
UTH
UCZELNIA
TECHNICZNO-HANDLOWA
im. H. Chodkowskiej
w Warszawie
Twoja
przyszłość
zaczyna się w 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

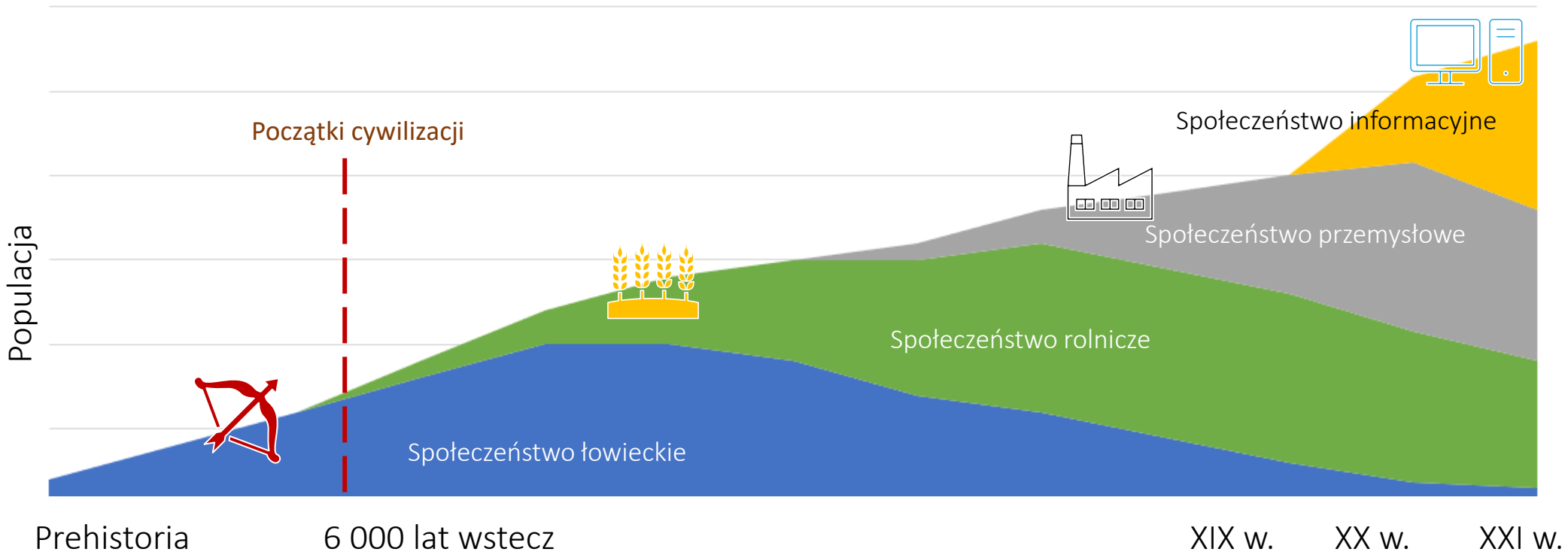
Bezpieczne korzystanie z mediów społecznościowych

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.

