

**UTH**

**UCZELNIA  
TECHNICZNO-HANDLOWA  
im. H. Chodkowskiej  
w Warszawie**

Twoja  
przyszłość  
zaczyna się w UTH.



**UTH** UCZELNIA  
TECHNICZNO-HANDLOWA  
im. H. Chodkowskiej  
w Warszawie

---

dr inż. Michał Malinowski

<https://www.drmalinowski.edu.pl/>

mgr Małgorzata Musiał

<https://mmusial.owlstown.net>

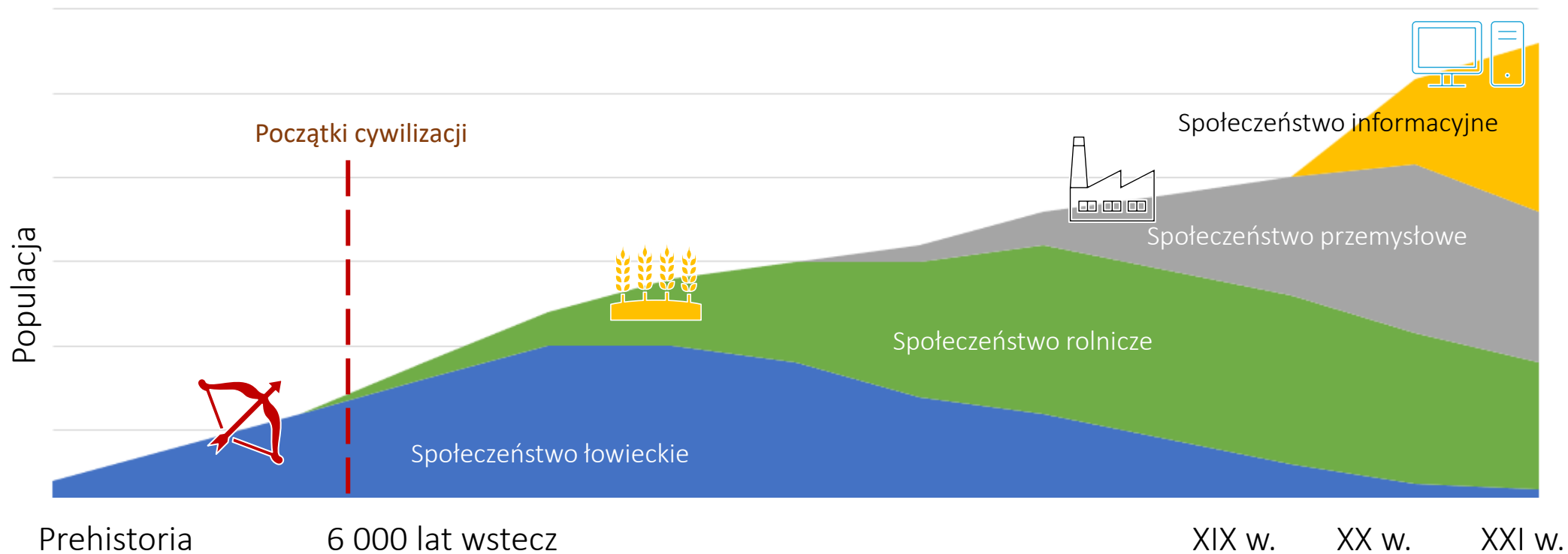
# Bezpieczne korzystanie z mediów społecznościowych

czyli

ochrona przed cyberzagrożeniami i ich skutkami

Cyberbezpieczny z UTH

# Gdzie teraz jesteśmy.. ?



# Informacja - najważniejszy zasób

## Społeczeństwo informacyjne

podstawą społeczeństwa informacyjnego jest gospodarka oparta na wiedzy (dane, informacje), a jej zasadniczym zasobem gospodarczym są informacje skumulowane w bazach.



### Kreacja informacji

Tworzenie danych  
Zbieranie danych  
Analiza danych  
Udostępnianie danych  
Konsolidacja danych

