

Jak wiele informacji o sobie udostępniamy w Internecie

Paulina Brzęcka 184701 Marek Borzyszkowski 184266

30 marca 2025

SPIS TREŚCI

SPIS TREŚCI.....	2
1. WSTĘP I CEL RAPORTU	3
1.1. Cel pracy	3
2. ŹRÓDŁA POZYSKIWANIA INFORMACJI	4
2.1. Identyfikacja i analiza publicznie dostępnych źródeł	4
2.1.1. Media społecznościowe	4
2.1.2. Fora, sekcje komentarzy, blogi.....	5
2.1.3. Rejestry publiczne i portale firmowe	5
2.1.4. Urządzenia IoT	6
2.1.5. Czat AI jako nieświadome źródło informacji.....	6
2.2. W jaki sposób dane trafiają w niepowołane ręce?	7
3. ZAGROŻENIA.....	8
3.1. Zagrożenia wynikające z udostępniania danych	8
3.1.1. Wprowadzenie	8
3.1.2. Kradzież tożsamości	8
3.1.3. Naruszenie prywatności i poufności danych	9
3.1.4. Cyberstalking i nękanie	12
3.1.5. Oszustwa socjotechniczne i internetowe.....	15
3.1.6. Konsekwencje reputacyjne	16
3.1.7. Odpowiedzialność prawna.....	17
4. ZALECENIA DOTYCZĄCE PRYWATNOŚCI	19
4.1. Czego nie udostępniać w internecie?.....	19
4.1.1. Adres e-mail i numer telefonu	19
4.1.2. Adres domowy i lokalizacja geograficzna	19
4.1.3. Zdjęcia nieletnich	19
4.1.4. Kompromitujące zdjęcia.....	19
4.1.5. Dokumenty osobiste	19
4.1.6. Opinia, skargi i kontrowersyjne komentarze.....	19
4.1.7. Prywatne rozmowy.....	19
4.2. Jak się chronić?.....	19
WYKAZ LITERATURY	22

1. WSTĘP I CEL RAPORTU

W dobie powszechnej cyfryzacji coraz więcej aspektów naszego życia przenosi się do świata wirtualnego. Codziennie korzystamy z mediów społecznościowych, wyszukiwarek internetowych, aplikacji mobilnych i wielu innych platform, nie zawsze zastanawiając się, jakie informacje o sobie udostępniamy i jakie mogą być tego konsekwencje. Dane, które pozostawiamy w sieci - świadomie lub nieświadomie - mogą obejmować zarówno podstawowe informacje, takie jak imię i nazwisko, wiek czy miejsce zamieszkania, jak i bardziej wrażliwe dane, takie jak zainteresowania, preferencje zakupowe czy historia przeglądania stron. Współczesny Internet sprawia, że budowanie profilu użytkownika na podstawie dostępnych informacji jest niezwykle łatwe, a same dane mogą być wykorzystywane na różne sposoby przez rozmaite podmioty.

Niniejszy raport ma na celu analizę skali i sposobów udostępniania danych w Internecie. W kolejnych rozdziałach omówiona zostanie budowa profilu użytkownika na podstawie podstawowych informacji, źródła pozyskiwania danych oraz sposoby ich wykorzystywania przez firmy, instytucje i inne organizacje. Szczególna uwaga zostanie poświęcona zagrożeniom wynikającym z nadmiernego udostępniania informacji, takim jak kradzież tożsamości, nieuprawnione śledzenie aktywności czy manipulacja preferencjami użytkowników. W końcowej części raportu przedstawione zostaną rekomendacje dotyczące ochrony prywatności i minimalizacji ryzyka związanego z publikowaniem danych w sieci.

1.1. *Cel pracy*

Celem niniejszego raportu jest zbadanie, w jakim stopniu i w jaki sposób użytkownicy Internetu udostępniają swoje dane oraz jakie niesie to za sobą konsekwencje. Szczególny nacisk zostanie położony na analizę różnych źródeł informacji, mechanizmów zbierania danych oraz podmiotów, które je przetwarzają i wykorzystują. Poprzez dokładne przeanalizowanie tego procesu możliwe będzie wskazanie zagrożeń związanych z nadmiernym udostępnianiem informacji oraz ocena, w jakim stopniu użytkownicy mają nad nim kontrolę.

Drugim, równie istotnym celem raportu, jest przedstawienie praktycznych zaleceń dotyczących ochrony prywatności w Internecie. Omówione zostaną sposoby minimalizowania ilości udostępnianych danych, techniki zabezpieczania informacji oraz narzędzia, które mogą pomóc w ochronie tożsamości cyfrowej. Ostatecznym efektem pracy będzie zwiększenie świadomości czytelników na temat zagrożeń i sposobów zabezpieczenia swoich danych w sieci, co pozwoli im podejmować bardziej świadome decyzje dotyczące własnej prywatności.

2. ŹRÓDŁA POZYSKIWANIA INFORMACJI

2.1. Identyfikacja i analiza publicznie dostępnych źródeł

W dobie powszechnego dostępu do Internetu oraz ogromnej popularności mediów społecznościowych, zdobycie informacji na temat osoby prywatnej, przedsiębiorcy czy pracownika jest dziś łatwiejsze niż kiedykolwiek wcześniej. Użytkownicy często sami - świadomie lub nieświadomie - pozostawiają po sobie szereg danych, które można wykorzystać do stworzenia precyzyjnego profilu.

