JOURNAL of COMPUTER SCIENCES INSTITUTE

JCSI 14 (2020) 48-54
Wysłane: 2019-10-17
Przyjęte: 2019-10-28

Ocena świadomości studentów informatyki w zakresie bezpieczeństwa komunikatorów internetowych

Paweł Stręciwilk*, Grzegorz Kozieł
Politechnika Lubelska, Katedra Informatyki, Nadbystrzycka 36B, 20-618 Lublin, Polska

Streszczenie. Komunikatory internetowe, choć obecne z nami już od dziesięcioleci, zyskały dużą popularność w tej dekadzie. Dziś są najczęściej wykorzystywaną formą komunikacji, szczególnie wśród młodych ludzi. Jednak tam, gdzie są przesyłane informacje, istnieje również ryzyko ich przechwycenia, manipulacji czy udaremnienia przekazu. Ważną kwestią stało się zatem bezpieczeństwo komunikatorów internetowych, które powinny chronić nie tylko wrażliwe dane swoich użytkowników, ale także ich prywatność. Niemniej ważną kwestią jest także świadomość użytkowników, którzy z tego oprogramowania korzystają. Czy są oni świadomi zagrożenia wysyłania poufnych informacji tą drogą? Czy sami odpowiednio zabezpieczają się przed ewentualną próbą włamania? Artykuł powstał w celu zaprezentowania oceny świadomości użytkowników w zakresie bezpieczeństwa komunikatorów internetowych.

Słowa kluczowe: komunikacja; bezpieczeństwo; komunikatory internetowe

*Autor do korespondencji.

Adresy e-mail: pawel.streciwilk@pollub.edu.pl, g.koziel@pollub.pl

An Assessment of IT Students' Awareness in the Field of Instant Messengers Security

Paweł Stręciwilk*, Grzegorz Kozieł
Department of Computer Science, Lublin University of Technology, Nadbystrzycka 36B, 20-618 Lublin, Poland

Abstract. Instant Messengers, though being around for decades, only in recent years they have managed to gain much more popularity. Today, they are the most common way of communicating, especially among young people. However, where information is being transferred there is a potential risk of it being intercepted, manipulated or disrupted. Thus, Security of Instant Messengers became a matter of high importance comprising of not only protecting the users' sensitive information but also privacy. Also important is the awareness of the users. Are they aware of the dangers that come with directing sensitive information in this manner? Are they taking the necessary steps to shield themselves from breach attempts? This article was written to present and evaluate the awareness of IT students in the field of instant messengers security.

Keywords: communication; security; instant messengers

*Corresponding author.

E-mail addresses: pawel.streciwilk@pollub.edu.pl, g.koziel@pollub.pl

1. Wstęp

Komunikacja z użyciem komunikatorów internetowych staje się obecnie standardem. Dotyczy to zarówno sfery prywatnej, jak również zawodowej. W sferze prywatnej prym wiedzie Messenger – komunikator opracowany przez Facebook [1]. W sferze zawodowej komunikator zazwyczaj narzucany jest przez firmę, w jakiej użytkownik podejmuje zatrudnienie. Powodem jest konieczność posiadania jednej platformy komunikacji pozwalającej wszystkim pracownikom na łatwą komunikację. Nie mniej istotne jest również bezpieczeństwo oferowane przez zastosowane oprogramowanie[1]. Istotne jest jednak pytanie czy wśród użytkowników prywatnych świadomość bezpieczeństwa jest równie rozwinięta. Aby odpowiedzieć na to pytanie postawiono 3 hipotezy robocze:

H1. Użytkownicy związani z dziedziną informatyki mają wysoki poziom świadomości w sferze bezpieczeństwa komunikatorów internetowych.

H2. Użytkownicy posiadający wysoki poziom wiedzy w dziedzinie bezpieczeństwa wybierają komunikatory ze względu na oferowane przez nie zabezpieczenia.

H3. Dla użytkowników prywatnych podczas używania komunikatorów liczy się przede wszystkim prywatność.

W celu zweryfikowania tych hipotez przeprowadzono ankietę na grupie stu osób. Wszystkie z nich były związane z branżą informatyczną. Większość, bo aż 88 osób, była studentami trzeciego roku informatyki na Politechnice Lubelskiej. Grupa została dodatkowo uzupełniona o 12 osób, które edukację nadal kontynuują lub już ją zakończyły i wciąż rozwijają się w branży. Ankieta miała na celu sprawdzenie jaką świadomość, preferencje i doświadczenia mieli użytkownicy z bezpieczeństwem komunikatorów internetowych.