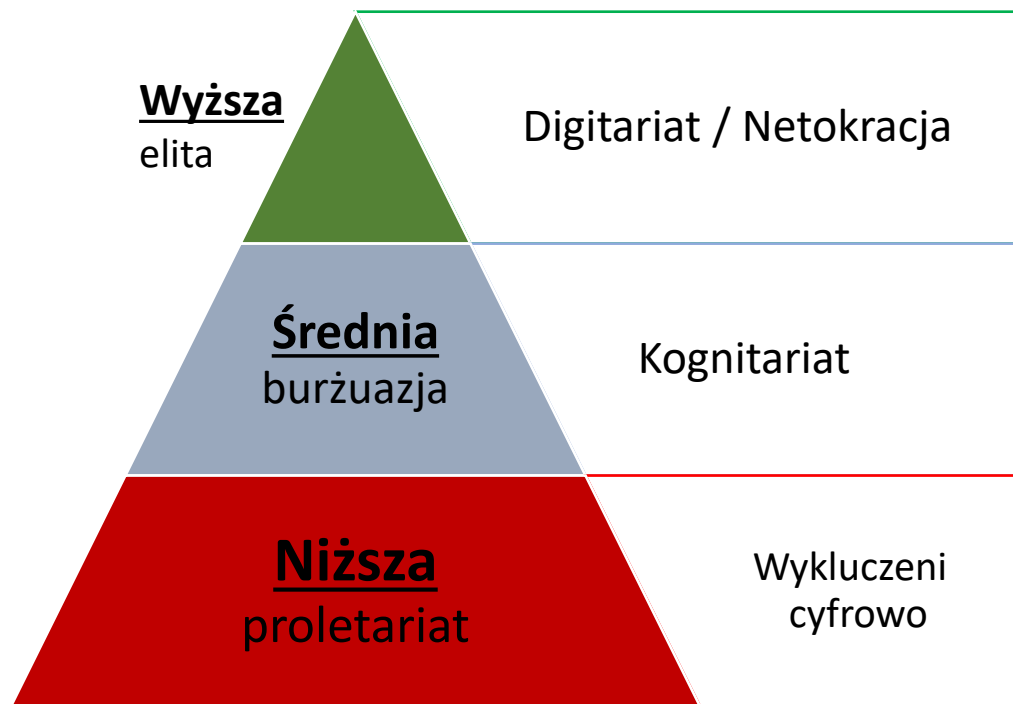
#### Zbiory danych

Autor

Czytelnik



### Klasy społeczne



Wyższa  
elita

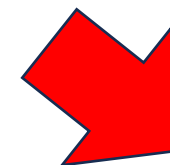
Digitariat / Netokracja

Średnia  
burżuazja

Kognitariat

Niższa  
proletariat

Wykluczeni  
cyfrowo



### Destrukcja informacji

Usuwanie danych  
Dezinformacja  
Zniekształcenie danych  
Brak aktualizacji  
Zaniedbania w archiwizacji

#### Ataki cybernetyczne

Obrońca

Atakujący



# Co to są media społecznościowe?

Media społecznościowe to platformy internetowe, które umożliwiają użytkownikom tworzenie i udostępnianie treści, nawiązywanie interakcji, komunikację oraz budowanie relacji w środowisku online.

Są to narzędzia umożliwiające tworzenie społeczności wirtualnych oraz dzielenie się informacjami w czasie rzeczywistym.

**W Polsce z mediów społecznościowych korzysta prawie 69% populacji**



JAN 2024

# OVERVIEW OF SOCIAL MEDIA USE

HEADLINES FOR SOCIAL MEDIA ADOPTION AND USE (NOTE: USER IDENTITIES MAY NOT REPRESENT UNIQUE INDIVIDUALS)



POLAND

NUMBER OF SOCIAL MEDIA USER IDENTITIES



27.90 MILLION

QUARTER-ON-QUARTER CHANGE IN SOCIAL MEDIA USER IDENTITIES



0% [UNCHANGED]

