JOURNAL
COMPUTER SCIENCES INSTITUTE

JCSI 26 (2023) 68–74
Received: 30 September 2022
Accepted: 26 October 2022

Researching users' knowledge in the Field of Instant Messengers Security

Badanie wiedzy użytkowników w zakresie bezpieczeństwa komunikatorów internetowych

Yevhenii Tsyliurnyk*, Oleksandr Tomenchuk, Grzegorz Kozieł

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

Abstract

Nowadays, many people contact other people through various types of social networks and instant messaging. However, these platforms are often not a secure way to exchange information among people. In recent times, most people have started to pay attention to the level of security offered by communicators and the technologies used in them, which results in the emergence of communicators focused primarily on safe communication. However, the question arises: "Are user actions not negatively affecting security?" Do users consciously choose instant messaging? Do they use modern methods to protect accounts? The conducted study confirmed the relationship between the user's actions and the security of communication. Additionally, the aspects most influencing the choice of communicator were found.

Keywords: security; instant messengers; privacy

Streszczenie

W dzisiejszych czasach wiele osób kontaktuje się z innymi ludźmi poprzez różnego typu portale społecznościowe i komunikatory internetowe. Platformy te nie są jednak często bezpiecznym sposobem wymiany informacji pomiędzy ludźmi. W ostatnich czasach większość osób zaczęła zwracać uwagę na poziom bezpieczeństwa oferowany przez komunikatory oraz wykorzystane w nich technologie, wskutek czego powstają komunikatory nastawione przede wszystkim na bezpieczną komunikację. Pojawia się jednak pytanie: „Czy działania użytkowników nie wpływają negatywnie na bezpieczeństwo?”. Czy użytkownicy świadomie wybierają komunikatory? Czy wykorzystują nowoczesne sposoby ochrony kont? Przeprowadzone badanie potwierdziło zależność między działaniami użytkownika, a bezpieczeństwem komunikacji. Dodatkowo zostały znalezione aspekty, najbardziej wpływające na wybór komunikatora.

Słowa kluczowe: bezpieczeństwo; komunikatory internetowe; prywatność

*Corresponding author

Email address: **yevhenii.tsyliurnyk@pollub.edu.pl** (Y. Tsyliurnyk)

1. Wstęp

Obecnie coraz więcej rozmów realizujemy za pomocą komunikatorów internetowych. Wykorzystujemy je zarówno w życiu prywatnym, jak i przy rozmowach służbowych. Przy komunikacji służbowej, pracodawcy często sami decydują, z jakiego narzędzia komunikacji chcą korzystać w firmie, kierując się przy tym przede wszystkim takimi aspektami jak bezpieczeństwo i wykorzystane technologie szyfrujące. Natomiast w życiu codziennym użytkownicy podczas wyboru komunikatora kierują się najczęściej popularnością wśród znajomych oraz dodatkowymi funkcjami takimi jak np. animowane emotki, możliwość prowadzenia rozmów wideo lub połączenia głosowego. Istotna jest również możliwość powiązania komunikatora z profilem na portalach społecznościowych.

Nasuwa się więc pytanie, czy dla użytkowników prywatnych istotny jest stopień bezpieczeństwa i czy wpływa to na wybór komunikatora do celów prywatnych? Aby zgłębić ten problem, postawiono 2 hipotezy robocze:

H1. Użytkownicy, dla których ważne jest bezpieczeństwo, przede wszystkim zwracają uwagę na zabezpieczenia zastosowane w komunikatorach, a dopiero później na interfejs oraz dostępną funkcjonalność.

H2. Użytkownicy dbający o swoje bezpieczeństwo używają dodatkowych funkcji komunikatorów, aby zwiększyć poziom bezpieczeństwa.

W celu zweryfikowania hipotez przeprowadzono ankietę na grupie 100 osób. Respondenci biorący udział w badaniu posiadali różny stopień wiedzy dotyczący komunikatorów oraz ich bezpieczeństwa. Połowa przebadanej grupy to studenci Politechniki Lubelskiej z kierunku Informatyka, więc możemy założyć, że ich wiedza w tym zakresie jest na wysokim poziomie. Druga połowa ankietowanych nie posiada wykształcenia kierunkowego, ale regularnie korzysta z komunikatorów. Tak dobrana grupa badawcza pozwoliła otrzymać wyniki odzwierciedlające prawdziwe grono użytkowników komunikatorów. Respondenci mogli wskazać dowolną liczbę komunikatorów, co pozwoliło dokładniej oszacować popularność każdego z dostępnych rozwiązań. Celem ankiety było sprawdzenie świadomości użytkowników o istniejących zagrożeniach, metodach zwiększenia swojego bezpieczeństwa oraz doświadczenia związanego z korzystaniem z komunikatorów internetowych.