1.1. Przegląd literatury

Publikacja „Guide to Chat Apps” [1] stanowiła doskonałą drogę, by lepiej zrozumieć naturę komunikatorów internetowych, kierunek ich rozwoju i pozycję we współczesnym świecie. Pokazuje jak ważna jest dziś ta forma komunikacji, zwłaszcza wśród młodszego pokolenia. Pozycja Holta, Freilicha i Chermaka [2] pomogła z kolei zidentyfikować współczesne zagrożenia, na jakie narażeni są użytkownicy. Dziś hakerzy atakują już nie tylko kierowani chęcią szybkiego zarobku, ale przyświecają im także szkodliwe idee – takie jak ekstremizm popychający do terroryzmu. Targetowanie przez nich swoich ofiar daje dodatkowe powody, by szczególnie dbać o swoje bezpieczeństwo i prywatność. Lektura pozycji Mitnicka, Simona oraz Wozniaka [3] daje wgląd w jedną z najsłabszych ogniw bezpieczeństwa niemal każdego systemu – element ludzki. Można wysunąć dość jasny wniosek, że każdy system jest tak bezpieczny jak społeczność go tworząca. Zainspirowało to stworzenie ankiety wśród użytkowników, by sprawdzić czy ich świadomość w zakresie bezpieczeństwa jest wystarczająca, by nie narażać systemu (a więc także innych użytkowników) na luki ze swojej strony. Powstanie artykułu zostało poprzedzone także odpowiednim przygotowaniem z podstawowych pojęć z dziedziny kryptografii, by móc lepiej zrozumieć mechanizmy stojące za szyfrowaniem przekazywanych informacji i ewentualne problemy, jakie te może napotkać [4]. Pozostałe pozycje [5-10] stanowiły lektury uzupełniające, które pozwoliły lepiej przygotować się do omówionego tematu, poprzez spojrzenie na problem bezpieczeństwa w informatyce z różnych perspektyw.

2. Porównanie komunikatorów

Rynek komunikatorów internetowych nie może narzekać na pustki czy stagnację. Użytkownicy mają do wyboru niezliczone ilości komunikatorów – zależnie od potrzeb na pewno znajdzie się pozycja, która powinna je spełnić. Oczywiście nie sposób opisać je wszystkie, więc na podstawie przeprowadzonej ankiety zawężono wybór, a następnie krótko opisano kilka z nich. Wybrano Facebook Messenger, WhatsApp, Telegram, Discord oraz Skype. Wszystkie posiadają unikalne dla siebie cechy. Facebook Messenger jest komunikatorem wywodzącym się z największej sieci społecznościowej na świecie, Facebooka, i w związku z tym cieszy się ogromną bazą użytkowników. WhatsApp jest jedną z pierwszych aplikacji, która przebiła się do świadomości użytkowników (dziś mówimy o liczbie ponad 1 miliarda pobrań) i przyśpieszyła rozwój rynku komunikatorów internetowych. Telegram jest aplikacją konkurencyjną dla WhatsAppa, stawiającą głównie na bezpieczeństwo i ochronę prywatności. Bardzo szybko zyskujący na popularności Discord jest aplikacją przeznaczoną dla bardzo konkretnej grupy odbiorców, wokół której rozwija swoje funkcjonalności. Skype natomiast może pochwalić się silnym zakorzenieniem wśród świadomości użytkowników. Wszystkie te aplikacje oczywiście różnią się nie tylko funkcjonalnością, ale również podejściem ich twórców do zagadnień bezpieczeństwa oraz prywatności swoich użytkowników.

Tabela 1. Wykorzystywane przez komunikatory szyfrowanie

Nazwa komunikatora	**Szyfrowanie**	
	Podstawowe algorytmy	**End-to-end**
Messenger	Tak	Opcjonalne
WhatsApp	Nie	Tak
Telegram	Tak	Opcjonalne
Discord	Brak informacji	Nie
Skype	Tak (nie zawsze)	Nie

Komunikatory te zostały poddane analizie bezpieczeństwa i prywatności na podstawie ogólnie dostępnych informacji na ich temat – zaczynając na tych udostępnionych przez samych twórców, na artykułach o złamanych zabezpieczeniach kończąc. Najważniejsze uwagi zostały zaprezentowane w Tabeli 2.

Tabela 2. Wyniki szczegółowej analizy poszczególnych komunikatorów.