Według raportu „Digital 2021” (We Are Social i Hootsuite), z Internetu w Polsce korzysta 31,97 mln osób, a 25,9 mln aktywnie używa mediów społecznościowych. To oznacza, że większość społeczeństwa codziennie generuje cyfrowe ślady, które mogą być później analizowane.[1]

2.1.1. Media społecznościowe

Facebook, Instagram, X, LinkedIn czy Snapchat gromadzą dane zarówno świadomie podawane przez użytkowników (np. miejsce pracy), jak i te zbierane automatycznie - lokalizacja, adres IP, urządzenia. Dane mogą pochodzić także z aplikacji firm trzecich, programów lojalnościowych czy partnerów marketingowych.[2]

Szczegółowe zestawienie, jakie dane są gromadzone w mediach społecznościowych zostały przedstawione w poniższej tabeli. [3]

Zakres danych / Działanie	Facebook	X	LinkedIn
DANE OSOBOWE			
Imię i nazwisko	+	+	+
E-mail	+	+	+
Numer telefonu	+	+	+
Data urodzenia	+	+	+
Adres zamieszkania	+	+	+
Poprzednie miejsca zamieszkania	+		
Zdjęcia profilowe	+	+	+
Rodzina i związki	+		
Wykształcenie	+		+
Języki obce	+		+
Poglądy polityczne	+		
Przekonania religijne	+		
Wydarzenia z życia	+		
DANE ZAWODOWE I LOKALIZACYJNE			
Miejsce pracy	+		+
Kwalifikacje	+		+
Wynagrodzenie			+
Płatności	+		+
Lokalizacja	+	+	+
Urządzenia	+	+	+
Adres IP	+	+	+

Kalendarz			+
ŹRÓDŁA POZYSKIWANIA INFORMACJI			
Od użytkownika	+	+	+
Od innych użytkowników	+	+	+
Od partnerów zewnętrznych	+		+
Z aplikacji zewnętrznych	+	+	
Z aktywności (kliknięcia)	+	+	
ZASTOSOWANIA I UDOSTĘPNIANIE			
Reklamy	+	+	+
Personalizacja	+	+	+
Oznaczanie na zdjęciach	+		
Meldowanie w lokalizacjach	+	+	
Sugestie kontaktów	+		+
Udostępnianie firmom	+	+	+
Cele badawcze i analityczne	+	+	+

Jesli chodzi o Facebook, to gromadzi on najszerszy zakres danych - zarówno prywatnych, jak i zawodowych, w tym dane kontaktowe, lokalizacyjne, relacyjne i behawioralne. Dane są również pozyskiwane od partnerów i aplikacji zewnętrznych. Warto zaznaczyć, że domyślne ustawienia prywatności, których większość użytkowników nigdy dokładnie nie czyta przed akceptacją, bardzo często sprzyjają upublicznieniu informacji, a około 40% użytkowników nie zmienia nigdy ustawień prywatności, co czyni ich dane łatwo dostępnymi.

W aplikacji X domyślnie wszystkie posty (tweety) są publiczne. Dodatkowo dane gromadzone również poprzez partnerów i aplikacje zewnętrzne, a polityka firmy jest dosyć liberalna i udostępnia dane badaczom.

Firma LinkedIn dodatkowo profiluje użytkowników głównie pod kątem danych zawodowych (miejsce pracy, kwalifikacje, języki), które potem są wykorzystywane komercyjnie i sprzedawane firmom rekrutacyjnym. Może być to szczególnie niebezpieczne przy atakach typu spear-phishing, gdzie precyzyjne informacje są używane do podszywania się i oszustw.

2.1.2. *Fora, sekcje komentarzy, blogi*

Uznawane za „anonimowe”, w rzeczywistości łatwe do deanonimizacji. Powtarzające się pseudonimy, zdjęcia profilowe, adresy IP - wszystko to pozwala powiązać konto z konkretną osobą, po mniej lub bardziej wnikliwym poszukiwaniu.

2.1.3. *Rejestry publiczne i portale firmowe*

Z racji powszechnej cyfryzacji, przed udostępnieniem niektórych danych w internecie nie można się uchronić. Szczególnie osoby prowadzące firmy lub działalności gospodarcze, a nawet osoby posiadające nieruchomości. Nie wspominając o tym, że prawie każdy dorosły człowiek w dzisiejszych czasach pracuje w jakiejś firmie, gdzie często dane kontaktowe, adresy e-mail, a czasem także numery telefonów pracowników czy właścicieli firm są udostępniane na stronie firm, bardzo często nawet bez wiedzy samych zainteresowanych.[4]

Niektóre dane są dostępne w postaci rejestrów internetowych:

- **CEIDG** - zawiera dane o jednoosobowej działalności gospodarczej, w tym adres, który nierzadko

jest miejscem zamieszkania.

- **KRS** - dane zarządu, często z numerem PESEL, umożliwia pozyskanie numeru PESEL i daty urodzenia członków zarządu spółek.
- **CRBR** - udostępnia dane beneficjentów rzeczywistych, w tym numery PESEL udziałowców spółek.
- **Elektroniczne Księgi Wieczyste** - umożliwiają dotarcie do danych właścicieli nieruchomości.
- **Portale ogłoszeniowe, firmowe** - e-maile, telefony, nazwiska

2.1.4. Urządzenia IoT

Inteligentne urządzenia domowe (głośniki, żarówki, lodówki) zbierają dane o rutynie, lokalizacji i obecności użytkownika. Coraz więcej urządzeń domowych (np. tostery, żarówki, głośniki) jest wyposażonych w moduły internetowe. Nawet jeśli nie oferują realnych funkcji online, dane z nich są zbierane i mogą być wykorzystywane marketingowo. Koszt wdrożenia łączności IoT dla producenta jest niewielki, a dane mają wysoką wartość.