2. Przegląd literatury

Publikacja została użyta jako przykład analizy porównawczej komunikatorów [1]. Ułatwiła ona sprecyzowa-

nie aspektów, na jakie trzeba zwrócić uwagę oraz polepszyła rozumienie współcześnie wykorzystywanych zabezpieczeń w komunikatorach. Praca opisuje jakie zagrożenia nadal występują w aplikacjach i jak ich kombinacje pozwalają złamać nawet szyfrowanie end-to-end [2]. Podobne problemy opisuje również publikacja [3]. Dla lepszego rozumienia zagrożeń musimy znać cele, jakie atakują hakerzy. Obecnie duża część ataków przeprowadzana jest nie tylko w celu zarobkowych, ale również dla pokazania swoich możliwości wpływu za pomocą szantażu na pewne grupy ludzi i ich świadomość. Znane są przypadki, w których hakerzy są ściśle związani z polityką, bezpieczeństwem narodowym i działaniami wojennymi. W pracach zostały opisane najbardziej rozpowszechnione motywy hakerów oraz to, w jaki sposób wybierają swoje cele i jakie strategie wykorzystują [4-5]. Książka „Computer security literacy: Staying safe in a digital world" pokazuje, że niemal każde działanie użytkownika sieci wpływa na jego bezpieczeństwo w Internecie [6]. Można to również wywnioskować z prac, które opisują czynniki wpływające na bezpieczeństwo systemów komputerowych [7-8]. Istnienie zagrożenia wynikającego z nieświadomych działań samych użytkowników jest obecnie dużym problemem, dlatego zadaniem twórców oprogramowania, oprócz doskonalenia bezpieczeństwa systemu, jest również poszerzanie wiedzy użytkowników o istniejących zagrożeniach i sposobach przeciwdziałania im.

W celu sprawdzenia świadomości użytkowników o istniejących zagrożeniach i wiedzy na temat cyberbezpieczeństwa została stworzona ankieta. Wyniki ankiety pozwolą na weryfikację poprawności założonych hipotez.

Książka ułatwia zrozumienie technologii, które już dawno są używane na rynku i obecnie stały się standardem szyfrowania [9]. Praca opisuje mechanizm kontroli uprawnień aplikacji, wykorzystany w OS Android i związane z nim problemy [10]. Jednym z wymienionych problemów jest nieumyślne nadanie wszystkich uprawnień, do których aplikacja żąda dostępu oraz brak świadomości użytkowników, jakie uprawienia dają dostęp do prywatnych danych.

Wiedza zaczerpnięta z wyżej wymienionych prac pozwoliła przygotować się do napisania artykułu, dobrać kryteria oceniania bezpieczeństwa badanych komunikatorów oraz prawidłowo zinterpretować wyniki z przeprowadzonej ankiety.