YEAR-ON-YEAR CHANGE IN SOCIAL MEDIA USER IDENTITIES



+1.5% +400 THOUSAND

AVERAGE DAILY TIME SPENT USING SOCIAL MEDIA



1H 54M YOY: -7 MINS

AVERAGE NUMBER OF SOCIAL PLATFORMS USED EACH MONTH



5.9

SOCIAL MEDIA USER IDENTITIES vs. TOTAL POPULATION



68.8%

SOCIAL MEDIA USER IDENTITIES AGED 18+ vs. POPULATION AGED 18+



74.7%

SOCIAL MEDIA USER IDENTITIES vs. INDIVIDUALS USING THE INTERNET



78.0%

FEMALE SOCIAL MEDIA USER IDENTITIES vs. TOTAL SOCIAL MEDIA USER IDENTITIES



50.4%

MALE SOCIAL MEDIA USER IDENTITIES vs. TOTAL SOCIAL MEDIA USER IDENTITIES



49.6%

<https://empemedia.pl/digital-poland-2024-raport-social-media-w-polsce/>

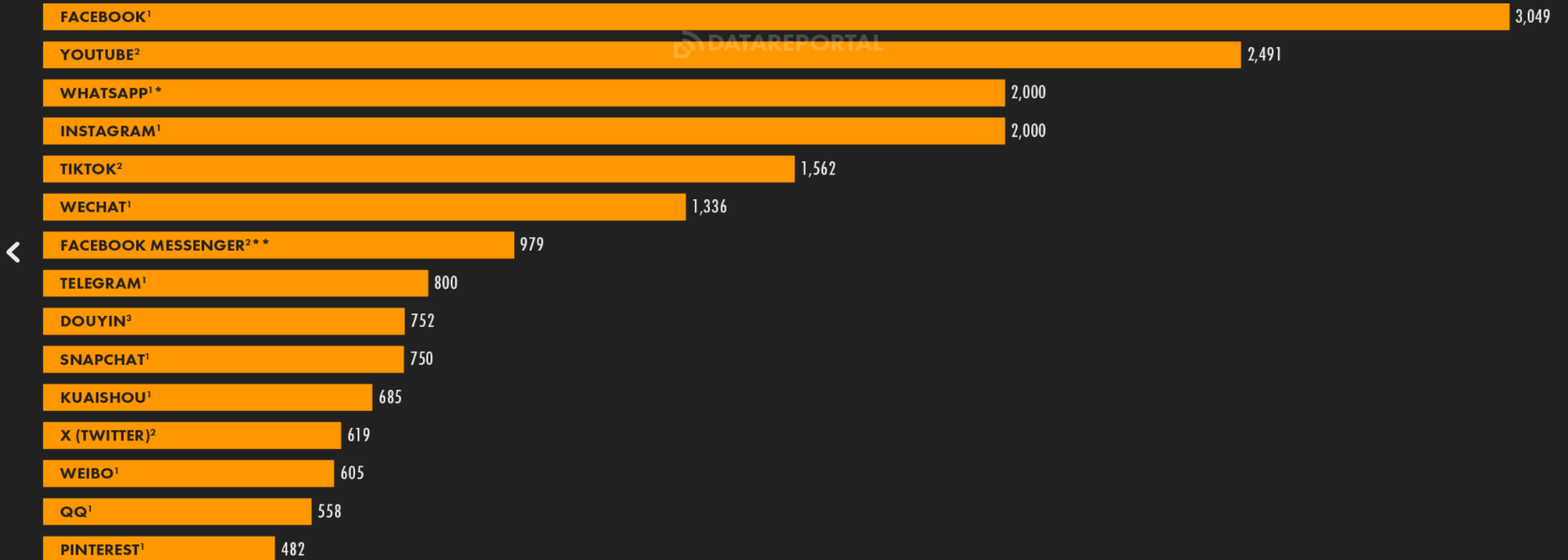
**JAN  
2024**

# THE WORLD'S MOST USED SOCIAL PLATFORMS

RANKING OF SOCIAL MEDIA PLATFORMS BY GLOBAL ACTIVE USER FIGURES (IN MILLIONS) (NOTE: USERS MAY NOT REPRESENT UNIQUE INDIVIDUALS)



