczególnie dominują tu osoby z przedziału wiekowego 20-24 (16,67% wszystkich badanych) i 25-39 lat (15,10% wszystkich badanych). Największy odsetek osób nie mających wiedzy w tym zagadnieniu jest w wieku 10-15 lat – te osoby stanowią 16,15% wszystkich badanych osób.

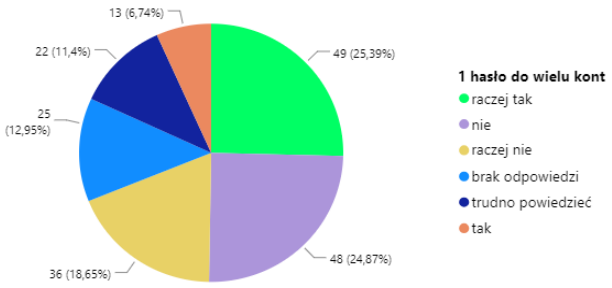
Kolejnym zagadnieniem jakie sprawdzono była wiedza z zakresu znanych form przestępczości. Rezultat przedstawiono na wykresie na Rysunku 3.



Rysunek 3: Znane formy przestępczości – wyniki ogólne.

Ankietowani najczęściej wskazywali na znajomość spamu (29,55%) oraz wirusa komputerowego (25,7%). Najmniej znane były zagrożenia, których nazwy dotyczą oprogramowania szantażującego (ransomware – 2,14%) i ataków na strony lub aplikacje internetowe (SQL injection – 1,5%).

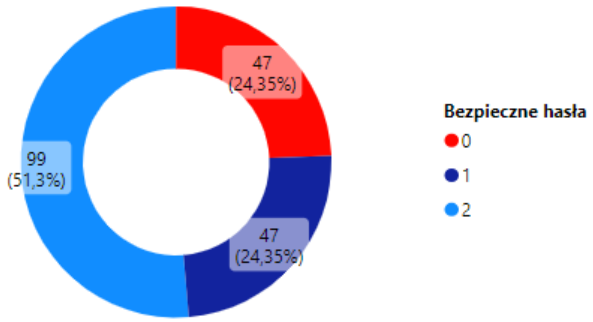
Jak widać na Rysunku 4 blisko 32% ankietowanych zaznaczyło odpowiedź “Raczej tak” lub “Tak”, z drugiej strony blisko 42% osób zaznaczyło odpowiedź “Nie” lub “Raczej nie”.



Rysunek 4: Czy posiada Pan/Pani jedno hasło do większości kont internetowych? - wyniki ogólne.

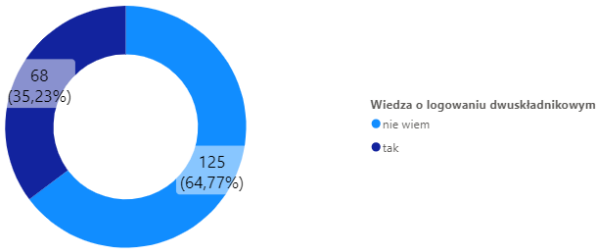
Kolejne pytanie dotyczyło znajomości ustawiania silnych haseł. Ustalono, że maksymalna liczba punktów do zdobycia za w pełni poprawną odpowiedź to 2 punkty. Każda błędna odpowiedź zmniejszała tę wartość o 1 punkt.

Prawie 52% osób uzyskało maksymalną liczbę punktów za to pytanie, 1 punkt zdobyło ponad 24% respondentów (Rysunek 5). Wyniki pomiędzy kobietami a mężczyznami praktycznie się nie różnią.

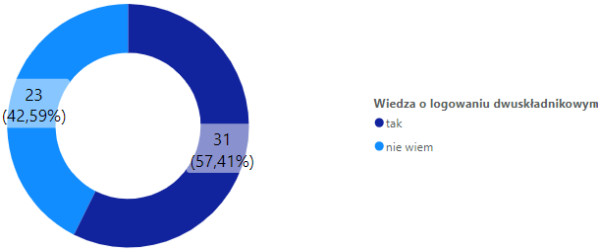


Rysunek 5: Wskazanie poprawnych haseł - wyniki ogólne.