3. Omówienie oraz porównanie komunikatorów

Nikogo nie dziwi, że rynek komunikatorów internetowych staje się coraz większy i pojawiają się nowe aplikacje do komunikacji. Użytkownicy mają duży wybór dostępnych funkcji, dopasowanych do własnych potrzeb. Trudno opisać wszystkie funkcje każdego z komunikatorów, jednak na podstawie przeprowadzonej ankiety zostały przeanalizowane i omówione najczęściej wybierane aplikacje. Do analizy wybrane zostały najpopularniejsze [11] komunikatory, takie jak znane wszystkim: Facebook Messenger, Instagram, popularne głównie na wschodzie Telegram i Viber, oraz Microsoft Teams. Każdy komunikator jest unikalny względem wyglądu oraz dostępnych funkcji, lecz wszystkie posiadają wspólne podstawowe funkcje: wysłanie natychmiastowej wiadomości, możliwość dodania do wysyłanej wiadomości emotki, wysyłania plików graficznych, oraz możliwość połączenia głosowego lub wideo. Facebook Messenger pochodzi z największej sieci społecznościowej na całym świecie - Facebooka, na skutek czego cieszy się ogromną bazą użytkowników. Użytkownicy mogą wysyłać wiadomości, zdjęcia, filmy i inne pliki, a także reagować na wiadomości i posty znajomych. Aplikacja Facebook Messenger oferuje możliwość szyfrowania wiadomości oraz ich usuwania. Instagram należy do fotograficznych serwisów społecznościowych hostingu zdjęć, co znaczy, że komunikator pomimo wysyłania natychmiastowych wiadomości umożliwia użytkownikom edycję zdjęć i filmów, stosowanie do nich filtrów cyfrowych oraz udostępnianie ich w innych serwisach społecznościowych. W 2012 roku serwis został kupiony przez Facebook. Wielkim problemem Instagrama jest duża ilość fałszywych kont, wykorzystywanych do wysyłania spamu na platformie. Telegram to darmowy bazujący na chmurze obliczeniowej komunikator internetowy, który posiada funkcjonalność zbliżoną do mikroblogów. Użytkownicy mogą wysyłać wiadomości, zdjęcia, filmy oraz pliki dowolnego typu i rozmiaru, a także tworzyć kanały do nadawania wiadomości do nieograniczonej liczby odbiorców. Zaletą komunikatora Telegram jest szyfrowane metodą end-to-end połączeń głosowych i wideo. Jako opcję dodatkową można włączyć szyfrowanie wiadomości „punkt-punkt", co zapewnia jeszcze wyższy poziom bezpieczeństwa, jednak taka opcja nie jest dostępna dla rozmów grupowych oraz wersji desktopowej programu. Viber jest komunikatorem internetowym do prowadzenia rozmów telefonicznych. Wykorzystuje technologię Voice over IP (VoIP) przeznaczoną dla smartfonów oraz komputerów. Technologia ta jest rozwijana przez firmę Viber Media. Podobnie jak w przypadku omówionych wyżej komunikatorów użytkownicy Viber mogą przesyłać zdjęcia, filmy oraz pliki audio. Jedną z zalet tego komunikatora jest jego wieloplatformowość. Aplikacja kliencka jest dostępna na platformy Mac OS, Android, BlackBerry OS, iOS, Series 40, Symbian, Bada, Windows Phone, i Microsoft Windows. Wersja 64-bitowa dla systemów Linux jest dostępna w dwóch repozytoriach: jako .deb i .rpm przeznaczonych dla systemów Debian i Ubuntu oraz Fedora i openSUSE. Microsoft Teams jest usługą internetową opartą na chmurze, która zawiera w sobie narzędzia i usługi pozwalające na wygodną pracę zespołową. Funkcjonalność innych produktów firmy Microsoft, na przykład takich jak Microsoft Office czy Skype, które wchodzą
w skład Microsoft 365, jest bezpośrednio połączona z omawianym komunikatorem. Dzięki Microsoft Teams można pracować w trybie online w obrębie plików Excel, Word oraz PowerPoint. Opisane wyżej komunikatory internetowe różnią się nie tylko dostępnymi funkcjami, ale również podejściem twórców do bezpieczeństwa

i prywatności użytkowników. Wyniki analizy porównawczej komunikatorów przedstawiono w tabeli numer 1.

Tabela 1: Analiza porównawcza wybranych komunikatorów

Nazwa komunikatora	**Wykorzystane techniki zabezpieczające**
Facebook Messenger	Szyfrowanie podstawowe; szyfrowanie powiadomień technologią end-to-end jest wykorzystywane tylko w tajnej konwersacji; możliwość wysłania wiadomości znikających po pewnym czasie; dodatkową opcją jest możliwość włączenia powiadomień o nierozpoznanych logowaniach; możliwość włączenia uwierzytelniania dwuskładnikowego podczas logowania.
Instagram	Uwierzytelnianie dwuskładnikowe – dodatkowa opcja, która dodaje do warstwy logowania element uwierzytelniania, można ją włączyć w ustawieniach; możliwość wysłania zdjęć znikających po obejrzeniu; szyfrowanie podstawowe.
Telegram	Opiera się na protokole MTProto, który zapewnia zgodność zabezpieczeń z szybką dostawą i niezawodność przy połączeniach niskiej jakości; możliwość wysłania wiadomości znikających po pewnym czasie; szyfrowanie klient-serwer jest używane w czatach Telegram; specjalne sekretne czaty zabezpieczone szyfrowaniem end-to-end, które nie pozostawiają żadnych śladów na serwerach Telegram.
Viber	Podstawowe szyfrowanie podczas przesyłania danych; szyfrowanie end-to-end; możliwość wysłania „tajnych" wiadomości znikających po pewnym czasie; możliwość ustawienia kodu PIN, bez którego dostęp do wiadomości jest niemożliwy; funkcja ukrywania numeru telefonu.
Microsoft Teams	Do szyfrowania danych zostały wykorzystane technologie, będące standardami branżowymi, takie jak TLS i SRTP; regulowany jest dostęp do zespołu, poprzez kontrolowanie ustawień prywatności i roli gościa zespołu; technologia Advanced Threat Protection pozwala chronić użytkowników przed złośliwym oprogramowaniem ukrytym w plikach; usługa Cloud App Security identyfikuje i zapobiega podejrzanej aktywności w chmurze.