GLOBAL OVERVIEW



<https://empemedia.pl/digital-poland-2024-raport-social-media-w-polsce/>

JAN  
2024

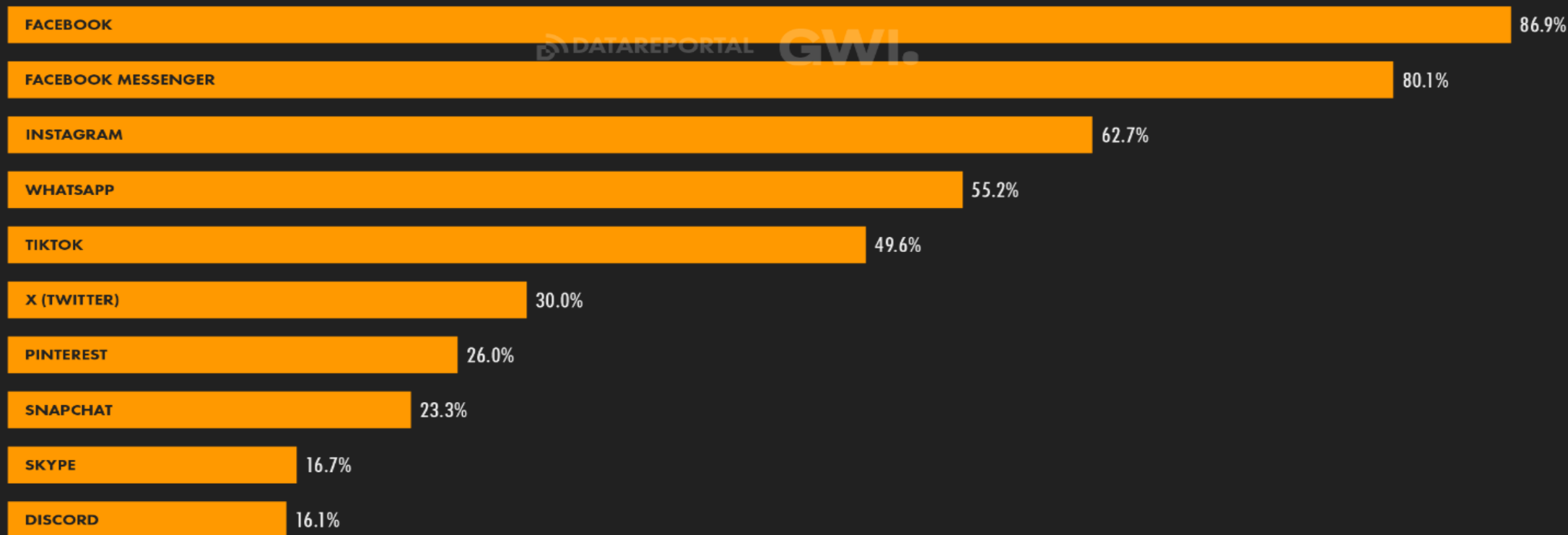
# MOST USED SOCIAL MEDIA PLATFORMS

PERCENTAGE OF INTERNET USERS AGED 16 TO 64 WHO USE EACH PLATFORM EACH MONTH

**NOTE:** YOUTUBE IS NOT OFFERED AS AN ANSWER OPTION FOR THIS QUESTION IN GWI'S SURVEY, SO IT WILL NOT APPEAR IN THIS RANKING



POLAND



60

**SOURCE:** GWI (Q3 2023). FIGURES REPRESENT THE FINDINGS OF A BROAD SURVEY OF INTERNET USERS AGED 16 TO 64. SEE [GWI.COM](https://www.gwi.com). **NOTE:** YOUTUBE IS NOT OFFERED AS AN ANSWER OPTION FOR THIS QUESTION IN GWI'S SURVEY. **COMPARABILITY:** A VERSION OF THIS CHART THAT APPEARED IN OUR PREVIOUS REPORTS WAS BASED ON A PREVIOUS QUESTION IN GWI'S SURVEY THAT INCLUDED YOUTUBE AS AN ANSWER OPTION. GWI'S CURRENT SURVEY FEATURES A REVISED VERSION OF THIS QUESTION THAT DOES NOT INCLUDE YOUTUBE AS AN ANSWER OPTION, WHILE OTHER CHANGES TO THE QUESTION'S WORDING MAY MEAN THAT THE VALUES AND RANK ORDER SHOWN HERE ARE NOT DIRECTLY COMPARABLE WITH THOSE SHOWN ON A SIMILAR CHART IN PREVIOUS REPORTS.

we  
are  
social

Meltwater

<https://empemedia.pl/digital-poland-2024-raport-social-media-w-polsce/>

**UTH** UCZELNIA  
TECHNICZNO-HANDLOWA  
im. H. Chodkowskiej  
w Warszawie

# Dlaczego warto mówić o bezpieczeństwie online?



## Codziennie Użycie Technologii

W dzisiejszych czasach młodzi ludzie spędzają dużo czasu online – od mediów społecznościowych, przez gry, po zakupy i edukację.



## Prywatność i Dane Osobowe

Ochrona prywatności i danych osobowych jest kluczowa, aby uniknąć kradzieży tożsamości, oszustw finansowych oraz nieautoryzowanego dostępu do prywatnych informacji.



## Zagrożenia w Sieci

Wzrost liczby cyberataków, takich jak phishing, malware, cyberbullying, wymaga od nas świadomego i odpowiedzialnego podejścia do korzystania z internetu.



## Długoterminowe Konsekwencje

Niezabezpieczone działania online mogą prowadzić do długoterminowych konsekwencji, takich jak problemy z reputacją, finansowe straty czy nawet problemy prawne

# Najczęstsze zagrożenia w mediach społecznościowych

Phishing i oszustwa

Cyberprzemoc  
(cyberbullying)

Niebezpieczne  
kontakty online

Nadmierne  
dzielenie się  
informacjami  
(oversharing)