Nazwa	**Uwagi**
Messenger	Ogromna baza użytkowników. Duża ilość zbieranych o użytkownikach informacji. Skanowanie wiadomości w sposób automatyczny oraz okazjonalne czytanie ich przez pracowników firmy. Dobre zabezpieczenie na etapie logowania.
WhatsApp	Dobra edukacja użytkowników na temat bezpieczeństwa. Obowiązkowe szyfrowanie end-to-end. Brak jakiegokolwiek szyfrowania kopii zapasowej historii rozmów. Długi czas reakcji na krytyczne błędy bezpieczeństwa.
Telegram	Decentralizacja przechowywania kluczy szyfrujących dane w chmurze. Możliwość usuwania wiadomości po stronie rozmówcy. Szybka reakcja na krytyczne błędy bezpieczeństwa. Wysoki poziom prywatności. Liczne funkcjonalności komunikatora wpływające na bezpieczeństwo – np. brak możliwości wykonania zrzutów ekranu, opcja samozniszczenia konta, dodatkowy ekran blokujący komunikator). Ograniczona dostępność w niektórych regionach.
Discord	Szczątkowe informacje na temat bezpieczeństwa. Funkcje prywatności ograniczone do ustawień wewnątrz grupy i trybu streamowania. Rozwój oprogramowania dyktowany przypodobaniem się graczom.
Skype	Brak szyfrowania połączeń podczas używania sieci publicznych. Brak szyfrowania gromadzonych plików lokalnych. Brak funkcjonalności zwiększających bezpieczeństwo i prywatność.

Analiza ta pozwoli na lepsze zrozumienie wartości, jakimi kierowali się ankietowani podczas wyboru używanych przez siebie komunikatorów – a tym samym wyników przeprowadzonej ankiety.

3. Badanie

3.1. Metodyka badań

Badanie zostało podzielone na dwie części. Pierwszą z nich jest przedstawiona już analiza komunikatorów internetowych, drugą z kolei przeprowadzenie ankiety badającej kilka aspektów związanych z bezpieczeństwem. Obie części uzupełniają się, by możliwe było wyciągnięcie jak najlepszych wniosków.

3.2. Dobór grupy badawczej

Grupa badawcza stanowiła 100 osób, 88 z nich to studenci Politechniki Lubelskiej trzeciego roku informatyki. Grupa ta została dodatkowo uzupełniona o 12 osób związanych z branżą informatyczną, by sprawdzić, czy pojawią się ewentualne odchyły w uzyskanych wynikach. Założono, że wybrana grupa powinna być bardziej świadoma istniejących zagrożeń aniżeli przeciętni użytkownicy, na co dzień niezwiązani w żaden sposób z informatyką.

3.3. Przebieg badań

Przeprowadzona ankieta pokryła kilka kwestii związanych z bezpieczeństwem komunikatorów internetowych. Użytkowników zapytano o:

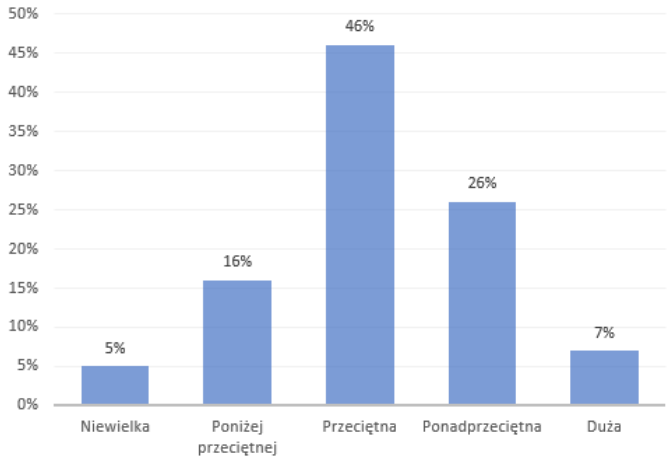
- wiedzę w zakresie cyberbezpieczeństwa,
- ich preferencje względem używanych komunikatorów, co wpłynęło na ich wybór,
- przywiązywanie uwagi do bezpieczeństwa komunikacji,
- podejście do zapewnienia prywatności,
- jak sami dbają o swoje bezpieczeństwo,
- doświadczenia związane z naruszeniem tego bezpieczeństwa,
- co postrzegają jakie największe zagrożenie dla swojego bezpieczeństwa.

Wyniki zostały następnie przeanalizowane. Wzięto pod uwagę zarówno pojedyncze odpowiedzi oraz wyciągnięto wnioski z krzyżowania wybranych pytań.