Analiza pokazała, że wszystkie badane komunikatory internetowe posiadają niezbędne szyfrowanie podstawowe. Rozwój technologii w dzisiejszych czasach powoduje, że szyfrowanie podstawowe jest bardzo proste do złamania przez hakerów, którzy potrzebują do tego coraz mniej czasu. Niektóre z wyżej wymienionych komunikatorów korzystają z szyfrowania end-to-end, co daje dużo większy poziom zabezpieczenia w porównaniu z podstawowym szyfrowaniem. Wielką zaletą szyfrowania end-to-end jest to, że tylko osoby komunikujące się mogą odczytać wiadomości w formie jawnej. Oznacza to, że przy korzystaniu z takiej formy szyfrowania wiadomość przekazywana jest bezpośrednio do finalnego odbiorcy w formie zaszyfrowanej, a po otrzymaniu wiadomości odbiorcy odszyfrowują ją samodzielnie. Ważnym elementem bezpieczeństwa jest również możliwość włączenia usuwania wiadomości po wybranym czasie.

Niestety wykorzystywane przez producenta technologie nie mogą na sto procent zagwarantować bezpieczeństwa naszych danych osobowych. Na bezpieczeństwo wpływa również zachowanie użytkownika, wykorzystywanie przez niego dodatkowych funkcji oraz kontrola nad dostępem do urządzenia. W celu sprawdzenia wpływu opisanych czynników na poziom bezpieczeństwa przeprowadzono badanie opisane w następnym rozdziale.

4. Badania

4.1. Metodyka badań

Badanie zostało przeprowadzone w dwóch etapach. Pierwszy polegał na porównaniu komunikatorów na podstawie ich specyfikacji oraz informacji dostępnych w Internecie. Wyniki porównania zostały przedstawione w rozdziale 3. Drugi etap polegał na przeprowadzeniu ankiety sprawdzającej wiedzę użytkowników w dziedzinie bezpieczeństwa użytkowania komunikatorów.

4.2. Dobór grupy badawczej

W badaniu wzięło udział 100 osób, 87 z nich w wieku 18-25 lat. Wśród uczestników 45 osób to studenci Politechniki Lubelskiej studiujące na kierunku Informatyka, pozostałych 55 respondentów to osoby studiujące na innych kierunkach i uczelniach, których życie codzienne nie jest związane z informatyką. Wszyscy respondenci na co dzień korzystają z komunikatorów internetowych, 94 osoby mają konta w co najmniej trzech z nich.

4.3. Przebieg badań

W celu uzyskania kompletnej informacji o posiadanej wiedzy, preferencjach oraz doświadczeniu respondentów zapytano ich o :

- wiedzę o bezpieczeństwie w Internecie,
- preferowane komunikatory,
- oczekiwany poziom bezpieczeństwa w różnych sytuacjach,
- aspekty wpływające na wybór komunikatora,
- korzystanie z dodatkowych funkcji komunikatorów,

- popularne sposobach podnoszenia poziomu bezpieczeństwa,
- doświadczenia związane z wyciekiem danych.

Wyniki ankiety poddano analizie, a uzyskane wnioski opisano w dalszej części artykułu. Dla lepszego rozumienia wyników, odpowiedzi na niektóre pytania analizowano dzieląc respondentów na grupy.

5. Dyskusja wyników

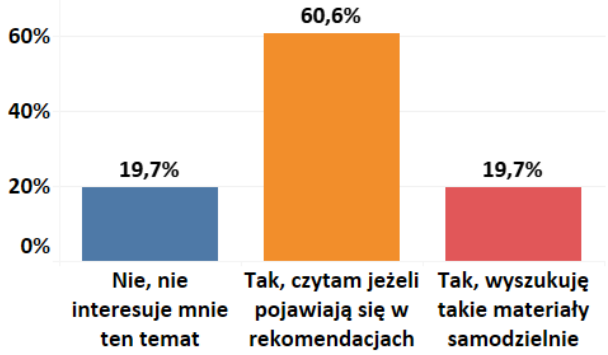
Ankieta została przeprowadzona na różnorodnej grupie respondentów, część z nich jest ściśle związana ze sferą IT, inni mają z nią do czynienia sporadyczne. Taka grupa pozwoliła na otrzymanie wyników charakteryzujących szerokie grono użytkowników komunikatorów.

Na początku zapytano ankietowanych o to, czy dbają o swoje bezpieczeństwo w Internecie. Takie pytanie wprost pozwala zobaczyć, ile osób jest świadomych istnienia zagrożeń oraz gotowych do przeciwdziałania im. Wyniki zaprezentowano na Rysunku 1.

Rysunek 1: Grupy użytkowników o różnym zaangażowaniu w dbałość o własne bezpieczeństwo w Internecie.

Zdecydowana większość (71%) odpowiedziała „Tak". Tylko 8% ankietowanych zadeklarowało, że nie zwraca uwagi na zagrożenia pochodzące z sieci. Część osób (26%) nie potrafiła konkretnie odpowiedzieć na to pytanie. Wyniki pokazują, że temat bezpieczeństwa jest znany większości osób i są one gotowi dokonywać pewnych działań, aby chronić swoją prywatność.