Fake newsy  
i manipulacje

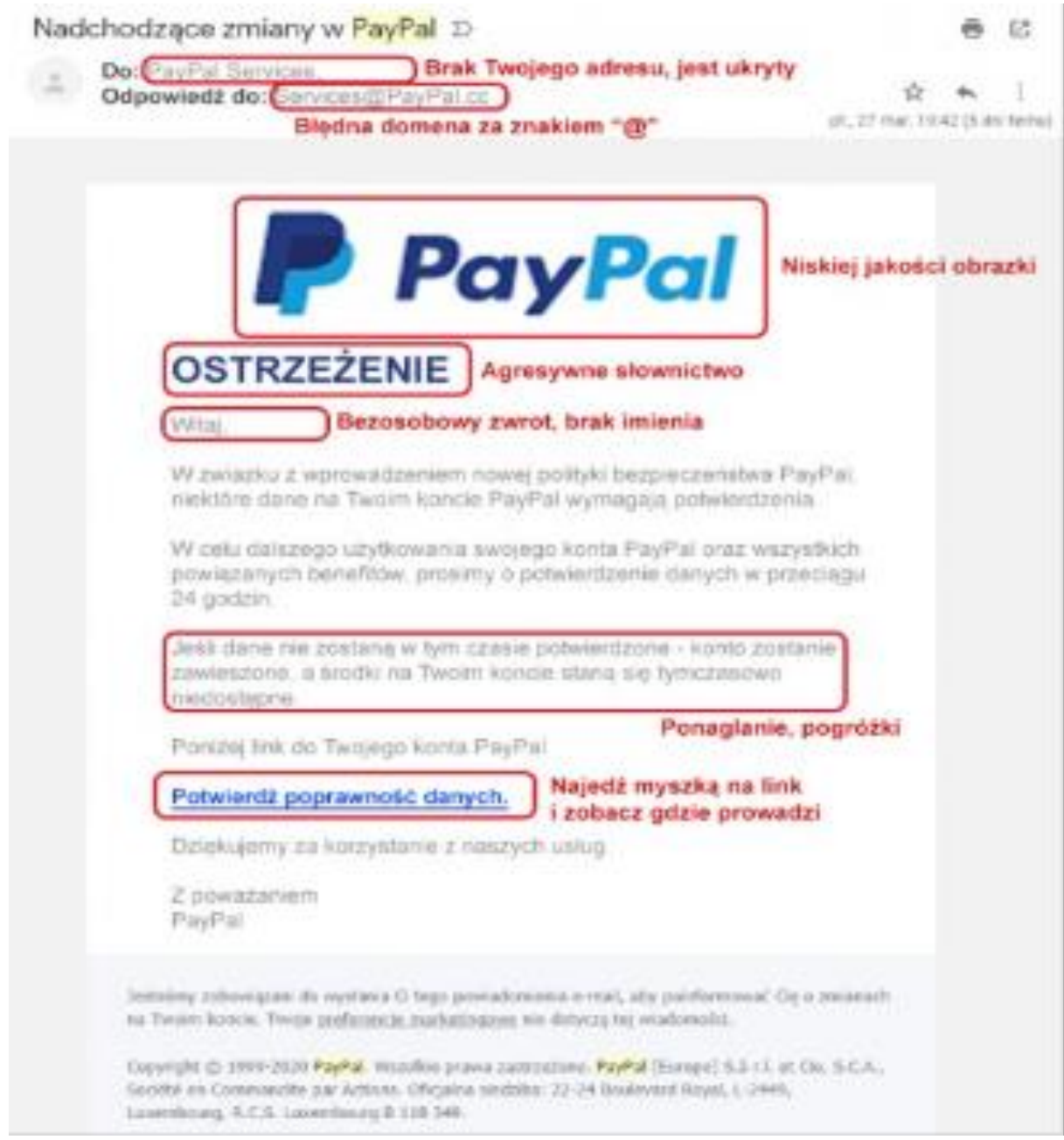
Uzależnienie  
od mediów  
społecznościowych

# Phishing i oszustwa

**Phishing** to rodzaj cyberprzestępstwa, którego celem jest wyłudzenie poufnych informacji, takich jak hasła, dane logowania, numery kart płatniczych czy inne wrażliwe dane osobowe.

**Oszuści** podszywają się pod zaufane osoby lub organizacje, aby skłonić użytkownika do podjęcia określonych działań.





# Jak rozpoznać phishing?

# Cyberprzemoc (cyberbullying)

Cyberprzemoc to wszelkie działania mające na celu zastraszenie, poniżenie, ośmieszenie lub wykluczenie danej osoby przy użyciu mediów społecznościowych, aplikacji komunikacyjnych czy innych narzędzi internetowych.



# Formy cyberprzemocy

- ✓ Komentarze obrażające wygląd, przekonania lub styl życia.
- ✓ Rozpowszechnianie nieprawdziwych informacji lub plotek.
- ✓ Publikowanie kompromitujących zdjęć/filmów bez zgody.
- ✓ Tworzenie fałszywych profili, by ośmieszyć inną osobę.