4. Dyskusja wyników

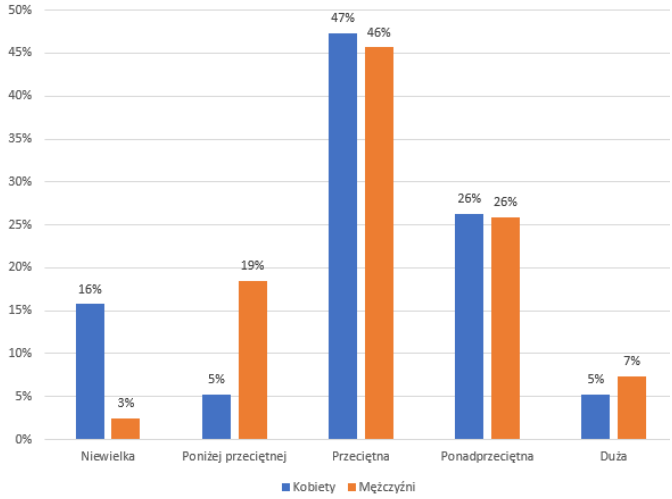
Ankieta została przeprowadzona w środowisku, któremu zagadnienia z dziedziny kryptologii nie powinny być trudne do przyswojenia. Zapytano ich w takim razie, jak oceniają swoją wiedzę o cyberbezpieczeństwie. Można było odpowiedzieć w pięciostopniowej skali – od wiedzy niewielkiej do dużej. Wyniki zaprezentowano na Rys.1.

Jak widać zdecydowana większość (46%) określa swoją widzę jako przeciętną – dając sobie pewne miejsce na uzupełnienie braków. Pośród pozostałych użytkowników 26% deklaruje, że ich wiedza jest ponadprzeciętna, a 7% mówi wręcz o dużej wiedzy. Szczególnie ta grupa była bardzo pomocna w ocenieniu, które komunikatory zasługują na uwagę pod względem bezpieczeństwa. Dodatkowo 16% oceniło swoją wiedzę na poniżej przeciętną, a 5% na niewielką – dalsza analiza wyników pokaże czy nie jest to dyktowane dozą ostrożności w tym temacie.



Rys, 1. Deklarowana wiedza o cyberbezpieczeństwie

Naturalnym następstwem byłoby także zbadanie korelacji, między różnymi grupami badanych – ta jest jednak bardzo jednolita. Szczególnie jeżeli chodzi o wiek badanych wahający się między 21 a 23 lata, z kilkoma wyjątkami. Na Rys.2. można jednak sprawdzić jak deklarowana wiedza wygląda przy reprezentacji różnych płci.

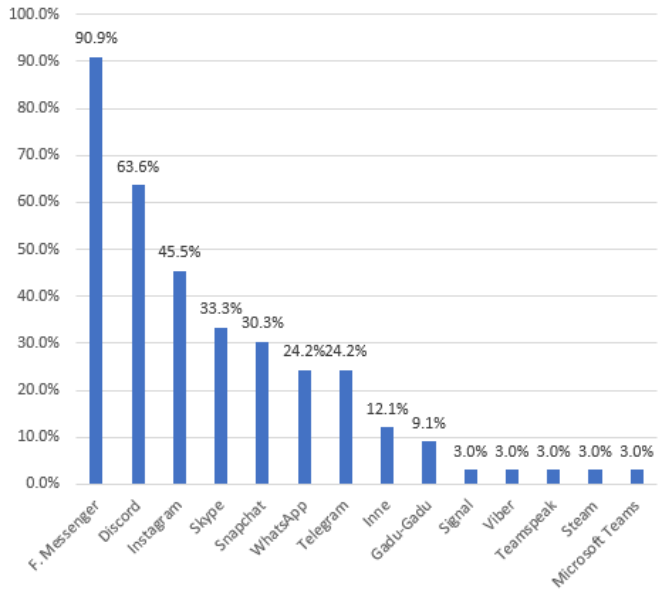


Rys. 2. Deklarowana wiedza wśród kobiet i mężczyzn

Kobiety i mężczyźni są dość zgodni jeżeli chodzi o ocenę swojej wiedzy o cyberbezpieczeństwie. Jedyna niewielka różnica występuje przy deklarowaniu wiedzy niewielkiej i poniżej przeciętnej – nie mając przy tym większego wpływu na całość. Można to tłumaczyć faktem, iż mimo podziału na płeć wszystkie te osoby dzielą wspólną pasję, rozwijając się na uczelni na kierunku Informatyki, której to kryptologia jest nieodłącznym elementem. Osoby takie chętnie również

adaptują nowe technologie, co może skutkować w zgłębianie się w szczegóły działania wybieranych rozwiązań.