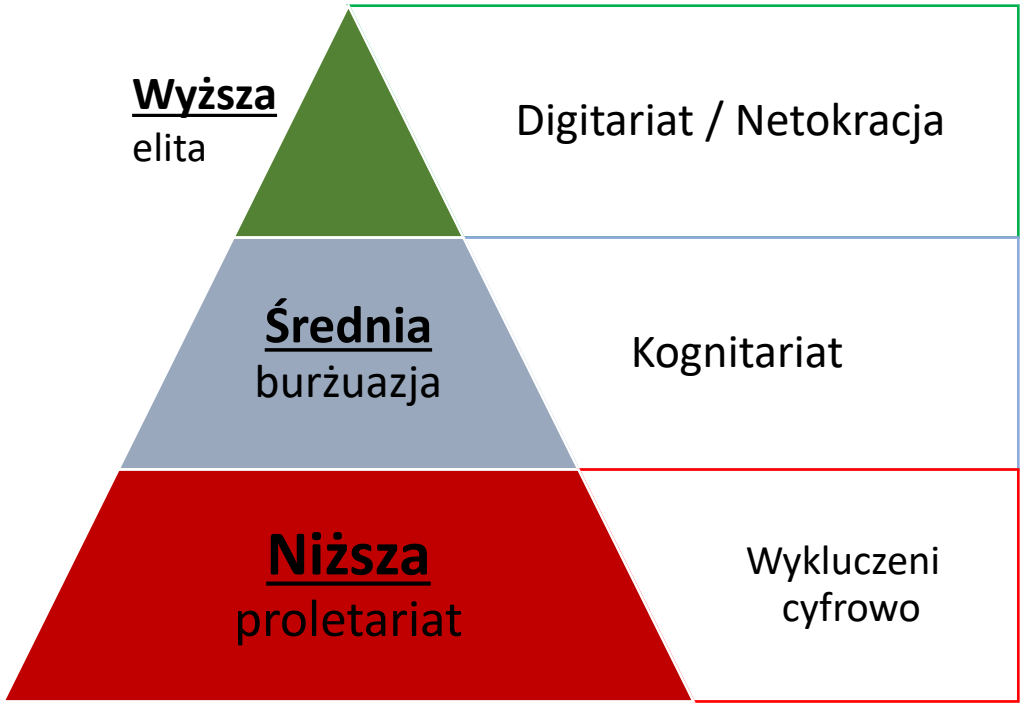
Kreacja informacji

Tworzenie danych
Zbieranie danych
Analiza danych
Udostępnianie danych
Konsolidacja danych
Zbiory danych

Autor

Czytelnik

Klasy społeczne



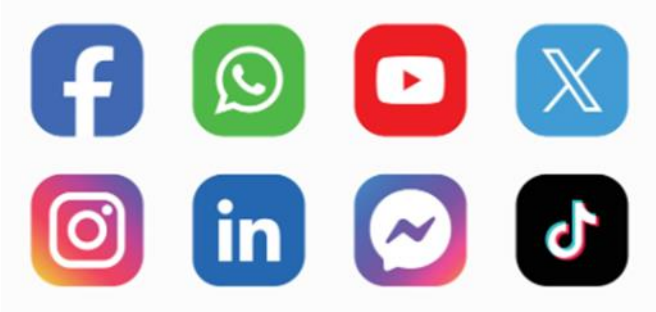
Destrukcja informacji

Usuwanie danych
Dezinformacja
Zniekształcenie danych
Brak aktualizacji
Zaniedbania w archiwizacji
Ataki cybernetyczne

Obrońca

Atakujący

Co to są media społecznościowe?