„Kupując sprzęt domowy, możemy nieświadomie nabyć urządzenie IoT. Kluczowym zasobem są dane - które mogą zostać sprzedane lub wykorzystane przez producenta.” - Mikko Hypponen

2.1.5. Czat AI jako nieświadome źródło informacji

Coraz więcej osób korzysta z narzędzi opartych na sztucznej inteligencji (AI), takich jak ChatGPT czy Bing Chat, aby wspierać się w pracy zawodowej. Według badań aż 43% pracowników używa AI do realizacji swoich zadań.[5] Choć AI oferuje wygodne i szybkie odpowiedzi, istnieją zagrożenia dotyczące prywatności i bezpieczeństwa danych, o których warto pamiętać, że:

- dane mogą być przetwarzane lub analizowane przez ludzi,
- platformy zastrzegają prawo do przechowywania zapytań,
- AI modele, takie jak ChatGPT, mogą uczyć się na podstawie zadawanych pytań. Dlatego nie powinno się wprowadzać do nich żadnych danych osobowych ani poufnych.

Co zdarza się ludziom udostępnić, a nie powinno się tego robić:

- Imię i nazwisko,
- Data urodzenia,
- Adres zamieszkania,
- Numer dowodu osobistego,
- Telefon, adres e-mail,
- Kod źródłowy lub dane z projektów w fazie rozwoju,
- Poufne informacje o produktach i usługach,
- Niezaprezentowane jeszcze pomysły lub rozwiązania,
- Numery kart kredytowych,
- Numery kont bankowych,
- Hasła i dane logowania,
- Wyniki badań,

- Diagnozy lekarskie,
- Informacje dotyczące leczenia.

Aby korzystać z AI w sposób odpowiedzialny i bezpieczny, warto stosować się do kilku prostych zasad:

- Używanie jedynie informacji ogólnodostępnych i nieidentyfikujących,
- Podawanie dane fikcyjne lub zanonimizowane, jeśli konieczne jest podanie przykładu.
- Nie publikowanie szczegółowych planów podróży lub wakacji — może to narażać na kradzież lub inne ryzyko offline.
- Założenie drugiego, anonimowego konta, które nie jest powiązane z właściwą tożsamością.
- Korzystanie z bezpiecznego połączenia internetowego — unikanie otwartych sieci Wi-Fi w kawiarniach czy hotelach.
- Nie udostępnianie haseł ani nie proszenie AI o ich generowanie na potrzeby konkretnej usługi.
- Zachowanie ostrożności przy danych zdrowotnych, finansowych i prywatnych,
- Zapoznanie się z regulaminem i polityką prywatności chatu AI,
- Sprawdzenie, jakie dane są przechowywane, jak długo i komu mogą być udostępniane,
- Zwrócenie uwagi, czy narzędzie przewiduje możliwość przeglądu zapytań przez człowieka w celach jakościowych.

2.2. W jaki sposób dane trafiają w niepowołane ręce?

Chociaż skoro myślimy, że udostępniamy bardzo mało danych, bądź wcale, istnieją aktualnie techniki, które są na tyle zaawansowane, że na podstawie jednej, bądź kilku informacji można stworzyć czyiś profil osobowy. Do jednej z nich zalicza się biały wywiad. Open Source Intelligence, czyli biały wywiad, to wyspecjalizowana technika polegająca na analizie dostępnych publicznie informacji w celu identyfikacji i gromadzenia danych o wybranej osobie.

- przeszukiwanie stron internetowych pod kątem danych kontaktowych,
- wyszukiwanie kont społecznościowych na podstawie adresu e-mail lub loginu,
- analizę zdjęć w celu rozpoznania wizerunku i odnalezienia powiązanych treści,
- korelowanie fragmentarycznych danych z różnych źródeł (np. fora, blogi, komentarze).

Aktualne narzędzie umożliwiają bardzo wnikliwą analizę, między innymi:

- automatyczne przeszukiwanie domen internetowych w celu odnalezienia adresów e-mail,
- sprawdzanie, na jakich portalach społecznościowych zarejestrowano konkretne nazwy użytkowników,
- analizę zdjęć za pomocą sztucznej inteligencji w celu identyfikacji osoby.

Chociaż prawda jest taka, że nie potrzeba żadnych profesjonalnych narzędzi, aby komuś uprzykrzyć życie. Dostęp do danych wrażliwych może mieć każda osoba prywatna, wystarczy tylko odrobina negatywnej motywacji oraz chwila czasu spędzona na poszukiwaniu i wnioskowaniu, ale o tym więcej w następnych rozdziałach.

3. ZAGROŻENIA

3.1. Zagrożenia wynikające z udostępniania danych

3.1.1. Wprowadzenie

Współczesne organizacje i użytkownicy indywidualni coraz częściej stają się ofiarami zagrożeń wynikających z niekontrolowanego udostępniania danych. Informacje osobiste mogą zostać wykorzystane zarówno przez zewnętrznych atakujących, jak i osoby z wewnątrz firmy — obecnych lub byłych pracowników, kontrahentów, a nawet przypadkowych użytkowników popełniających błędy.

Najczęstsze błędy popełniane przez użytkowników to:

- publikowanie selfie z oznaczeniem daty i lokalizacji,
- udostępnianie postów o planowanych lub trwających wyjazdach wakacyjnych,
- włączona na stałe geolokalizacja w telefonie
- stosowanie haseł łatwych do odgadnięcia, np. oparte na imionach członków rodziny lub zwierząt, dat urodzin i braku zmiany hasła co jakiś czas,
- hejtowanie, umieszczanie kontrowersyjnych treści w internecie.