Wracając do samych komunikatorów, biorąc pod uwagę jedynie osoby o ponadprzeciętnej i dużej wiedzy o cyberbezpieczeństwie możemy sprawdzić na Rys.3. jakich komunikatorów używa ta grupa i sprawdzić czy pojawia się tendencja do komunikatorów uznawanych za bezpieczne.



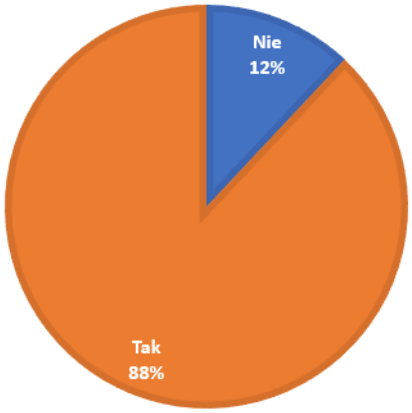
Rys.3. Komunikatory używane przez osoby o ponadprzeciętnej i dużej wiedzy o cyberbezpieczeństwie.

Wykres jasno pokazuje, że duża wiedza nie ma większego wpływu na wybór używanych komunikatów. Wysokie pozycje Facebook Messengera, Snapchata i Instagrama można jednak tłumaczyć nie tyle chęcią komunikacji, co posiadania konta na portalu społecznościowym. Pamiętać należy także, że portale te posiadają dużą bazę użytkowników, którzy mogą być niedostępni nigdzie indziej. Jednak wysoka świadomość zagrożenia może nadal w dużym stopniu wpłynąć na sposób w jaki korzystają z nich użytkownicy.

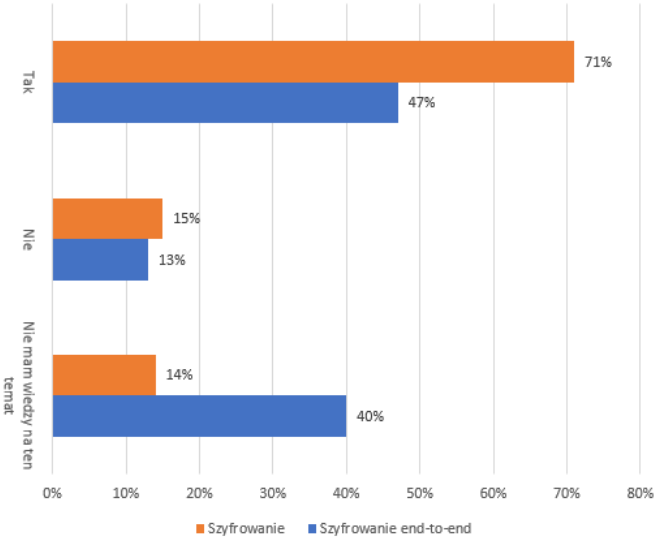
By rozwinąć tę kwestię i poszukać odpowiedzi gdzie indziej, zapytano czy użytkownicy zwracają uwagę na swoje bezpieczeństwo korzystając z owych komunikatorów, a tym samym są świadomi istniejącego zagrożenia.

Diagram widoczny na Rys.4. może budzić optymizm, biorąc pod uwagę, że aż 88% ankietowanych zwraca uwagę na bezpieczeństwo. Można więc założyć, że mimo że wiedza o cyberbezpieczeństwie nie wpływa bezpośrednio na wybór komunikatora, to wpływa na sposób ich używania.

Uzupełniającym pytaniem będzie, czy użytkownikom zależy na szyfrowaniu oraz szyfrowaniu end-to-end. Przedstawia to Rys. 5.



Rys. 4. Procent wszystkich użytkowników zwracających uwagę na bezpieczeństwo komunikacji.



Rys. 5. Procent użytkowników, którym zależy na szyfrowaniu.

Biorąc pod uwagę duży procent użytkowników, którzy zwracają uwagę na bezpieczeństwo oraz równie duże zapotrzebowanie na szyfrowanie wiadomości można wyciągnąć pewne wnioski. Mimo deklarowania przez większość przeciętnej wiedzy na temat cyberbezpieczeństwa jest ona wystarczająca, by świadomie korzystać z komunikatorów internetowych i skutecznie zapobiegać zagrożeniom.