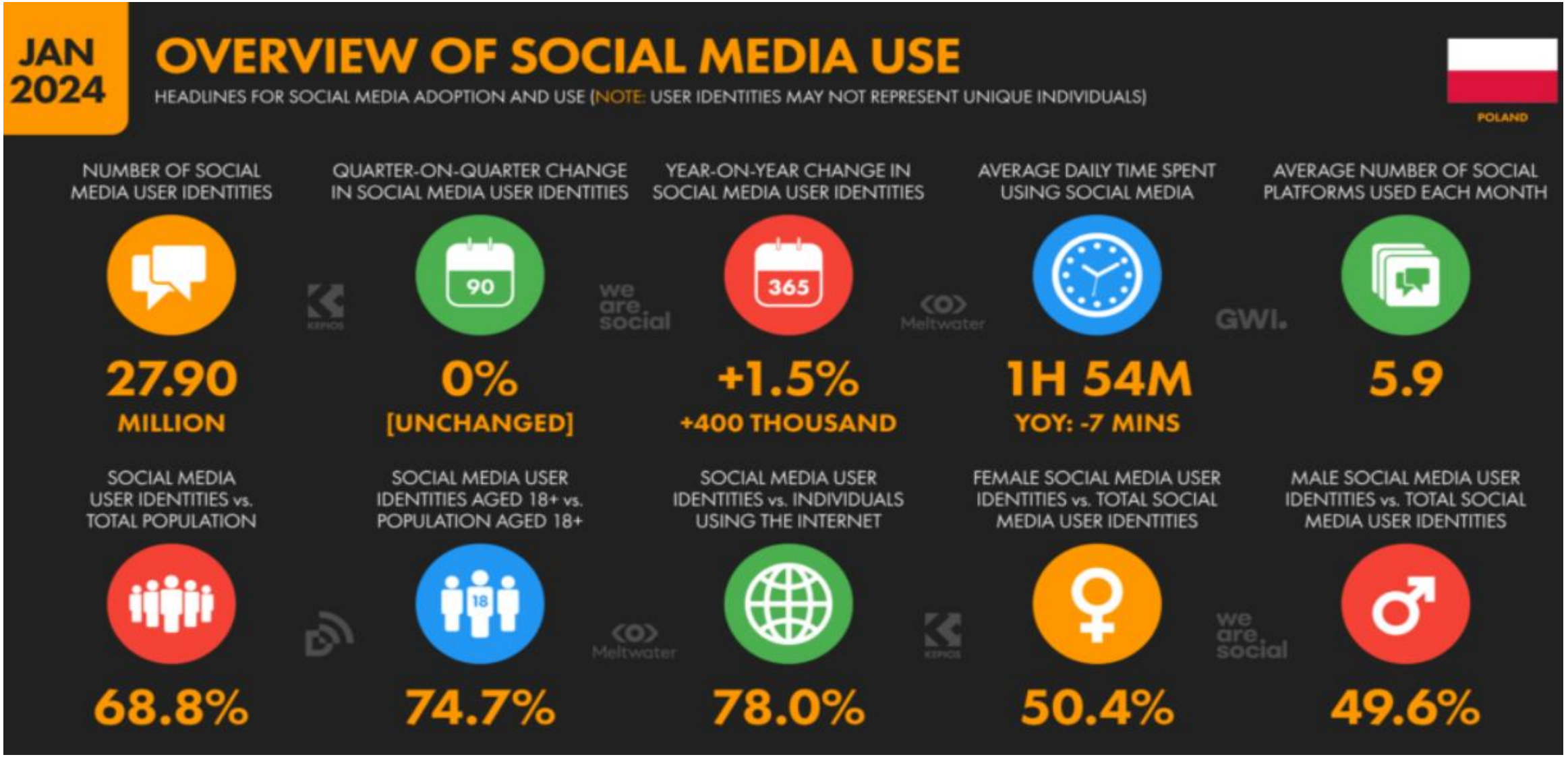


Media społecznościowe to platformy internetowe, które umożliwiają użytkownikom tworzenie i udostępnianie treści, nawiązywanie interakcji, komunikację oraz budowanie relacji w środowisku online.

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

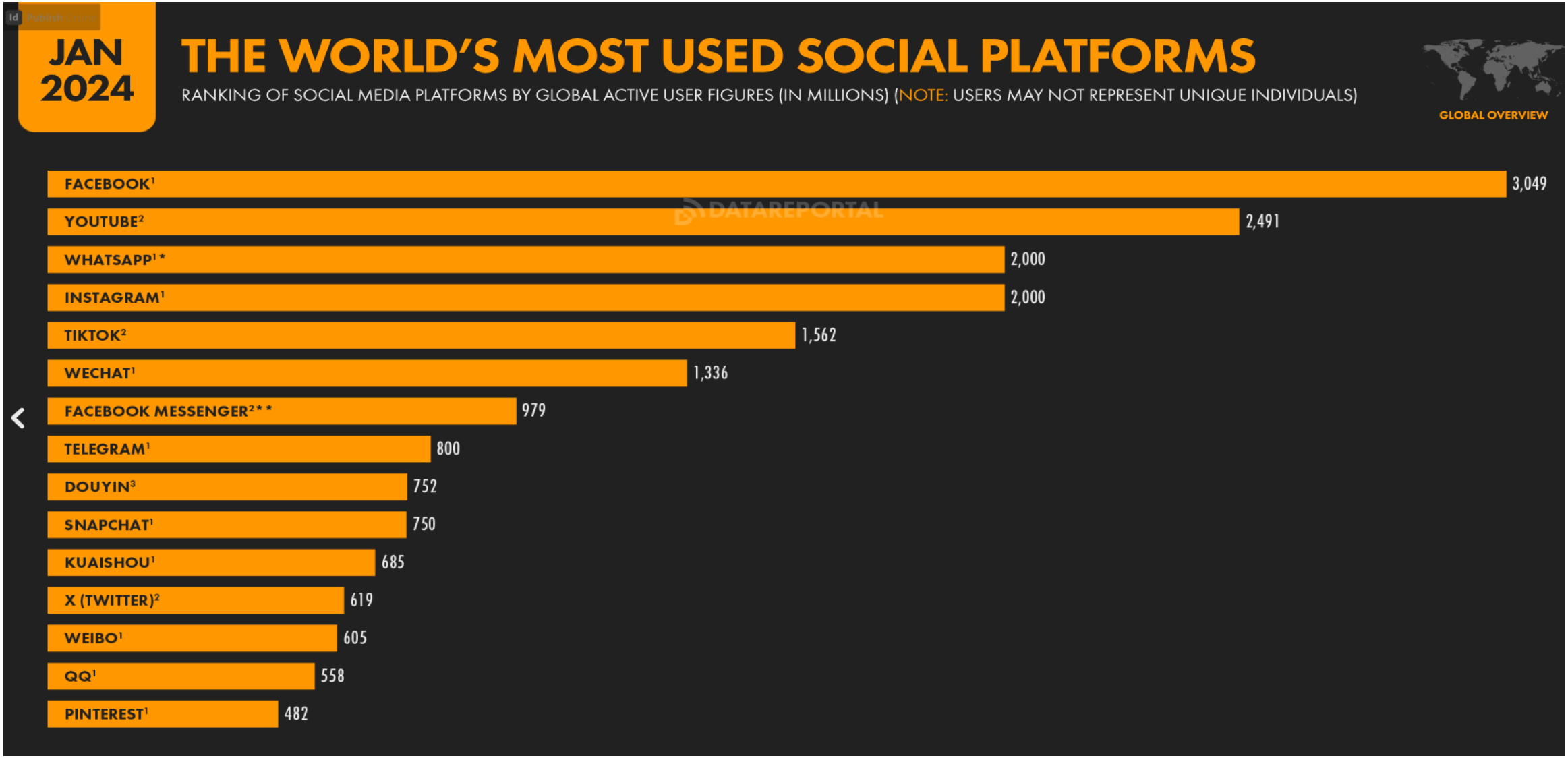
W Polsce z mediów społecznościowych korzysta prawie 69% populacji