Przestępcy mogą wykorzystać te dane do okradzenia mieszkania. Firmy windykacyjne mogą szybciej ustalić lokalizację użytkownika. Złodzieje mogą śledzić nawyki i rutynę użytkownika z pomocą danych GPS.

Z kolei stworzenie listy kombinacji haseł na podstawie udostępnianych w internecie informacji nie wymaga specjalistycznej wiedzy i pozwala na złamanie hasła w krótkim czasie. Ujawnianie danych osobistych i zwyczajów może prowadzić do łatwego odgadnięcia haseł do kont społecznościowych, bankowości elektronicznej, poczty, czy chmur obliczeniowych. Może to skutkować utratą danych osobistych i prywatnych zasobów, a także podszywanie się pod użytkownika, aby móc wyłudzić informacje lub pieniądze.

Kontrowersyjne treści publikowane w internecie mogą skutkować:

- Problemami zawodowymi - kontrowersyjne komentarze mogą dotrzeć do pracodawcy.
- Pozwem cywilnym - za naruszenie dóbr osobistych innych osób.
- Utratą reputacji - zarówno prywatnej, jak i zawodowej.

W następnej sekcji przedstawiono opis konkretnych zagrożeń wraz z przykładami z życia codziennego. [6, 7]

3.1.2. Kradzież tożsamości

Opis zagrożenia

Udostępnienie danych osobowych, takich jak imię, nazwisko, PESEL, numer dowodu czy adres e-mail, może skutkować:

- podszywaniem się pod ofiarę w celu zaciągnięcia pożyczki, otwarcia konta bankowego czy przeprowadzenia transakcji,
- wykorzystaniem danych w oszustwach ubezpieczeniowych, zdrowotnych lub podatkowych,

- długoterminowymi problemami finansowymi i prawnymi ofiary.

Przykłady z życia

W ataku na Marriott w 2020 r. wyciekło ponad 5 mln rekordów gości, zawierających dane kontaktowe, urodziny i numery kont lojalnościowych.

5 maja 2020 roku w internecie błędnie zidentyfikowano CEO firmy Propine, Tuhinę Singh, jako kobietę z Singapuru, która została aresztowana po tym, jak w viralowym nagraniu odmówiła założenia maseczki w miejscu publicznym. W wyniku pomyłki internauci zaczęli publikować jej zdjęcia, numer telefonu, prywatny adres e-mail oraz dane jej współpracowników, co doprowadziło do fali gróźb i rasistowskich obelg. Skala nagonki była na tyle duża, że firma Propine wydała oficjalne oświadczenie, w którym wyjaśniła, że doszło do pomyłki, a prawdziwa sprawczyni została już zidentyfikowana i odpowiednio ukarana przez władze.

3.1.3. Naruszenie prywatności i poufności danych

Opis zagrożenia

Dane, które zostaną ujawnione - nawet nieświadomie - mogą naruszyć prywatność pracowników, klientów czy partnerów biznesowych. Skutki to:

- utrata kontroli nad własnymi informacjami,
- możliwość ich dalszego rozpowszechniania,
- narażenie na nieautoryzowane monitorowanie.

Przykłady z życia

Były pracownik Tesli w 2023 r. ujawnił dane ponad 75 000 pracowników, w tym numery SSN i informacje finansowe.


W kwietniu 2020 roku w Meridian (Idaho) policjant aresztował kobietę, która odmówiła opuszczenia zamkniętej części parku publicznego. Ograniczenie było związane z lockdownem COVID-19. Inne części parku pozostały otwarte. Po nagłośnieniu sprawy, libertariańska organizacja Idaho Freedom Foundation opublikowała na Facebooku imię, nazwisko i zdjęcie funkcjonariusza, wzywając ludzi, by „dali znać departamentowi policji w Meridian, co o tym sądzą”. Dodatkowo, lider grupy Ammon Bundy rozpowszechnił adres domowy policjanta, m.in. wysyłając go na listę mailingową i zapisując na tablicy podczas spotkania grupy. Nagranie z widocznym adresem obejrzano ponad 1200 razy. Bundy wcześniej twierdził, że „jeśli prawa jakiejś osoby są łamane, tysiące ludzi powinno ją otoczyć, nagłośnić sprawę i pociągnąć sprawców do odpowiedzialności”. Wypowiadał się też za obecnością broni na protestach, mówiąc: „Pierwsza poprawka jest chroniona przez drugą”. W wyniku ujawnienia danych osobowych, przed domem policjanta zebrały się dziesiątki protestujących, żądając, by przyjął 13-stronicową skargę. Republikański poseł z Idaho, Greg Chaney, skomentował, że działania Bundy’ego narażyły policjanta i jego rodzinę na poważne zagrożenie i ryzyko.



Idaho Freedom Foundation



53 mins •

This is  He authorized the arrest of Sarah Walton Brady today at a Meridian Park.

Let the Meridian Police Department know how you feel.