*"Jesteś żałosny/a. Nikt cię nie lubi."*

*„Nie należysz do nas.”*

# Niebezpieczne kontakty online

**Niebezpieczne kontakty online** to sytuacje, w których użytkownicy (często dzieci lub młodzież) są manipulowani, wykorzystywani lub wprowadzani w relacje z osobami, które mają złe intencje.

**Grooming** jest jedną z najbardziej niebezpiecznych form takich kontaktów, wykorzystuje relacje w celu manipulacji, uzyskania prywatnych informacji, zdjęć, a nawet nadużyć seksualnych.



## Nawiązanie kontaktu

*„Hej! Widziałem twoje zdjęcia na Instagramie, fajnie się ubierasz, chciałbym cię lepiej poznać.”*

## Budowanie zaufania

*„Widzę, że masz ciężki dzień w szkole. Mi też kiedyś dokuczali. Możesz ze mną o wszystkim porozmawiać.”*

## Izolacja od bliskich

*„Twoi rodzice cię nie rozumieją, ale ja tak. Tylko mi możesz ufać.”*

## Manipulacja i wymuszanie

*„Jeśli mi nie wyślesz więcej zdjęć, pokażę wszystkim, co mi już wysłałaś.”*



# Nadmierne dzielenie się informacjami (oversharing)

Oversharing to nadmierne udostępnianie osobistych, poufnych lub prywatnych informacji w mediach społecznościowych, które może prowadzić do naruszenia prywatności i stwarzania zagrożeń, takich jak kradzież tożsamości, stalking czy cyberprzemoc.



Udostępnianie szczegółów życia prywatnego

Publikowanie dokładnej lokalizacji

Pokazywanie danych osobowych na zdjęciach

Publikowanie zdjęć dzieci lub bliskich bez zastanowienia

Dzielenie się informacjami finansowymi

Publiczne narzekanie na pracę lub szkołę

Publikowanie zdjęć z imprez

# Realne przykłady

## Włamanie do domu po publikacji lokalizacji:

W 2017 roku we Francji para włamywaczy wykorzystywała posty w mediach społecznościowych, aby dowiedzieć się, kiedy właściciele są na wakacjach. Śledzili profile na Facebooku, a następnie włamywali się do pustych domów.

## Strata pracy po nieprzemyślanym poście:

W USA pracownik lotniska opublikował na Twitterze obraźliwy wpis na temat pasażerów. Post stał się wiralowy, a pracownik został zwolniony za naruszenie zasad etyki zawodowej.

## Stalking po publikacji lokalizacji:

Influencerka na Instagramie udostępniła zdjęcia z wakacji, oznaczając dokładne miejsce, w którym przebywała. Stalker wykorzystał tę informację, by ją śledzić i kontaktować się z nią w realnym świecie.

# Fake newsy i dezinformacja



- **FAKE NEWSY:** Fałszywe informacje rozpowszechniane w celu wprowadzenia w błąd lub wywołania paniki.

Przykład: Fałszywe wiadomości dotyczące zdrowia, polityki lub wydarzeń społecznych.

- **DEZINFORMACJA:** Celowe szerzenie nieprawdziwych informacji w celu manipulowania opinią publiczną lub osiągnięcia określonych celów politycznych.

Przykład: Kampanie dezinformacyjne podczas wyborów.

# Jak unikać fake newsów?



- ✓ Sprawdź źródło informacji
- ✓ Weryfikuj informacje na kilku niezależnych źródłach
- ✓ Zwróć uwagę na emocjonalny język i sensacyjne nagłówki
- ✓ Bądź ostrożny wobec zdjęć i materiałów wizualnych
- ✓ Sprawdź datę publikacji
- ✓ Weryfikuj fakty za pomocą specjalistycznych platform fact-checkingowych:  
**Polska:** [Demagog.org.pl](http://Demagog.org.pl)  
**Świat:** [Snopes.com](http://Snopes.com), [FactCheck.org](http://FactCheck.org), [Google Fact Check Explorer](http://Google Fact Check Explorer).
- ✓ Analizuj intencje i źródła finansowania mediów
- ✓ Bądź ostrożny wobec „zrzutów ekranu”

# Uzależnienie od mediów społecznościowych

Uzależnienie od mediów społecznościowych to stan, w którym użytkownik odczuwa przymus ciągłego korzystania z platform takich jak Facebook, Instagram, TikTok czy Snapchat.

Charakteryzuje się nadmiernym zaangażowaniem w korzystanie z tych aplikacji, kosztem codziennych obowiązków, relacji międzyludzkich i zdrowia psychicznego.