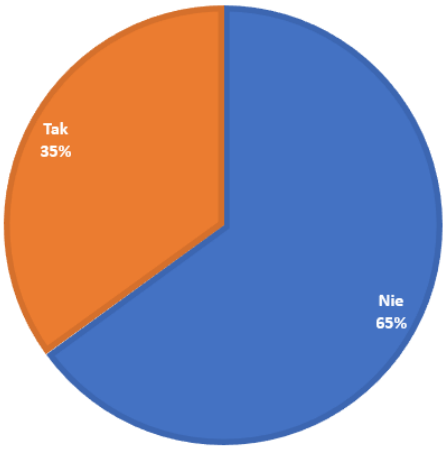
Można więc częściowo zweryfikować hipotezę H1. Użytkownicy związani z branżą informatyczną mają dużą świadomość zagrożenia. Nie przekłada się to jednak na posiadanie specjalistycznej wiedzy z tej dziedziny, czego dowodzi m.in. 40% użytkowników, którzy nie mają wiedzy na temat szyfrowania end-to-end – jednego z podstawowych zagadnień w bezpieczeństwie komunikatorów internetowych.

Pamiętając, że użytkownicy o dużej wiedzy o cyberbezpieczeństwie korzystają z tych samych komunikatorów co reszta grupy, warto zadać sobie pytanie co kieruje ich wyborem.

Zapytano użytkowników o powody, z których korzystają z wybranych rozwiązań. Oto wybrane odpowiedzi:

- „Bezpieczeństwo, funkcjonalność, design”,
- „Znajomi ich używali”,
- „Funkcjonalność”,
- „Nacisk otoczenia ” (przetłumaczone z „peer pressure”),
- „Prywatność, bezpieczeństwo, łatwość użycia”,
- „Bezpieczeństwo, naklejki, wygoda”,
- „Coraz mniej osób korzystało ze starego komunikatora, przeniosłem się tam, gdzie miałem najwięcej znajomych – dodatkowo miał fajne ficzery.”,
- „Ilość znajomych korzystających z danego rozwiązania, oferowana funkcjonalność, bezpieczeństwo rozmów”,
- „Ilość znajomych korzystających z komunikatora”,
- „Duża ilość znajomych”.

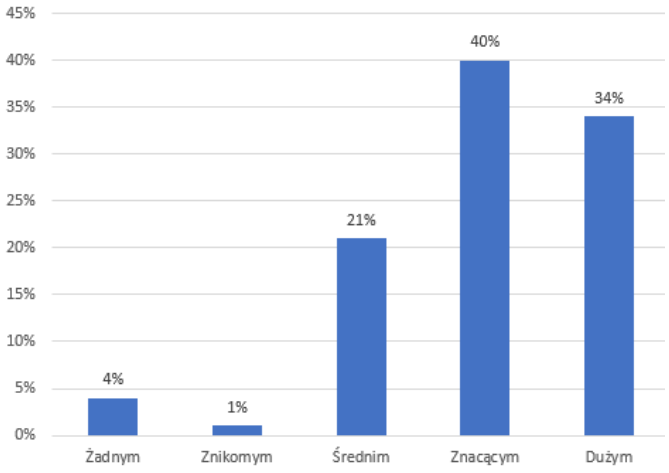
Jak widać, kryteria są dość uniwersalne – liczba funkcjonalności, prywatność, bezpieczeństwo, ale przede wszystkim liczba znajomych korzystająca już z danego rozwiązania. To dowodzi, czemu to właśnie komunikatory wywodzące się z sieci społecznościowych mają największą liczbę użytkowników. Uzupełniającym pytaniem było zapytanie wprost, czy użytkownicy kierują się bezpieczeństwem komunikatora podczas jego wyboru.



Rys. 6. Procent użytkowników kierujących się bezpieczeństwem podczas wyboru komunikatora.

Dla aż 65% użytkowników bezpieczeństwo nie jest priorytetem podczas tego wyboru. Mimo świadomości zagrożenia, to inne czynniki wpływają na używane komunikatory. Pozwala to obalić hipotezę H2.