   63

39 Comments • 20 Shares




Like



Comment



Share

 Learn More



W marcu 2025 roku w Niebezpieczniku[8] pojawiło się ogłoszenie dotyczące sprzedaży rzekomej bazy danych zawierającej informacje o 24 milionach klientów Empiku. Zgodnie z opisem, baza miała zawierać takie dane jak: imię i nazwisko, numer telefonu, adres (zamieszkania lub dostawy), adres e-mail oraz informacje o zamówieniach (ich liczba i daty). Co istotne, w ogłoszeniu oraz w udostępnionej próbce danych nie znalazły się żadne hasła ani ich hashe. Pojawiły się jednak wątpliwości co do autentyczności i pochodzenia danych - m.in. podejrzenie wysoka liczba rekordów (24 mln), która mogła wynikać z błędnego formatowania (sugerowano, że mogło chodzić o 2,4 mln). Sugerowano również, że źródłem danych może być nie Empik, lecz zewnętrzny system reklamowy lub trackingowy, który mógł generować duplikaty.

Empik zareagował na incydent, publikując oświadczenie, w którym poinformował, że:

- większość danych z próbki nie występuje w ich systemach,
- format danych różni się od stosowanego w systemach wewnętrznych firmy,
- część ujawnionych informacji to ogólnodostępne dane produktowe z katalogu Empik.com,
- nie doszło do wycieku haseł, historii zakupów ani danych płatniczych,
- zgodnie z normą PCI DSS firma nie przechowuje numerów kart płatniczych.

Zalecano klientom zachowanie ostrożności i zmianę hasła na wypadek, gdyby dane jednak pochodziły z realnego wycieku i przypomniano, że na podstawie danych takich jak nazwisko, e-mail, adres czy numer telefonu można wzajemnie ustalić inne informacje o osobie. Aktualizacja z 23 marca 2025 roku przyniosła kolejne, kluczowe oświadczenie Empiku: po szczegółowej analizie stwierdzono jednoznacznie, że rzekoma baza danych była fałszywa i została spreparowana na podstawie danych pochodzących z historycznych wycieków z innych firm, najprawdopodobniej w celu oszukania potencjalnych kupujących. Empik zapewnił, że nie doszło do żadnego incydentu bezpieczeństwa po ich stronie, dane klientów są bezpieczne, a firma natychmiast po pojawieniu się sygnałów o możliwym wycieku uruchomiła proces weryfikacji z pomocą zespołu CERT. Firma również przestrzegła przed powielaniem niezweryfikowanych informacji dotyczących bezpieczeństwa danych.

Przykłady z życia

Angela Dunn to epidemiolog nękana przez protestujących, po tym jak opublikowano ulotki z jej adresem na Facebooku, protestujący pojawili się pod jej domem, oskarżając ją o zniszczenie gospodarki przez lockdown.



Rysunek 3.4: Protesty pod domem Angeli Dunn

Laurie Jones, czyli urzędniczka zdrowia publicznego znalazła się pod ostrzałem gróźb. Po kontakcie z osobą zakażoną COVID-19, gdzie kobieta zadzwoniła do osoby zakażonej, aby przypomnieć jej o tym by została w domu, chociaż zakażona osoba tego nie przestrzegała. Pojawiły się później w internecie pod jej adresem fałszywe oskarżenia o szpiegostwo, szerzenie paniki, co wywołało falę hejtu i groźby śmierci. Kobieta doświadczyła traumy, musiała zainstalować zabezpieczenia w domu. Do dziś ma obawy przed wychodzeniem z domu i stała się chorobliwie zachowawcza.

W styczniu 2021 roku senator Mitch McConnell spotkał się z falą krytyki po tym, jak zablokował propozycję zwiększenia kwoty wypłat w ramach rządowej pomocy COVID-19. W odpowiedzi, niektórzy oburzeni obywatele odnaleźli jego domowy adres i dokonali aktu wandalizmu na jego drzwiach pojawił się napis „Gdzie są moje pieniądze?”, a na ganku umieszczono wulgarne hasła. Protest został zorganizowany przez grupę DC Under Siege, która opublikowała wydarzenie na Facebooku. Rankiem przed domem senatora zebrała się grupa demonstrantów wyposażonych w megafony i transparenty. McConnell odniósł się do zajścia, podkreślając, że docenia prawo obywateli do udziału w procesie demokratycznym, również tych, którzy się z nim nie zgadzają. Jednocześnie stanowczo potępił akty wandalizmu i zastraszania, stwierdzając, że „polityka strachu nie ma miejsca w naszym społeczeństwie”.



Rysunek 3.5: Akt wandalizmu na drzwiach senatora

W lipcu 2020 roku fani Taylor Swift zaczęli atakować krytyczkę muzyczną Jillian Mapes po tym, jak opublikowała recenzję albumu *Folklore*, która ich zdaniem nie była wystarczająco pochlebna. Wkrótce po publikacji recenzji w internecie zaczęły krążyć prywatne dane Mapes, w tym jej adres domowy, numery telefonów oraz zdjęcia jej i jej domu. Już godzinę po pojawieniu się recenzji zaczęła otrzymywać telefony m.in. o drugiej w nocy oraz groźby przez Twittera, w tym nawoływania do „spalenia jej domu”. Jillian odpowiedziała na ataki we wpisie na Twitterze, pisząc, że dostaje wiadomości pełne nienawiści,

ale mimo strachu, jaki wywołała sytuacja, jest bezpieczna i trzyma się dobrze.