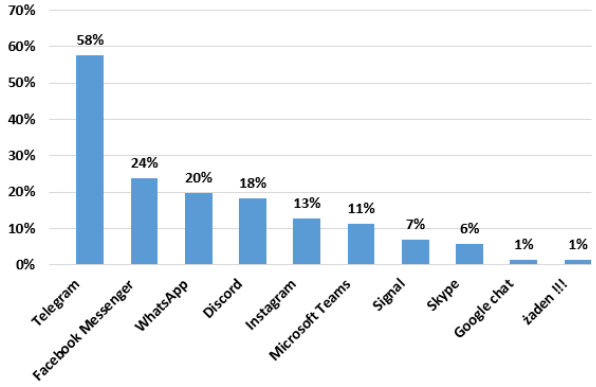
Następnie zapytano respondentów, czy interesują się informacjami na temat cyberbezpieczeństwa, wycieków danych lub ataków hakerskich. Na Rysunku 2 zaprezentowano odpowiedzi osób, które uważają, że dbają o swoje bezpieczeństwo w Internecie.



Rysunek 2: Zainteresowanie informacjami na temat bezpieczeństwa.

Jak widać na wykresie, tylko 20% respondentów omija ten temat, a zdecydowana większość osób badanych rozszerza swoją wiedzę w zakresie bezpieczeństwa. Warto zauważyć, że 60% badanych nie wyszukuje samodzielnie informacji, ale są zainteresowani artykułami, kiedy te pojawiają się w rekomendacjach lub jako reklama. Sugeruje to, że twórcy oprogramowania mogą znacząco wzbogacić wiedzę użytkowników w temacie bezpieczeństwa, dodając do swoich komunikatorów rekomendacje lub sugestie dotyczące bezpieczeństwa.

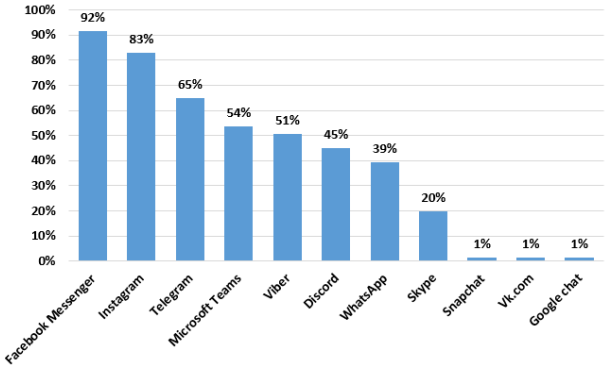
Respondentów zapytano również, który ze znanych im komunikatorów uważają za najbardziej bezpieczny. W tym pytaniu respondenci mogli wskazać dowolną liczbę komunikatorów, które one uważają za bezpieczne. Na Rysunku 3 przedstawiono wyniki pochodzące od grupy osób, które raportują, że dbają o swoje bezpieczeństwo w Internecie.



Rysunek 3: Jaki komunikator respondenci uważają za bezpieczny.

Widzimy, że większość pytanych osób uważa za najbardziej bezpieczny komunikator Telegram. Opierając się na przedstawionej powyżej analizie porównawczej komunikatorów, możemy stwierdzić, że jest to odpowiedź zbliżona do faktycznych danych. Kolejnym komunikatorem uważanym za bezpieczny jest FB Messenger, na który oddało głos 24% respondentów, niestety podczas analizy okazało się, że komunikator ten nie używa szyfrowania end-to-end, a w Internecie jest dużo informacji o wyciekach danych osobowych. Trzecie miejsce zajmuje WhatsApp, mimo tego, że ten komunikator również miał duże problemy z wyciekami danych. Ciekawe, że Viber, Signal i MS Teams mają dość przeciętne oceny, chociaż ich bezpieczność jest na wysokim poziomie, porównywalnym z Telegram-em.

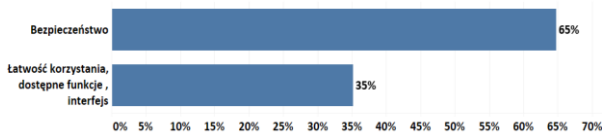
W następnym punkcie grupę respondentów raportujących zainteresowanie własnym bezpieczeństwem zapytano, z jakich komunikatorów korzystają, odpowiedzi przedstawiono na Rysunku 4.



Rysunek 4: Używane przez respondentów komunikatory.