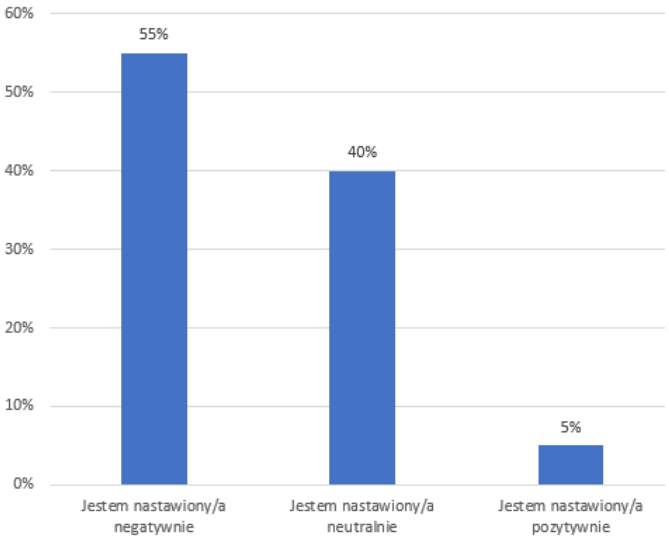
Ostatnią do omówienia kwestią jest prywatność. Mimo iż pojęcie prywatności jest bardzo bliska pojęciu bezpieczeństwa w przypadku komunikatorów internetowych, należy zaznaczyć, że nie każdy gwarantujący bezpieczeństwo komunikator, gwarantuje także prywatność. Ma to związek z przyjętą przez twórców polityką. Zapytano więc użytkowników jak bardzo cenią sobie prywatność. Przyjęto pięciostopniową skalę – od prywatności nie będącą istotną w żaden sposób do dużego znaczenia. Wynik widoczny jest na Rys. 7.



Rys. 7. Stopień w jakim użytkownicy cenią sobie swoją prywatność.

Jak widać nie jest to kwestia użytkownikom obojętna. Jedynie nieliczni ankietowani odpowiedzieli, że prywatność jest dla nich w żaden lub znikomy sposób istotna. Większość ankietowanych uważa, że prywatność jest dla nich aspektem znaczącym (40%) lub bardzo ważnym (34%). Z kolei 21% użytkowników ceni sobie swoją prywatność w średnim stopniu.

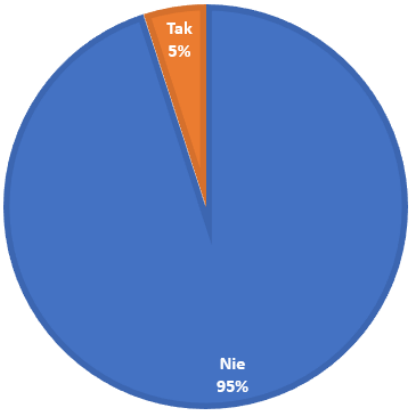
Głównym zagrożeniem dla prywatności jest oczywiście dostęp do wiadomości przez inne osoby. Czasem jednak to dostawcy oprogramowania korzystają z dostępu do treści rozmów w różnych celach: moderacja, analiza w celu dobierania reklam itd. W większości przypadków dzieje się to z wykorzystaniem zautomatyzowanych rozwiązań. Jakie zdanie mają użytkownicy na temat analizy treści ich konwersacji możemy zobaczyć na Rys. 8.



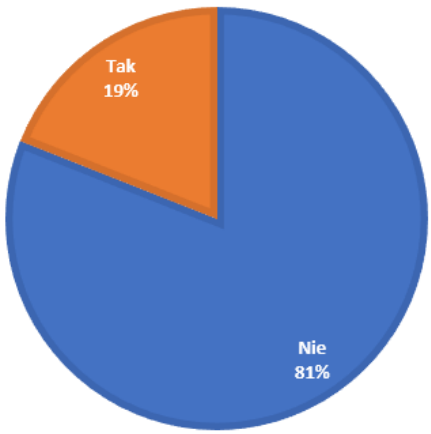
Rys. 8. Podejście użytkowników do zautomatyzowanej analizy treści.

Użytkownicy bardzo niechętnie podchodzą do tego typu praktyk. Ponad połowa ankietowanych – 55% – jest negatywnie nastawiona do analizy treści ich prywatnych wiadomości. Tylko 5% ma na ten temat pozytywne zdanie.

W celu uzupełnienia wyników zapytano użytkowników, czy zrezygnowaliby z prywatności na rzecz lepszego dopasowania materiałów marketingowych (Rys. 9) oraz pomocy służbom bezpieczeństwa narodowego (Rys. 10).



Rys. 9. Procent użytkowników, którzy byliby skłonni zrezygnować z prywatności na rzecz lepszego dopasowania materiałów marketingowych.



Rys. 10. Procent użytkowników, którzy byliby skłonni zrezygnować z prywatności na rzecz bezpieczeństwa narodowego.