Prawie 65% respondentów nie wie czym jest logowanie dwuskładnikowe (Rysunek 6). Analizując poszczególne grupy wiekowe można zauważyć, że wszystkie mają podobne wyniki do wyników ogólnych, z wyjątkiem przedziału wiekowego 20-14 lat (Rysunek 7), w którym 57% ankietowanych wie co to jest logowanie dwuskładnikowe. Największą wiedzę z grupy zawodów mają studenci bo 67% studentów wie co to jest logowanie dwuskładnikowe. Analizując wielkość zamieszkania respondentów można stwierdzić, że osoby mieszkające w mieście powyżej 300 tys. posiadają dużo większą wiedzę z zakresu logowania dwuskładnikowego ponieważ ich wiedza na ten temat jest wyższa o blisko 14 punktów procentowych większa od osób mieszkających w miastach o wielkości 30 tys. do 300 tys., natomiast porównując tę wiedzę do pozostałych grup osób to wynik jest lepszy o blisko 32 punkty procentowe.

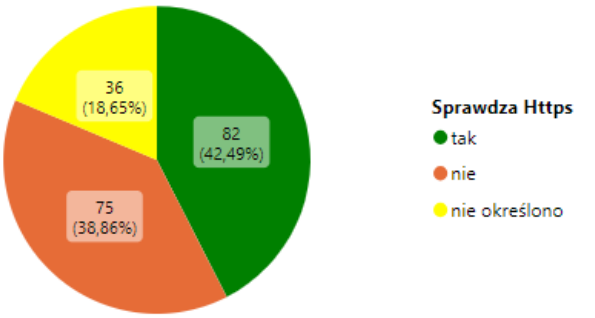


Rysunek 6: Wiedza o logowaniu dwuskładnikowym - wyniki ogólne.



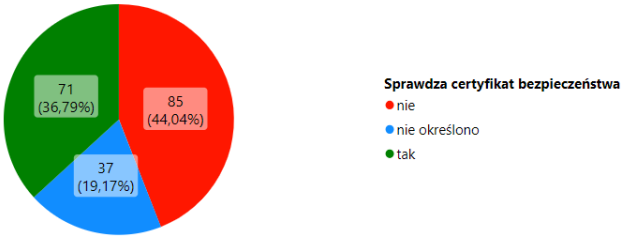
Rysunek 7: Wiedza o logowaniu dwuskładnikowym - wyniki grupy wiekowej 20-24.

Respondenci na pytanie odnośnie sprawdzania przedrostka HTTPS na stronie internetowej banku odpowiedzieli “Tak” w 42%. Prawie 19% ankietowanych nie odpowiedziało na to pytanie, może to oznaczać, że nie znają tego zagadnienia (Rysunek 8).

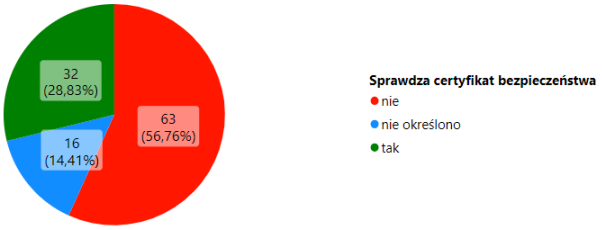


Rysunek 8:Sprawdzanie przedrostka HTTPS na stronie internetowej banku - wyniki ogólne.

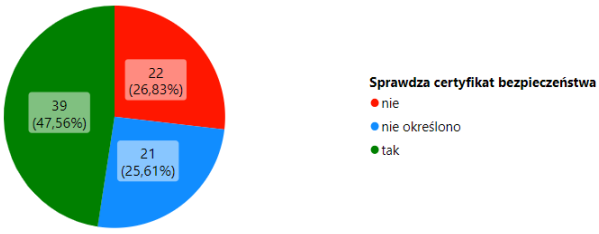
Tylko nieco ponad 44% ankietowanych sprawdza certyfikat bezpieczeństwa po wejściu na stronę internetową swojego banku (Rysunek 9). Warte zauważenia jest, że 56,76% kobiet (Rysunek 10) nie sprawdza certyfikatu bezpieczeństwa na stronach internetowych banków, natomiast 47,56% mężczyzn sprawdza wspomniane certyfikaty bezpieczeństwa (Rysunek 11).



Rysunek 9: Sprawdzanie certyfikatu bezpieczeństwa na stronie internetowej banku - wyniki ogólne.

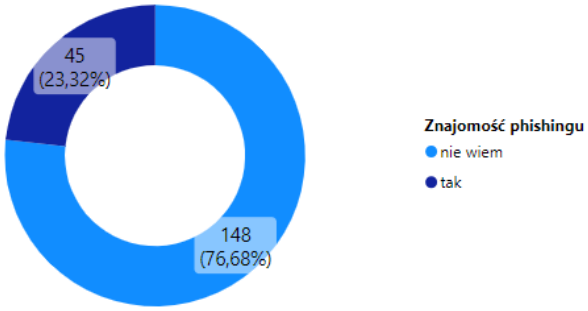


Rysunek 10: Sprawdzanie certyfikatu bezpieczeństwa na stronie internetowej banku - wyniki kobiet.