UCZELNIA TECHNICZNO-HANDLOWA im. H. Chodkowskiej w Warszawie



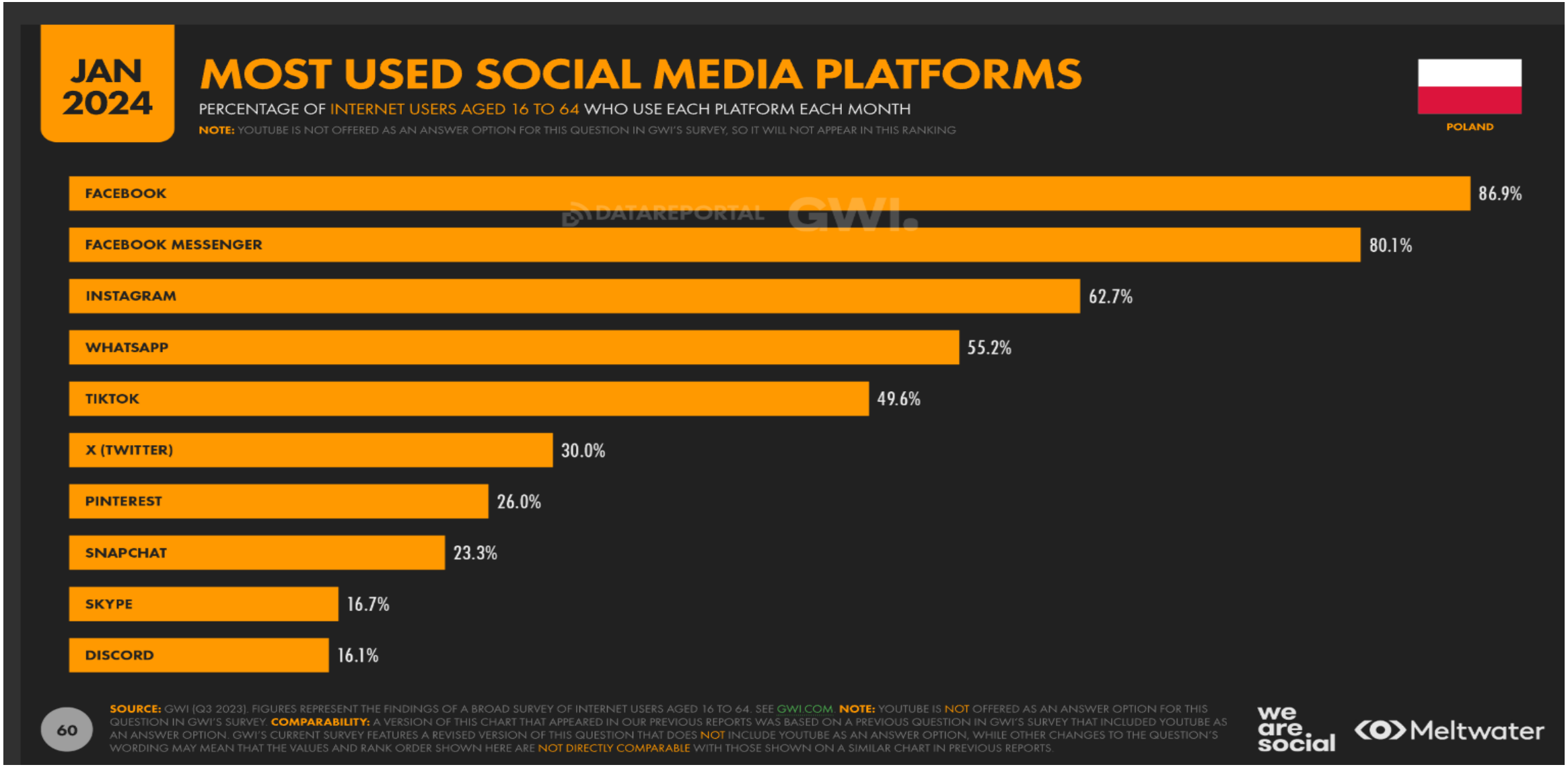
https://empemedia.pl/digital-poland-2024-raport-social-media-w-polsce/