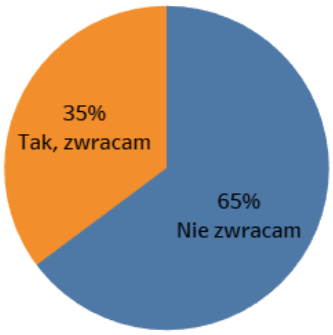
Jak widzimy, największą popularnością cieszą się komunikatory wywodzące się z sieci społecznościowych: Messenger i Instagram. Jest to spowodowane przede wszystkim tym, że wiele osób korzysta tylko z tych komunikatorów, co zmusza innych użytkowników do rozmów za pomocą tych aplikacji. Trzy kolejne miejsca zajmują Telegram, MS Teams oraz Viber, które są komunikatorami oferującymi wysoki stopnień bezpieczeństwa.

Aby określić czy użytkownicy dbający o swoje bezpieczeństwo w Internecie wybierają komunikatory ze względu na ich zabezpieczenia, zapytano ich: „Czy łatwość korzystania, dostępne funkcje oraz interfejs komunikatora mają dla Ciebie większe znaczenie niż bezpieczeństwo?”. Uzyskane wyniki zostały umieszczone na Rysunku 5.



Rysunek 5: Procent użytkowników wybierających łatwość korzystania, dostępne funkcje oraz interfejs komunikatora a nie bezpieczeństwo.

Około 65 procent użytkowników zadeklarowało, że bezpieczeństwo jest ważniejsze niż łatwość korzystania i dostępność dodatkowych funkcji w komunikatorze. Ważnym aspektem wpływającym na bezpieczeństwo komunikatora jest przesyłanie danych w postaci zaszyfrowanej. Respondentów zapytano, czy przy wyborze komunikatora zwracają uwagę na obecność szyfrowania przesyłanych danych oraz, czy rodzaj użytego szyfrowania ma dla nich znaczenie. Na Rysunku 6 i Rysunku 7 przedstawiono uzyskane wyniki.



Rysunek 6: Procent użytkowników zwracających uwagę na obecność szyfrowania przy wyborze komunikatora.

Z uzyskanych wyników możemy wywnioskować, że tylko 35% użytkowników przy wyborze komunikatora zwracają uwagę na obecność szyfrowania, a rodzaj użytego szyfrowania ma znaczenie tylko dla 8% odpytanych. Kolejnym punktem ważnym z punktu widzenia bezpieczeństwa jest wykorzystywanie aktualnych wersji oprogramowania oraz bieżące instalowanie aktualizacji bezpieczeństwa. W ankiecie zapytano użytkowników: „Czy dla Ciebie jest ważne korzystanie z najnowszej wersji komunikatora?”, odpowiedzi przedstawiono na Rysunku 8.

Rysunek 7: Procent użytkowników dla których ma znaczenie rodzaj użytego szyfrowania.

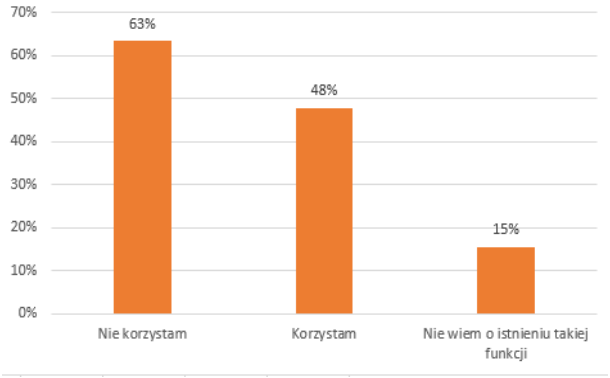
Rysunek 8: Procent użytkowników dla których ważne jest korzystanie z najnowszej wersji oprogramowania.

Jak i w poprzednich pytaniach, mimo zadeklarowanego dbania o swoje bezpieczeństwo, większość respondentów nie zwraca uwagi na aktualność używanego oprogramowania. Jednak w przypadku korzystania z komunikatorów na urządzeniach mobilnych domyślnie jest ustawiona automatyczna aktualizacja, co powoduje, że większość użytkowników i tak posiada aktualne wersje programów.

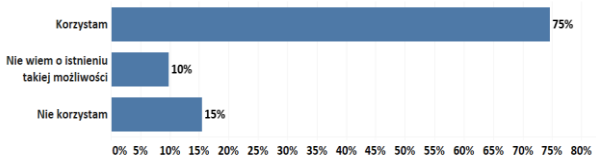
Uzyskane odpowiedzi pozwalają obalić hipotezę H1. Mimo deklarowanego dbania o swoje bezpieczeństwo większość użytkowników nie zwraca uwagi na podstawowe aspekty wpływające na zabezpieczenie komunikatora. Oprócz tego przy wyborze komunikatora użytkownicy kierują się jego popularnością i nadają przewagę komunikatorom wywodzącym się z sieci społecznościowych.