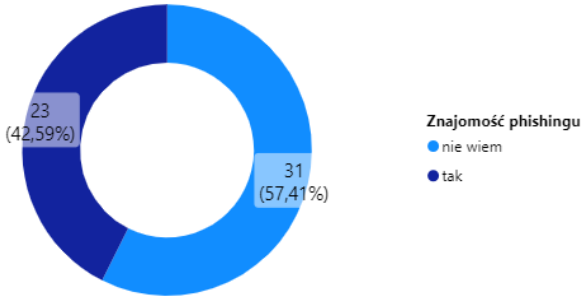
Rysunek 11: Sprawdzanie certyfikatu bezpieczeństwa na stronie internetowej banku - wyniki mężczyzn.

Zweryfikowano wiedzę z zakresu phishingu, aby respondenci podali jak rozumieją to pojęcie. Aby to sprawdzić poproszono o podanie krótkiej definicji, jak respondent rozumie dane zagadnienie. Tylko 23% ankietowanych było w stanie prawidłowo je wyjaśnić, pozostałe wyniki stanowią odpowiedzi błędne lub odpowiedzi "nie wiem" (Rysunek 12).



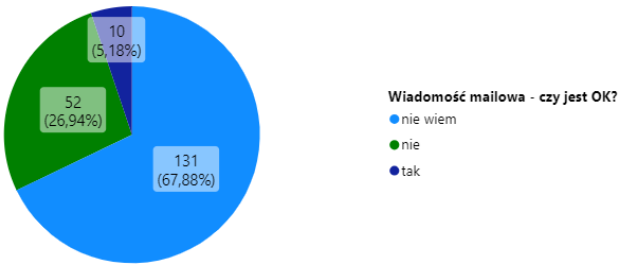
Rysunek 12: Czym jest phishing- wyniki ogólne.

Największą znajomością phishingu okazała się grupa wiekowa 20-24 lat (Rysunek 13) - blisko 43%. Podobny wynik uzyskały osoby z grupy student.

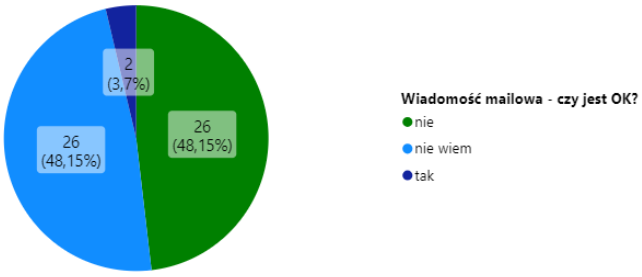


Rysunek 13: Czym jest phishing- wyniki grupy wiekowej 20-24 lat.

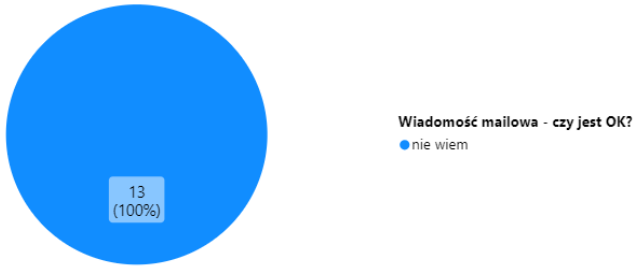
Następnie postanowiono sprawdzić czy respondenci są w stanie określić czy proponowana wiadomość jest próbką phishingu czy też nie. Odpowiedź prawidłowa na to pytanie brzmi – tak, jest to phishing. Dodatkowo ankietowani powinni wskazać dlaczego wydaje im się dlaczego tak wiadomość jest podejrzana lub też dlaczego nie jest. Tylko blisko 27% wskazało poprawną odpowiedź oraz wskazało elementy podejrzane, natomiast ponad 67% respondentów nie wiedziało, o co są pytani w tym pytaniu (Rysunek 14). Porównując wyniki poszczególnych grup wiekowych kolejny raz najlepszą znajomością danego zagadnienia okazała się grupa z przedziału wiekowego 20-24 lat – ponad 48% respondentów wskazało prawidłową odpowiedź i ją uzasadniło (Rysunek 15). Pozostałe grupy wiekowe odpowiadały w podobny sposób, z mniejszą częścią prawidłowych odpowiedzi, z wyjątkiem grupy 16-19 lat, w której nikt nie był w stanie określić czy ta wiadomość jest poprawna czy też nie (Rysunek 16).



Rysunek 14: Wiadomość mailowa phishing- wyniki ogólne.