UCZELNIA TECHNICZNO-HANDLOWA im. H. Chodkowskiej w Warszawie



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

UCZELNIA TECHNICZNO-HANDLOWA im. H. Chodkowskiej w Warszawie



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

UCZELNIA TECHNICZNO-HANDLOWA im. H. Chodkowskiej w Warszawie

Dlaczego warto mówić o bezpieczeństwie online?

UCZELNIA TECHNICZNO-HANDLOWA im. H. Chodkowskiej w Warszawie

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

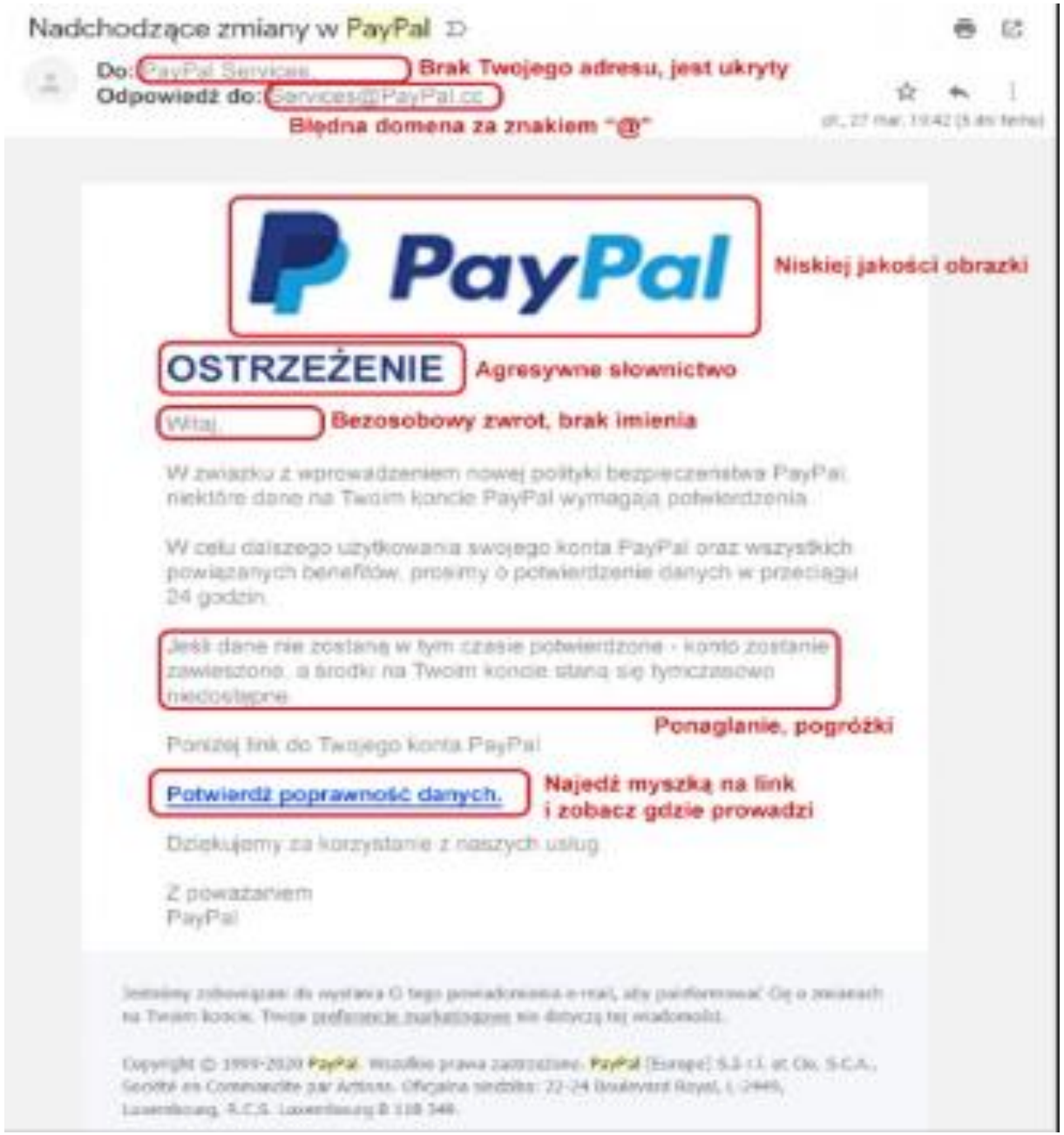
UCZELNIA TECHNICZNO-HANDLOWA im. H. Chodkowskiej w Warszawie