3.1.5. Oszustwa socjotechniczne i internetowe

Opis zagrożenia

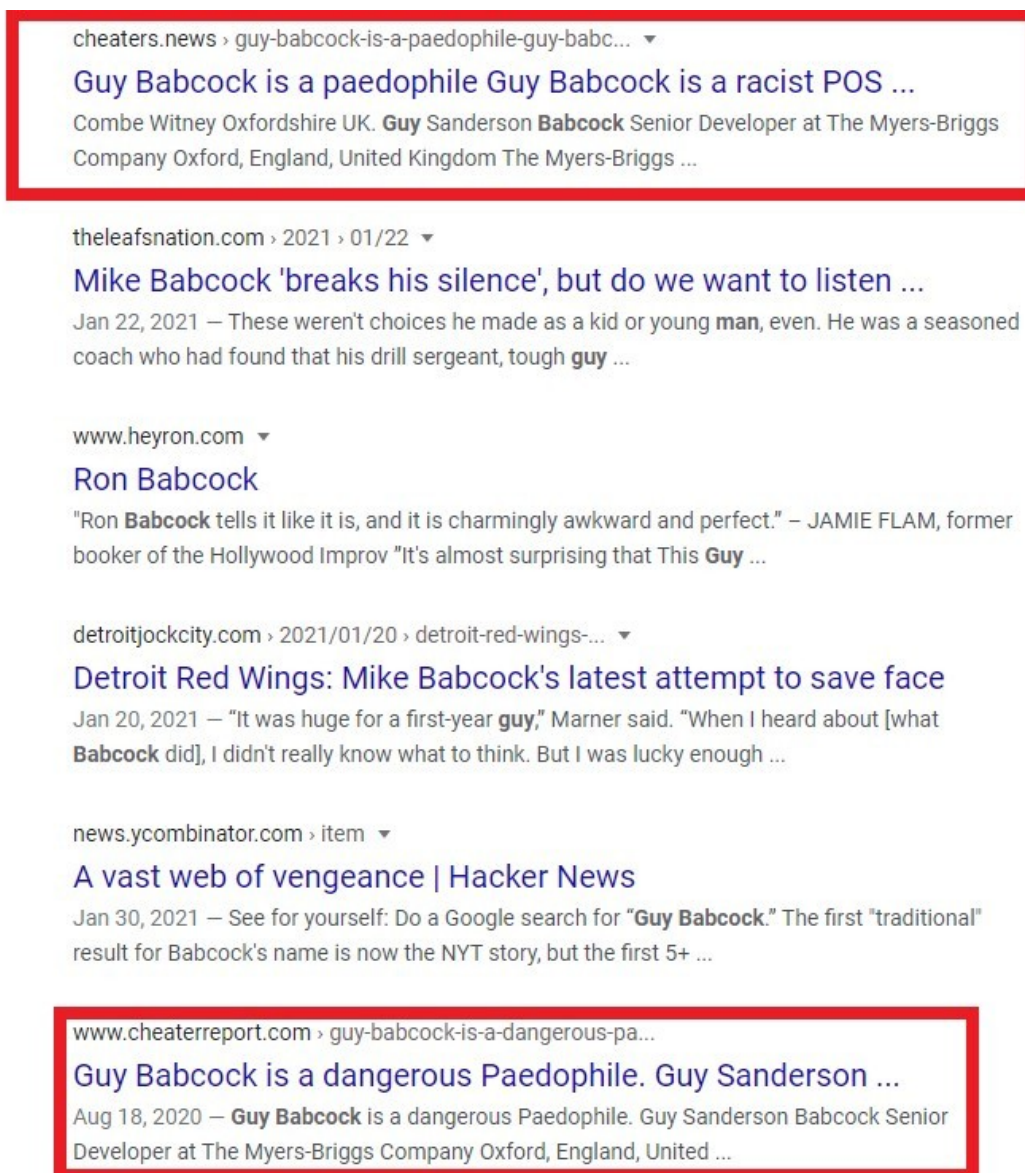
Ujawnione dane są wykorzystywane do:

- phishingu (fałszywe e-maile i strony),
- spear-phishingu (ukierunkowane ataki na konkretną osobę),
- vishingu (oszustwa telefoniczne),
- przekonywania ofiar do ujawnienia loginów i haseł.

Przykłady z życia

W 2020 r. grupa atakujących uzyskała dostęp do systemów Twittera, podszywając się pod pracowników i kradnąc dane do kont znanych osób.

Guy Babcock został niesłusznie oskarżony w internecie o pedofilię i złodziejstwo. Fałszywe wpisy na różnych forach zarzucały Babcockowi i jego rodzinie przestępstwa seksualne i kradzieże. Jego udostępnionych w internecie dane, czyli zdjęcia, miejsce pracy, dane kontaktowe z LinkedIna i Facebooka umożliwiły oszustom wiarygodne przedstawienie jego osoby i jego rodziny jako pedofila oraz złodziei, w postaci wpisów a forum. Wkrótce jego zdjęcia zaczęły krążyć w internecie z podpisem pedofila. Mężczyzna i jego rodzina zaczęli bać się o swoje kariery, reputację i o przyszłość swoich dzieci. I chociaż powstał nawet prostujący te informacje artykuł w magazynie „New York Times”, to rodzina wciąż boi się o swoje bezpieczeństwo i dobre mniemanie.



Rysunek 3.6: Fałszywe wpisy oskarżające o pedofilię

3.1.6. Konsekwencje reputacyjne

Opis zagrożenia

Dla osób publicznych, pracowników wysokiego szczebla lub właścicieli firm, ujawnienie danych może prowadzić do:

- utracenia zaufania klientów i partnerów,
- negatywnego rozgłosu medialnego
- trudności w znalezieniu nowej pracy lub rozwijaniu kariery.

Przykłady z życia

Wyciek danych w firmach takich jak Proofpoint, Apple czy Google nadszarpnął ich wizerunek jako liderów w dziedzinie innowacji i bezpieczeństwa.