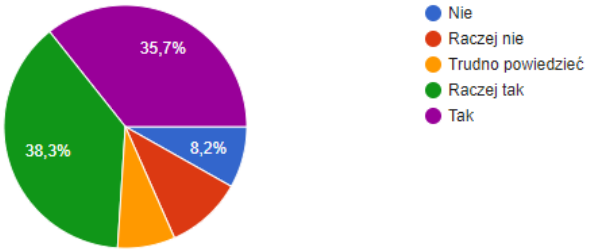


Rysunek 15: Wiadomość mailowa phishing- wyniki grupy wiekowej 20-24 lat.



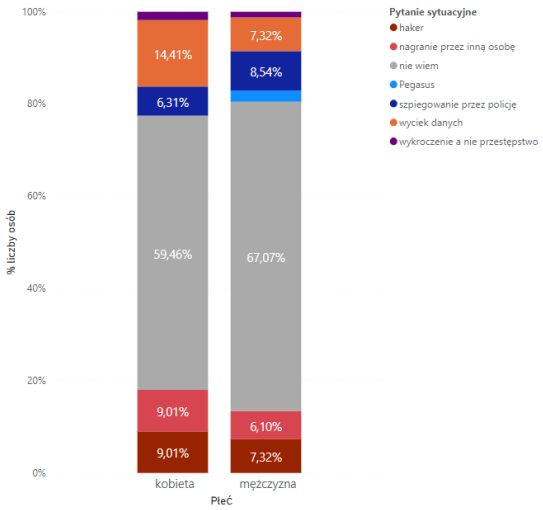
Rysunek 16: Wiadomość mailowa phishing- wyniki grupy wiekowej 16-19 lat.

Kolejne pytanie dotyczyło sprawdzania uprawnień przez użytkowników w instalowanych aplikacjach na ich telefonach. Można zauważyć, że 74% ankietowanych sprawdza lub raczej sprawdza uprawnienia instalowanych aplikacji internetowych (Rysunek 17).



Rysunek 17: Sprawdzenie uprawnień podczas instalowania aplikacji na telefonie- wyniki ogólne.

Ostatnie pytanie w tej sekcji jak i podsumowujące całą ankietę dotyczyło przeczytania pewnej historii, która wydarzyła się w życiu codziennym, i określenia co mogło spowodować taki a nie inny przebieg wydarzeń. Przytoczona historia miała na celu sprawdzić kreatywność ankietowanych pod względem świadomości pozostawania pod obserwacją instytucji oraz innych osób trzecich. Jak można zauważyć na Rysunku 18 wyniki kobiet oraz mężczyzn są bardzo zbliżone do siebie. Najczęściej ankietowani wskazywali na wyciek danych oraz działalność hakerów – blisko 25% kobiet wskazało te dwie odpowiedzi, natomiast mężczyźni dodatkowo wskazywali częściej śledzenie przez Policję. Niestety zdecydowana większość ankietowanych nie miała pomysłu co mogło spowodować przytoczoną sytuację.



Rysunek 18: Ocena sytuacji związanej z zagrożeniem cyberprzestępstwem - wyniki płci.

5. Wnioski

Postawiona teza 1, która brzmi: „Świadomość i podatność na zagrożenia wynikające z korzystania z Internetu jest najmniejsza dla skrajnych grup wiekowych (najmłodsi i najstarsi użytkownicy)" została potwierdzona. Skrajne grupy miały trudność w znalezieniu prawidłowej odpowiedzi na większość podstawowych pytań. Współczynnik odpowiedzi poprawnych do odpowiedzi niepoprawnych oscylował w okolicach 0.3, podczas gdy dla grup z najwyższą świadomością zawierał się w okolicach 0.7.

Teza „Osoby młodsze (wiek 18-29) mieszkające w mieście mają wyższy poziom wiedzy z zakresu cyberbezpieczeństwa niż osoby starsze (40+) mieszkające zarówno w mieście jak i na wsi. Wyniki w identycznych przedziałach wiekowych będą zbliżone" również została potwierdzona. Osoby młodsze zazwyczaj korzystały częściej z Internetu w przeciwieństwie do osób 40 lat i więcej, poświęcając więcej czasu na edukację w tym zakresie. Często te osoby miały styczność z komputerem we wcześniejszym wieku niż osoby starsze, wobec czego duża część pojęć nie jest im obca.

Duży wpływ na rezultaty badań miała pandemia COVID- 19, która przyczyniła się do wzrostu aktywności respondentów sieci oraz korzystania z komputera. Ludzie niezależnie od wieku byli zmuszeni do zmiany nawyków, gdyż codzienne życie skłoniło ich do korzystania z usług elektronicznych. Szczególnie dało się to zauważyć w zakresie nauki oraz pracy zdalnej. Zwiększony ruch sieciowy na całym świecie spowodował zwiększenie częstotliwości cyberataków.