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.

UCZELNIA TECHNICZNO-HANDLOWA im. H. Chodkowskiej w Warszawie



Jak rozpoznać phishing?

UCZELNIA TECHNICZNO-HANDLOWA im. H. Chodkowskiej w Warszawie

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."

UCZELNIA TECHNICZNO-HANDLOWA im. H. Chodkowskiej w Warszawie

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.

UCZELNIA TECHNICZNO-HANDLOWA im. H. Chodkowskiej w Warszawie

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."

UCZELNIA TECHNICZNO-HANDLOWA im. H. Chodkowskiej w Warszawie

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.

UCZELNIA TECHNICZNO-HANDLOWA im. H. Chodkowskiej w Warszawie

- 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.

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

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
  Świat: Snopes.com, FactCheck.org, Google Fact Check Explorer.
- ✓Analizuj intencje i źródła finansowania mediów
- ✓Bądź ostrożny wobec „zrzutów ekranu”

UCZELNIA TECHNICZNO-HANDLOWA im. H. Chodkowskiej w Warszawie

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.

UCZELNIA TECHNICZNO-HANDLOWA im. H. Chodkowskiej w Warszawie

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

UCZELNIA TECHNICZNO-HANDLOWA im. H. Chodkowskiej w Warszawie

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.

UCZELNIA TECHNICZNO-HANDLOWA im. H. Chodkowskiej w Warszawie

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.

UCZELNIA TECHNICZNO-HANDLOWA im. H. Chodkowskiej w Warszawie

Czy twój telefon jest bezpieczny?

Sprawdź te numery:

*#62#

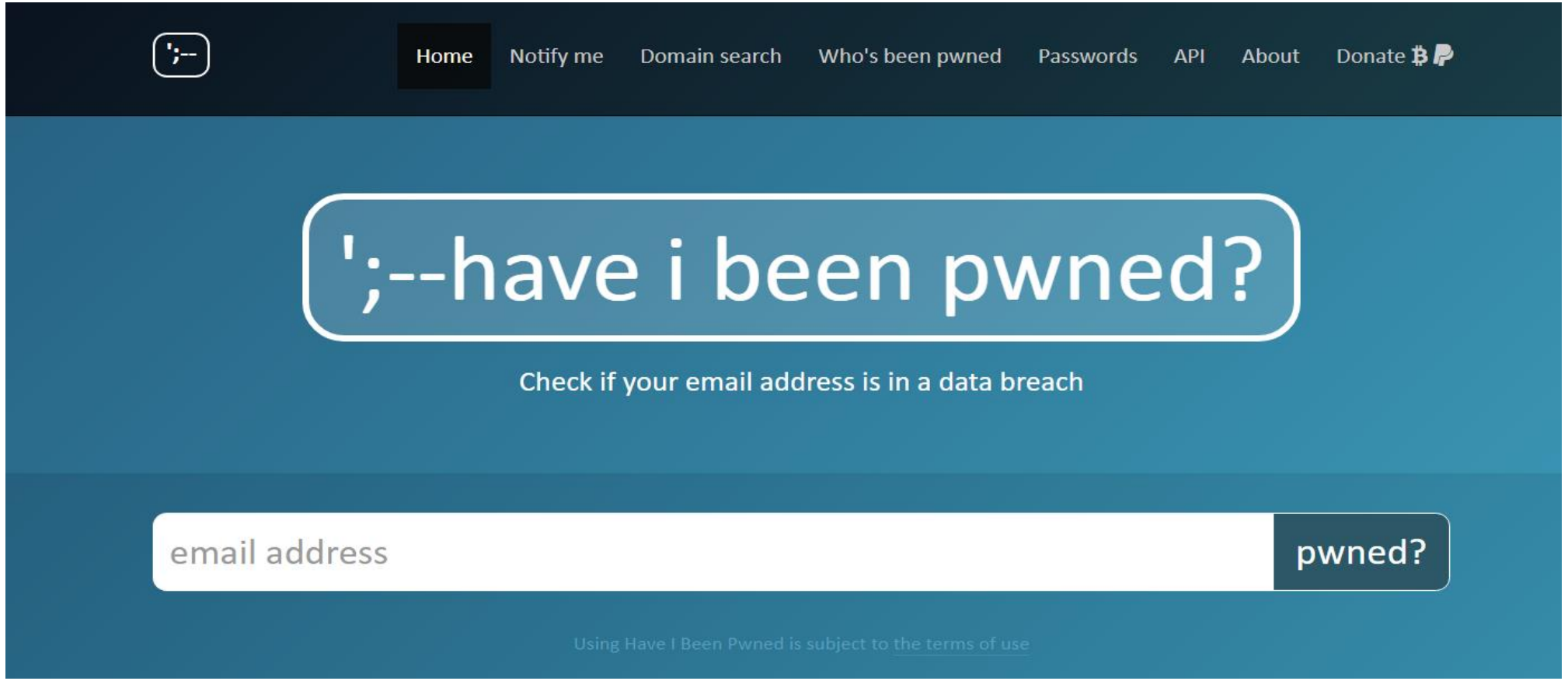
*#21#

*#06#

*#1234#

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

Czy moje dane wyciekły?



„Have I Been Pwned?”

https://haveibeenpwned.com/

UCZELNIA TECHNICZNO-HANDLOWA im. H. Chodkowskiej w Warszawie

7 Zasad Bezpiecznego Korzystania z Wi-Fi

Nr	Zasada	Opis	Przykład
1	**Unikaj korzystania z publicznych sieci Wi-Fi**	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	**Wyłącz udostępnianie plików na urządzeniach w publicznych sieciach Wi-Fi**	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	**Sprawdzaj, do jakiej sieci się łączysz**	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	**Wyłącz automatyczne łączenie z sieciami Wi-Fi**	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	**Stosuj silne hasła do swojej domowej sieci Wi-Fi**	Silne hasła utrudniają nieautoryzowany dostęp do Twojej sieci.	Użyj kombinacji liter, cyfr i symboli, np. "H@rd2Gu3ssP@ssw0rd".
6	**Zmień domyślne nazwy użytkownika i hasła routera**	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	**Aktualizuj oprogramowanie routera**	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.

UCZELNIA TECHNICZNO-HANDLOWA im. H. Chodkowskiej w Warszawie

„Magia” udostępnianych informacji

Amazing mind reader reveals his 'gift'

UCZELNIA TECHNICZNO-HANDLOWA im. H. Chodkowskiej w Warszawie

Więcej

Dawka informacji ze świata technologii, sztucznej inteligencji oraz cyberbezpieczeństwa.

UCZELNIA
TECHNICZNO-HANDLOWA
im. H. Chodkowskiej
w Warszawie

Dziękuję za uwagę !

Cyberbezpieczny z UTH