Facebook był w 2011 roku cytowany w 33% spraw rozwodowych. Wskazuje to na to, że treści udostępniane w internecie mogą być wykorzystywane przeciwko nam, jako dowody w sprawach sądowych.

W wyniku mylnej identyfikacji mężczyzny z nagrania z zamieszek na Kapitolu w 2021 roku, internauci uznali, że to David Quintavalle zabił policjanta. Pan David miał udostępniony w internecie swoje imię, nazwisko, stare zdjęcia, adres domowy. W efekcie doprowadziło to do gróźb, nękań, media przed domem, policyjna ochrona, trwałe powiązanie nazwiska z fałszywym oskarżeniem. Musiał wynająć prawnika, który musiał mu pomóc odbudować jego dobre imię, chociaż bardzo trudno było w pełni pozbyć się nękań.



Rysunek 3.7: Fragment nagrania zamieszek na Kapitolu

3.1.7. Odpowiedzialność prawna

Opis zagrożenia

Udostępnianie danych bez zgody lub ich niewłaściwe zabezpieczenie może skutkować:

- pozwami cywilnymi ze strony poszkodowanych osób,
- karami finansowymi za naruszenie przepisów o ochronie danych (np. RODO/GDPR),
- odpowiedzialnością dyscyplinarną lub karną.

Przykłady z życia

Microsoft mógłby zostać ukarany grzywną do 20 mln euro za wyciek danych z systemów GitHub, gdyby doszło do naruszenia danych klientów z UE.

Japończyk Hibiki Sato użył zdjęć z mediów społecznościowych i na podstawie refleksów w oczach i Google Street View, by odnaleźć kobietę i ją zaatakować. Po tym wydarzeniu kobieta musiała się długi czas zmagać z traumą, natomiast stalker poniósł odpowiedzialność prawną - skazanie na 30 miesięcy pozbawienia wolności w 2020 roku.



Rysunek 3.8: Hibiki Sato

Yue Chen, pacjent z rakiem w IV stadium, który oskarżył swoich lekarzy o traktowanie go jak „małą laboratoryjną”, odnalazł ich domowe adresy w rejonie zatoki San Francisco i planował ich zamordowanie. 31 maja 2017 roku członkowie rodziny Chen’a zgłosili jego zaginięcie. Gdy policja przybyła na miejsce, znalazła notatkę, w której mężczyzna napisał, że „musi dziś zabić tych lekarzy, ponieważ są źli”. Na szczęście Chen zgubił się i nie odnalazł żadnego z domów lekarzy. Policja zatrzymała go, gdy próbował wrócić do siebie. W jego samochodzie znaleziono dwie naładowane półautomatyczne pistolety, notatnik z ręcznie przepisnymi z Google Maps wskazówkami dojazdu do domów lekarzy oraz białą gumową maskę. Znaleziono również notatkę zatytułowaną „dlaczego zabijam”, w której napisał: „to jest możliwe, jeśli traktujecie ludzi jak zwierzę”.

4. ZALECENIA DOTYCZĄCE PRYWATNOŚCI

Poniżej przedstawione zostały aspekty, których przestrzeganie może nas uchronić przed zagrożeniami wynikającymi z udostępniania danych w internecie. Już na wstępie należy dodać, że eksperci jednogłośnie podkreślają, że nasza prywatność w sieci zależy przede wszystkim od naszej świadomości i ostrożności[9].

4.1. Czego nie udostępniać w internecie?

4.1.1. Adres e-mail i numer telefonu

Aby uniknąć spamu, phishingu, ataków socjotechnicznych, przejęcia kont, używaj oddzielnego e-maila do rejestracji i nie udostępniaj numeru telefonu publicznie.

4.1.2. Adres domowy i lokalizacja geograficzna

Aby zmniejszyć ryzyko włamania, śledzenia, identyfikacji miejsca zamieszkania, wyłącz geolokalizację w aplikacjach i unikaj publikowania informacji o podróżach czy codziennej rutynie.

4.1.3. Zdjęcia nieletnich

Dokładnie przemyśl publikację zdjęć dzieci i ustaw ściśle ograniczenia prywatności, aby uniknąć wykorzystanie zdjęć przez osoby nieuprawnione, ryzyko ich rozpowszechnienia bez zgody.

4.1.4. Kompromitujące zdjęcia

Nigdy nie udostępniaj intymnych zdjęć, nawet zaufanym osobom — tracisz nad nimi kontrolę. Może to doprowadzić do szantażu zdjęciami i cyberprzemocy.

4.1.5. Dokumenty osobiste

Nie publikuj dokumentów tożsamości, umów czy informacji bankowych; jeśli musisz przechowywać je online — szyfruj dane, aby uniknąć kradzieży tożsamości, oszustw finansowych.

4.1.6. Opinia, skargi i kontrowersyjne komentarze

Przemyśl każdą publikację; internet nie zapomina, a wypowiedzi mogą być błędnie zinterpretowane i spowodować naruszenie reputacji, konflikty, nękanie.

4.1.7. Prywatne rozmowy

Korzystaj z szyfrowanych komunikatorów; nie przysyłaj wrażliwych danych w czatach, aby uniknąć ujawnienia poufnych informacji, ryzyka naruszenia prywatności innych osób.

4.2. Jak się chronić?

W wielu przypadkach nie ma jednak wyjścia. Wymagane jest udostępnienie w swoich danych w internecie. Poniżej znajduje się podsumowanie tego co warto zrobić, aby ochronić dane już przez nas

udostępnione.