Przedstawione wyniki nie pozostawiają pola do dyskusji. Użytkownicy bardzo niechętnie rezygnują ze swojej prywatności. Jest to dla niech znacznie bardziej wrażliwy temat niż samo bezpieczeństwo komunikacji (które samo w sobie może oczywiście bardzo negatywnie odbić się na prywatności). Jedynie 5% ankietowanych byłaby skłonna zrezygnować z prywatności, by otrzymywać lepiej dopasowane materiały marketingowe, zbudowane na bazie wysyłanej przez siebie treści. Wszyscy pozostali nie godzili się na takie rozwiązanie. Podobną tendencję można zaobserwować przy rezygnacji z prywatności na rzecz bezpieczeństwa narodowego. Tutaj już nieco więcej – 19% ankietowanych byłaby skłonna zrezygnować z prywatności, by zapewnić służbom bezpieczeństwa odpowiednie informacje. Nadal 81% jest przeciwna temu pomysłowi, ponad wszystko ceniąc swoją prywatność. Pozwala to w pełni zweryfikować tezę H3.

5. Wnioski

Wspierając przeprowadzone badanie, artykuł miał na celu ocenę świadomości studentów informatyki w zakresie bezpieczeństwa komunikatorów internetowych. Artykuł odpowiedział na 3 postawione przed nim hipotezy. Dwie z nich zostały zweryfikowane, jedna z kolei obalona. Dodatkowo pozwolił na wysunięcie kilku wniosków, które mogą być przydatne zarówno dla użytkowników jak i twórców oprogramowania.

Przede wszystkim rynkiem komunikatorów internetowych steruje ich popularność i bardzo ciężko przełamać tę barierę alternatywnym podejściem. Duża baza użytkowników jest głównym powodem używania konkretnych rozwiązań, stąd też komunikatory wywodzące się z sieci społecznościowych cieszą się bardzo dużym zainteresowaniem. Bezpieczeństwo schodzi na drugi plan. Nawet świadomi użytkownicy rzadko kierują się tym kryterium podczas wyboru.. Wybierają komunikatory, na których już są ich znajomi, tym samym jeszcze bardziej powiększając ich bazę użytkowników.

Duża wiedza o cyberbezpieczeństwie może jednak pozytywnie wpłynąć na sposób korzystania z komunikatorów internetowych oraz oczekiwania wobec nich. Osoby takie mogą wpłynąć pozytywnie na bezpieczeństwo całej swojej sieci kontaktów, poprzez odpowiednie edukowanie swoich rozmówców, kiedy oprogramowanie nie robi tego dostatecznie dobrze. Może to skutkować tworzeniem się mniejszych sieci kontaktów, które będą opierać swoją komunikację na bezpieczniejszych rozwiązaniach i powoli zyskiwać nowych członków.

Niezwykle ważnym elementem dla użytkowników jest poszanowanie ich prywatności. Zdecydowana większość z nich negatywnie wypowiada się na temat jej naruszenia, nawet w takich celach jak zwiększenie bezpieczeństwa narodowego. Jednak mimo to, to właśnie Facebook Messenger (uznany w analizie za najmniej szanujący prywatność) jest najczęściej używanym komunikatorem wśród badanej grupy.

Należy także zaznaczyć, że żaden z ankietowanych nie jest ograniczony do wyboru jedynie jednego komunikatora. Zależnie od potrzeb i sieci znajomych może on korzystać z różnych rozwiązań jednocześnie.

Na koniec można wyciągnąć pewną lekcję. By zapewnić sobie bezpieczeństwo podczas używania komunikatorów internetowych, nie wystarczy jedynie wybór dobrego oprogramowania. Użytkownik oraz jego rozmówca muszą być w pełni świadomi ewentualnych zagrożeń i skutecznie im zapobiegać – w trosce o obu z nich.

Literatura

[1] Barot T., Oren, E., „Guide to chat apps.”, 2015, Tow Center for Digital Journalism, Columbia University,

[2] Holt T., Freilich J., Chermak S., „Exploring the Subculture of Ideologically Motivated Cyber-Attackers”, 2017,

[3] Mitnick K., Simon W., Wozniak S., „Sztuka podstępu. Łamałem ludzi, nie hasła.”, 2001, Wydawnictwo Helion,

[4] Karbowski M. „Podstawy Kryptografii.", 2006, Wydawnictwo Helion,

[5] Erickson J., „Hacking: The Art Of Exploitation, 2nd Edition", 2008, No Starch Press,US,

[6] Stallings W., Brown L., „Computer Security: Principles and Practice, Global Edition", 2018, Pearson Education Limited,

[7] Easttom W., „Computer Security Fundamentals", 2016, Pearson Education (US),

[8] Goodrich M., Tamassia R., „Introduction to Computer Security: Pearson New International Edition", 2013, Pearson Education Limited,

[9] Gunasekera S., „Android Apps Security", 2012. Apress,

[10] Szeliga M., Mendrala D., „Bezpieczeństwo Twojego komputera", 2004 , Wydawnictwo Helion.