Niektóre komunikatory posiadają dodatkowe funkcjonalności pozwalające zwiększyć ochronę przesyłanych danych. Jednak problem polega na tym, że użytkownik musi wiedzieć o ich istnieniu oraz używać w odpowiednim momencie. Jedną z takich funkcji jest usuwanie wiadomości po określonym czasie. Rysunku 9 przedstawia jaki procent respondentów dbających o swoje bezpieczeństwo z niej korzysta.

Wśród wybranej grupy mniej niż połowa osób używa tej funkcji. W przypadku uzyskania fizycznego dostępu do urządzenia pozwoli to na przeczytanie wszystkich wysłanych wcześniej wiadomości. Następnym ważnym elementem bezpieczeństwa jest dwuetapowa autentyfikacja. Ten mechanizm pozwala chronić konto nawet w przypadku gdy hasło zostanie skompromitowane. Na Rysunku 10 przedstawiono procent użytkowników korzystających z dwuetapowej autentyfikacji.



Rysunek 9: Procent osób wykorzystujących funkcje usuwania wiadomości po określonym czasie.



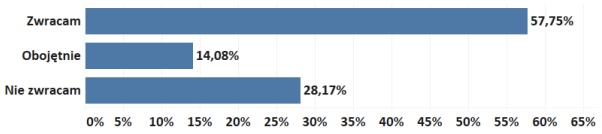
Rysunek 10: Procent osób korzystających z dwuetapowej autentyfikacji.

W tym przypadku możemy z pewnością konstatować, że zdecydowana większość grupy dba o bezpieczeństwo swojego konta. Dla potwierdzenia tego wniosku zapytano, czy dla różnych komunikatorów używane są różne hasła.

Rysunek 11: Procent użytkowników wykorzystujących różne hasła do różnych komunikatorów.

Diagram widoczny na Rysunku 11 pokazuje podobną tendencję do poprzedniego pytania, 76% użytkowników wykorzystują unikatowe hasła. Kombinacja unikatowego hasła i dwuetapowej autentyfikacji radykalnie zmniejsza ryzyko niepożądanego dostępu osób trzecich do naszego konta, i uniemożliwia wykonanie działań na koncie bez naszej wiedzy.

Często jednak oprócz samego komunikatora i zachowania użytkownika pojawia się trzeci czynnik wpływający na bezpieczeństwo informacji – system, na którym działa aplikacja. Najczęściej komunikatory używane są na urządzeniach mobilnych, na których zainstalowano wiele innych aplikacji. Podczas instalowania aplikacji użytkownik ma możliwość nadania jej pewnych uprawnień lub też odmówienia zgody na nadanie tychże uprawnień. Zwracanie uwagi na przydzielane uprawienia jest ważnym elementem bezpieczeństwa, gdyż niepożądany dostęp do systemu plików, kontaktów lub powiadomień może spowodować wyciek danych mimo wszystkich użytych w komunikatorze zabezpieczeń. Rysunek 12 przedstawia procent użytkowników zwracających uwagę na uprawnienia aplikacji podczas jej instalowania.

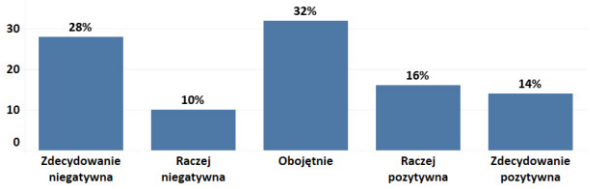


Rysunek 12: Procent użytkowników zwracających uwagę na uprawienia aplikacji pod czas instalowania.

Prawie 58% respondentów kontroluje, jakie uprawnienia są nadawane aplikacjom podczas instalowania. Jednak więcej niż 28% nie zwraca na to uwagi, czym naraża na niebezpieczeństwo nie tylko siebie, a również swoich współrozmówców.

Biorąc pod uwagę uzyskane wyniki, możemy częściowo potwierdzić hipotezę H2. Zdecydowana większość respondentów dobrze zabezpiecza swoje konta przed włamaniami. Również duża część użytkowników dbających o swoje bezpieczeństwo używa dodatkowych funkcji komunikatorów zwiększając swoje bezpieczeństwo. Jednak nadal pozostaje od 25 do 50 procent osób, zaniedbujących pewne aspekty bezpieczeństwa komunikatorów.

Dodatkowo zdecydowano się sprawdzić opinie użytkowników odnośnie możliwości analizy wysyłanych wiadomości w celach marketingowych. Respondentom zadano pytanie: „Jaka jest Twoja opinia na temat możliwej analizy wysłanych wiadomości przez twórcę oprogramowania?”. Respondenci udzielali odpowiedzi w pięciostopniowej skali - od „Zdecydowanie negatywnej” do „Zdecydowanie pozytywnej”. Wyniki zaprezentowano na Rysunku 13.