- **Skonfiguruj ustawienia prywatności** na swoich kontach - ogranicz widoczność treści tylko do osób zaufanych.
- **Używaj silnych, unikalnych haseł** - regularnie je zmieniaj i nie używaj ich wielokrotnie.
- **Uważaj na podejrzane linki** - sprawdzaj źródło wiadomości i nie klikaj w nieznane odnośniki.
- **Korzystaj z zaufanych źródeł cyberbezpieczeństwa** - np. Incibe, OSI,
- **Nie publikuj wrażliwych informacji** - szczególnie tych dotyczących lokalizacji, planów i życia prywatnego,
- **Wyłącz geolokalizację** jeśli nie jest potrzebna,
- **Używaj silnych i unikalnych haseł** nieopartych na łatwo dostępnych danych osobowych,
- **Zachowaj ostrożność w komentarzach** nawet pozorna anonimowość może być złudna,
- **Rozważ korzystanie z usług typu VPN**, szczególnie w publicznych sieciach Wi-Fi (na laptopie, smartfonie, tablecie).
- **Unikaj podawania numeru telefonu** tam, gdzie nie jest to absolutnie konieczne, ewentualnie do celów bezpieczeństwa (np. 2FA).
- **Świadomie analizuj, z jakich usług korzystasz i jakimi danymi płacisz za „darmowy” dostęp.**
- **Zastrzeż swój numer PESEL.** Od niedawna w Polsce można zastrzec swój numer PESEL, aby nikt nie wykorzystał go bez wiedzy osoby, do której ten numer należy. Z zastrzeżonym numerem PESEL można:
 - zarejestrować się do lekarza,
 - zrealizować receptę,
 - wypłacić środki w bankomacie,
 - zlecić przelew bankowy,
 - wyjechać za granicę lub
 - załatwić sprawę urzędową.

Natomiast z zastrzeżonym numerem PESEL:

- Nie można zaciągnąć kredytu, pożyczki, leasingu,
- Nie można otworzyć nowego rachunku bankowego,
- Nie można zmienić umowy kredytu lub pożyczki,
- Nie można wypłacić w placówce banku więcej pieniędzy niż trzykrotność minimalnego wynagrodzenia,
- Nie można załatwić niektórych spraw notarialnych,
- Nie można otrzymać duplikatu karty SIM.

Należy cofnąć zastrzeżenie numeru PESEL w momencie gdy zajdzie potrzeba wykonania powyższych czynności.

Od 1 czerwca 2024 r. instytucje finansowe (np. banki) mają obowiązek weryfikować, czy numer PESEL jest zastrzeżony przy zawieraniu np. umowy kredytu lub pożyczki.

Funkcjonalność ta oferowana przez urząd państwowy pozwala uniknąć wiele przykrych i niebezpiecznych sytuacji. Zastrzeżenie PESELu to sprawa, którą można załatwić bardzo szybko - przez internet, bądź osobiście w Urzędzie[10].

Bezpieczeństwo w sieci dobrze podsumowuje poniższy cytat:

Twoje dane to Twoja odpowiedzialność.

W świecie cyfrowym prywatność nie jest dana raz na zawsze - trzeba ją stale chronić.

WYKAZ LITERATURY

- [1] "Jakie ślady zostawiamy w internecie?" (Dostęp 2025-03-26). [Online]. Available: <https://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/1019082,prywatnosc-w-internecie.html>.
- [2] "Twitter, snapchat, internet rzeczy. dane konsumenta na wyciągnięcie ręki," (Dostęp 2025-03-26). [Online]. Available: <https://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/1017004,twitter-snapchat-iot-czyli-dane-konsumenta-na-wyciagniecie-reki-2000.html>.
- [3] Wiesław Wolny. "Bezpieczeństwo i prywatność danych w badaniach mediów społecznościowych," (Dostęp 2025-03-26). [Online]. Available: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.cejsh-06278ad0-d165-4b1c-8b2b-5817b3982416/c/07.pdf&ved=2ahUKEwjqnLHL35SMAxUwMRAIHewwFJAQFnoECBEQAQ&usg=A0vVaw3qYoSnGsBD_Z3EekwfdAoJ.
- [4] "Co wie o nas internet?" (Dostęp 2025-03-26). [Online]. Available: <https://www.infor.pl/prawo/prawa-konsumenta/konsument-w-sieci/5297247,Co-wie-o-nas-Internet.html>.
- [5] "Things you shouldn't share with chatgpt," (Dostęp 2025-03-26). [Online]. Available: <https://telefonicatech.com/en/blog/things-you-shouldnt-share-with-chatgpt>.
- [6] "11 real-life insider threat examples," (Dostęp 2025-03-26). [Online]. Available: <https://www.mimecast.com/blog/insider-threat-examples/>.
- [7] "10 times someone's online information made them unsafe in real life," (Dostęp 2025-03-26). [Online]. Available: <https://www.linkedin.com/pulse/10-times-someones-online-information-made-them-unsafe-bridges>.
- [8] "Wyciek danych klientów empiku," (Dostęp 2025-03-30). [Online]. Available: <https://niebezpiecznik.pl/post/wyciek-danych-klientow-empiku/>.
- [9] "Protect yourself online: Data you should never share," (Dostęp 2025-03-26). [Online]. Available: <https://telefonicatech.com/en/blog/data-you-should-never-share-how-to-protect-it>.
- [10] "Zastrzeż swój numer pesel lub cofnij zastrzeżenie," (Dostęp 2025-03-30). [Online]. Available: <https://www.gov.pl/web/gov/zastrzez-swoj-numer-pesel-lub-cofnij-zastrzezenie>.