W ankiecie również zawarto pytanie kontrolne mające na celu sprawdzenie czy deklarowany poziom znajomości informatyki i cyberbezpieczeństwa pokrywa się ze stanem rzeczywistym. Osoby młodsze częściej zaznaczały odpowiedź o wysokim lub bardzo wysokim stopniu znajomości informatyki, co nie miało odzwierciedlenia w uzyskanym wyniku. Zdecydowana większość ankietowanych zaznaczyła odpowiedź średni stopień znajomości informatyki, co odpowiada stanowi faktycznemu. Pomimo tego, że osoby z grupy wiekowej

20-24 lata wypadły najlepiej w tym badaniu to ich wiedza mogłaby być znacznie lepsza. Warto wziąć pod uwagę poprawę edukacji z zakresu informatyki oraz wiedzy o cyberbezpieczeństwie. Duży nacisk można by położyć na samorozwój poprzez kursy i szkolenia oraz obowiązkowe zajęcia na uczelniach lub w pracy z tego zakresu.

6. Podziękowanie

Autorzy przeprowadzanego badania dziękują wszystkim uczestnikom, którzy ochoczo i dobrowolnie wzięli w nim udział. Podziękowanie szczególnie kierują do wszystkich nauczycieli i dyrekcji szkół, w których umożliwiono przeprowadzenie ankiety.

Bibliografia

[1] M. Warner, Cybersecurity: A Pre-history, Intelligence and National Security 27(5) (2012) 781-799.

[2] A. Jastrzębska, W. Jastrzębska, Wykluczenie cyfrowe– przyczyny, zagrożenia i bariery jego pokonania. Studium przypadku, Nierówności społeczne a wzrost gospodarczy 25 (2012) 91-104.

[3] S. Wójcik, Zagrożenia dzieci i młodzieży w Internecie. Dziecko krzywdzone. Teoria, badania, praktyka 16(1) (2017) 270-287.

[4] E. Krok, Budowa kwestionariusza ankietowego a wyniki badań, Zeszyty Naukowe Studia Informatica/Uniwersytet Szczeciński, 2015.

[5] R. G. Brody, E. Mulig, V. Kimball, Phishing, pharming and identity theft, Academy of Accounting & Financial Studies Journal 11(3) (2007).

[6] D. Mielnik, Anonimowość w Internecie a problem cyberbezpieczeństwa, Aspekt prawny, 2019

[7] B. Buraczyńska, Zagrożenia bezpieczeństwa w sklepach internetowych, Monografie–Politechnika Lubelska 69 (2020).

[8] B. Kaczmarczyk, P. Szczepański, M. Dąbrowska, Wybrane zagadnienia cyberbezpieczeństwa, Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy 3(32) (2019).

[9] I. Hejduk, Rozwój technologii cyfrowych a wykluczenie społeczne osób 65 plus. Zeszyty Naukowe Uczelni Vistula, (46 (1) Ekonomia X. Pracownicy wiedzy 65 plus-nowe szanse (czy kontrowersje) wobec wyzwań współczesności) (2016) 64-78.

[10] R. Pitera, Współczesne problemy i zagrożenia cyberbezpieczeństwa w sektorze usług bankowości elektronicznej. Przegląd Nauk o Obronności 2 (2017) 181-192.

[11] M. K. Maciejczuk, K. Wnorowski, M. Olchanowski, Cyberbezpieczeństwo dzieci i młodzieży w prawie polskim, 2019

[12] Ankieta dotycząca cyberbezpieczeństwa w społeczeństwie – portal internetowy dobreprogramy.pl https://www.dobreprogramy.pl/wyniki-ogolnopolskiego-badania-wskazuja-ze-polacy-nie-doceniaja-wartosci-swoich-danych,6656565069908544a [15.03.2022r]

[13] Ankieta portalu internetowego controlengineering.pl cyberbezpieczeństwo w systemach sterowania - https://www.controlengineering.pl/cyberbezpieczenstwo-6-kluczowych-wnioskow-z-redakcyjnej-ankiety/ [15.03.2022r]

[14] Artykuł o wycieku danych Wojska Polskiego https://www.telepolis.pl/wiadomosci/wydarzenia/pegasus-wojsko-polskie-wyciek [15.03.2022r]

[15] Blog opisujący skutki wycieku danych https://www.ekransystem.com/pl/blogpolska/ile-kosztuje-wyciek-danych [15.03.2022r]