Rysunek 13: Opinia użytkowników na temat możliwej analizy wysłanych wiadomości.

Jak wynika z przeprowadzonego badania, liczna grupa respondentów odnosi się obojętnie do faktu analizy wysyłanych wiadomości, a kolejne 30% pozytywnie. Sama z siebie analiza wiadomości nie niesie dużego zagrożenia dla użytkowników, jednak świadczy o tym, że w konkretnym komunikatorze nie jest wykorzystywana metoda szyfrowania end-to-end, a wiadomości są w jakiś sposób otwierane i zapisywane na serwerach. Kombinacja tych dwóch czynników zwiększa ryzyko wycieku prywatnych danych w przypadku ataku na serwery komunikatora oraz robi go bardziej atrakcyjną celą dla hackerów.

6. Wnioski

Celem artykułu było zbadanie wiedzy użytkowników w zakresie bezpieczeństwa komunikatorów internetowych. Analizując dane przeprowadzonej ankiety, udało się zweryfikować pierwszą hipotezę i częściowo po-

twierdzić drugą. W procesie analizy wyników udało się wysunąć wnioski przydatne dla twórców komunikatorów oraz rekomendacje dla użytkowników.

Istotne jest to, że duża liczba użytkowników jest świadoma istniejących zagrożeń i gotowa wykonywać dodatkowe czynności, aby zwiększyć swoje bezpieczeństwo. Około 80% użytkowników zwracają uwagę na informacje o wyciekach danych, atakach hakerskich i wykrytych lukach bezpieczeństwa. Temat ten jednak nie jest dla większości użytkowników na tyle ciekawy, by samodzielnie poszukiwali wiedzy z tej dziedziny, więc zadaniem twórców oprogramowania jest dostarczanie użytkownikom informacji pozwalających na zwiększenie poziomu ich świadomości.

Istotny jest fakt, że mimo wiedzy o zagrożeniach oraz istnieniu lepiej zabezpieczonych komunikatorów użytkownicy dalej użytkują FB Messenger i Instagram, ze względu na ich popularność. Duża grupa użytkowników i dostępność niektórych znajomych wyłącznie na tych portalach w większości przypadków przeważa nad bezpieczeństwem danych. Natomiast trzy kolejne miejsca zajmują komunikatory z wysokim poziomem bezpieczeństwa, co świadczy o świadomym wyborze tych komunikatorów jako alternatywy i stopniowym przejściu na lepiej zabezpieczone kanały komunikacji.

Warto również zauważyć, że respondenci ceniący sobie bezpieczeństwo wykorzystują więcej dodatkowych możliwości podnoszenia poziomu własnego bezpieczeństwa i dobrze chronią swoje konta i urządzenia przed włamaniem.

Podsumowując, możemy powiedzieć, że wybór bezpiecznego komunikatora nie jest wystarczający do zapewnienia bezpiecznej komunikacji. Użytkownik, jak i jego współrozmówca muszą być świadomi istniejących zagrożeń i możliwości przeciwdziałania im, gdyż grono użytkowników i ich działania bezpośrednio wpływają na poziom bezpieczeństwa całego systemu.

Literatura

[1] J. Botha, C. Van't Wout, L. Leenen, A comparison of chat applications in terms of security and privacy, 18th European Conference on Cyber Warfare and Security (2019) 55-62.

[2] S. Prabhune, S. Sharma, End-to-end encryption for chat app with dynamic encryption key, 3rd International Conference on Advances in Computing Communication Control and Networking (2021) 1361-1366.

[3] J. Farnden, B. Martini, K. R. Choo, Privacy risks in mobile dating apps, 21st Americas Conference on Information Systems (2015) 118635-118647.

[4] S. Chng, H. Y. Lu, A. Kumar, D. Yau, Hacker types, motivations and strategies: A comprehensive framework, Computers in Human Behavior Reports 5 (2022) 100167 – 100175.

[5] K. Owen, M. Head, Motivation and demotivation of hackers in selecting a hacking task, Journal of Computer Information Systems 1 (2022) 1-15.

[6] D. Jacobson, J. Idziorek, Computer security literacy: Staying safe in a digital world, CRC Press, US, 2016.

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

[8] A. Kovacevic, N. Putnik, O. Toskovic, Factors related to cyber security behavior, IEEE Access 8 (2020) 125140-125148.

[9] M. Karbowski, Podstawy Kryptografii, Wydawnictwo Helion, 2006.

[10] Z. Fang, W. Han, Y. Li, Permission based android security: Issues and countermeasures, Computers and Security 43 (2014) 205-218

[11] Wyniki badania popularności komunikatorów za czerwiec 2022, https://pbi.org.pl/badanie-mediapanel/wyniki-badania-mediapanel-za-czerwiec-2022/, [29.09.2022].