# Zasady bezpiecznego korzystania

Zasada ograniczonego zaufania

Ustawienia prywatności

Silne hasła

Uwierzytelnianie dwuskładnikowe

Ochrona danych osobowych

Zasada „Zastanów się dwa razy”

Ograniczanie czasu spędzanego na mediach społecznościowych

# Twój Telefon, Twoja Twierdza



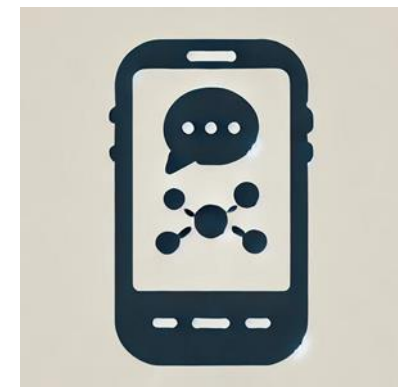
- **MALWARE:** Złośliwe oprogramowanie, które może infekować telefon przez zainstalowane aplikacje, pobierane pliki lub odwiedzane strony internetowe.

Przykład: Trojany, które mogą kraść dane, złośliwe oprogramowanie reklamowe (adware), które wyświetla niechciane reklamy.

- **SPYWARE:** Oprogramowanie szpiegowskie, które monitoruje i zbiera informacje o użytkowniku bez jego wiedzy.

Przykład: Aplikacje śledzące lokalizację, rejestrujące klawisze (keyloggery) lub nagrywające rozmowy.

# Twój Telefon, Twoja Twierdza



- **BRAK AKTUALIZACJI:** Aplikacje, które nie są regularnie aktualizowane, mogą zawierać luki bezpieczeństwa, które mogą być wykorzystane przez hakerów.

Przykład: Starsze wersje aplikacji bankowych lub mediów społecznościowych mogą być bardziej podatne na ataki.

- **PODEJRZANE ŹRÓDŁA:** Aplikacje pobierane spoza oficjalnych sklepów (Google Play, App Store) mogą zawierać złośliwe oprogramowanie.

Przykład: Aplikacje oferujące darmowe funkcje premium mogą być narzędziami do wykradania danych.

# Czy twój telefon jest bezpieczny?



Sprawdź te numery:

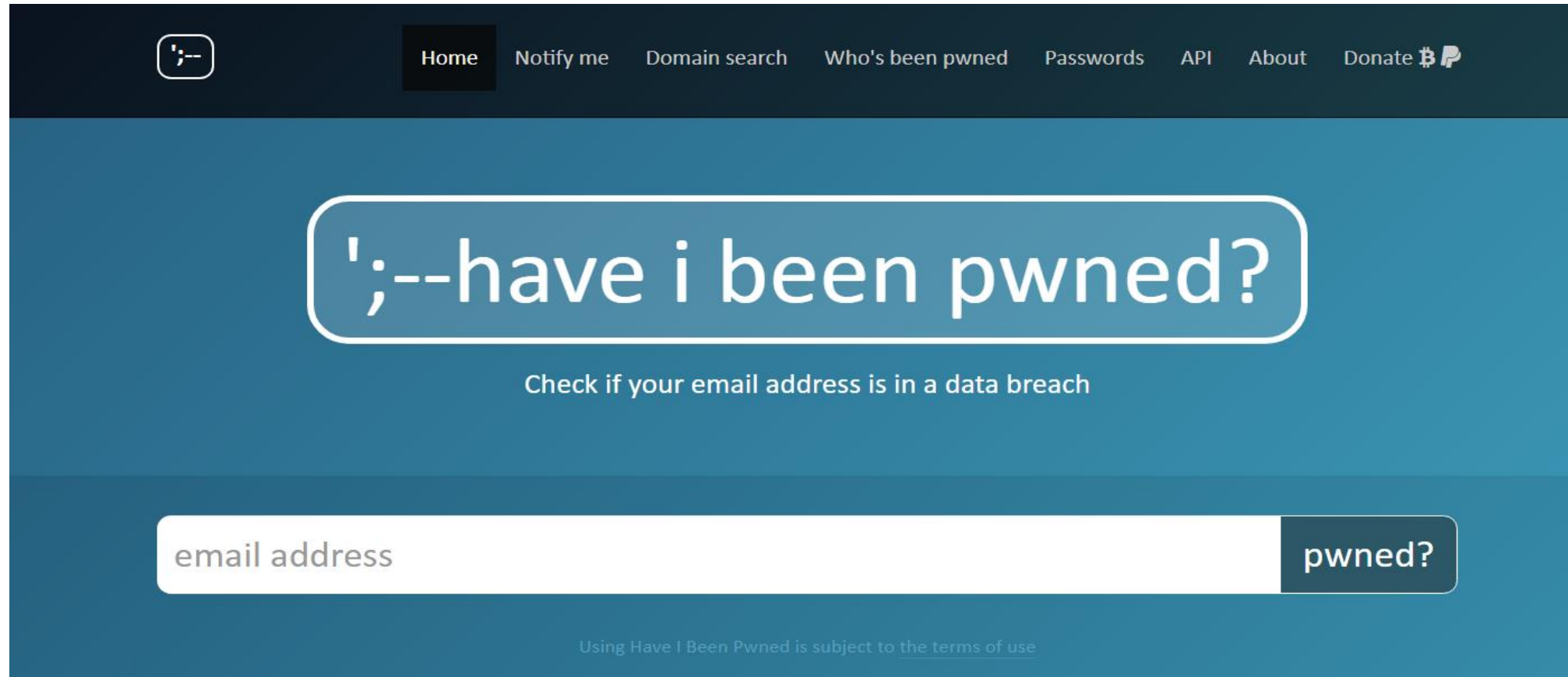
\*#62#

\*#21#

\*#06#

\*#1234#

# Czy moje dane wyciekły?



The screenshot shows the homepage of the 'Have I Been Pwned' website. At the top, there is a dark navigation bar with a logo on the left and menu items: Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate with a Bitcoin icon. The main content area has a blue background. In the center, a large white rounded rectangle contains the text ';---have i been pwned?'. Below this, it says 'Check if your email address is in a data breach'. At the bottom, there is a white input field with the placeholder text 'email address' and a dark button labeled 'pwned?'. A small link at the bottom reads 'Using Have I Been Pwned is subject to the terms of use'.

„Have I Been Pwned?”

<https://haveibeenpwned.com/>

# 7 Zasad Bezpiecznego Korzystania z Wi-Fi

Nr	Zasada	Opis	Przykład
1	<b>Unikaj korzystania z publicznych sieci Wi-Fi</b>	Publiczne Wi-Fi jest często niezabezpieczone, co zwiększa ryzyko przechwycenia danych przez osoby trzecie.	Korzystaj z danych mobilnych lub prywatnych, zabezpieczonych sieci Wi-Fi.
2	<b>Wyłącz udostępnianie plików na urządzeniach w publicznych sieciach Wi-Fi</b>	Udostępnianie plików może prowadzić do nieautoryzowanego dostępu do Twoich danych przez inne osoby w tej samej sieci.	Wyłącz funkcję udostępniania plików w ustawieniach swojego systemu operacyjnego.
3	<b>Sprawdzaj, do jakiej sieci się łączysz</b>	Upewnij się, że łączysz się z właściwą siecią, a nie z fałszywą siecią utworzoną przez cyberprzestępców.	Sprawdź nazwę sieci (SSID) i upewnij się, że jest zgodna z nazwą podaną przez właściciela miejsca.
4	<b>Wyłącz automatyczne łączenie z sieciami Wi-Fi</b>	Automatyczne łączenie z sieciami Wi-Fi może sprawić, że urządzenie połączy się z niezabezpieczoną lub fałszywą siecią.	Wyłącz automatyczne łączenie w ustawieniach Wi-Fi swojego urządzenia.
5	<b>Stosuj silne hasła do swojej domowej sieci Wi-Fi</b>	Silne hasła utrudniają nieautoryzowany dostęp do Twojej sieci.	Użyj kombinacji liter, cyfr i symboli, np. "H@rd2Gu3ssP@ssw0rd".
6	<b>Zmień domyślne nazwy użytkownika i hasła routera</b>	Domyślne dane logowania do routera są łatwe do odgadnięcia, co może umożliwić atak na Twoją sieć.	Zmień nazwę użytkownika i hasło na coś bardziej skomplikowanego i unikalnego.
7	<b>Aktualizuj oprogramowanie routera</b>	Regularne aktualizacje oprogramowania routera naprawiają luki bezpieczeństwa i chronią sieć przed nowymi zagrożeniami.	Sprawdź, czy Twój router ma opcję automatycznych aktualizacji lub ręcznie sprawdzaj dostępność aktualizacji.

# „Magia” udostępnianych informacji

[Amazing mind reader reveals his 'gift'](#)





Paczka wiedzy  
#02

Informatyka na dziś....



Paczka wiedzy  
#09

Informatyka na dziś....



Paczka wiedzy  
#06

Informatyka na dziś....



Dawka informacji ze świata technologii, sztucznej inteligencji oraz cyberbezpieczeństwa.



**UTH** UCZELNIA  
TECHNICZNO-HANDLOWA  
im. H. Chodkowskiej  
w Warszawie

---

**Dziękuję za uwagę !**

**Cyberbezpieczny z UTH**