Bezpieczna Wieś 2.0

Zwiększenie bezpieczeństwa cyfrowego społeczności lokalnej

KOMITET DO SPRAW POŻYTKU PUBLICZNEGO

NIW Narodowy Instytut Wolności Centrum Rozwoju Społeczeństwa Obywatelskiego

Rządowy Program Wsparcia Organizacji Pozarządowych Moc Małych Społeczności

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI – CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO W RAMACH RZĄDOWEGO PROGRAMU WSPARCIA ORGANIZACJI POZARZĄDOWYCH MOC MAŁYCH SPOŁECZNOŚCI

ESCUELA

Bezpieczna Wieś 2.0

zwiększenie bezpieczeństwa cyfrowego społeczności lokalnej

Autor:

Zbigniew Szulczyk

Skład i łamanie:

Zbigniew Szulczyk

Wydawca:

Fundacja Escuela

Podmieście 26

26-920 Gniewoszów

ISBN: 978-83-972964-0-4

Spis treści

Wstęp 6
Bezpieczne korzystanie z Internetu 7
Higiena cyfrowa 7
Korzystanie z mediów społecznościowych 11
Ćwiczenia 14
Cyberzagrożenia i ochrona danych osobowych 15
Tworzenie bezpiecznych haseł 15
Phishing 16
Wyłudzenia danych osobowych (Identity Theft) 16
Ransomware 17
Man in the Middle (MitM) 18
CEO Fraud 18
Niebezpieczne oprogramowanie 19
Próby wyłudzenia środków finansowych i szantaże 20
Podsumowanie 21
Ćwiczenia 22
Dezinformacja – zagrożenia i sposoby obrony 26
Wprowadzenie w temat 26
Pojęcia związane z dezinformacją 26
Zagrożenia związane z dezinformacją 28
Twórcy dezinformacji 29
Piramida twórców dezinformacji 29
Charakterystyczne cechy fake newsa 31
Dlaczego ulegamy dezinformacji 32
Walka z dezinformacją 33
Portale weryfikujące informacje 33
Programy weryfikujące informację 35

Wstęp

Żyjemy w świecie, w którym Internet i nowe technologie są obecne w niemal każdej sferze życia – od nauki i pracy, po zakupy, rozrywkę i kontakty z innymi ludźmi. Dają nam ogromne możliwości, ale jednocześnie stawiają przed nami nowe wyzwania związane z bezpieczeństwem cyfrowym, ochroną prywatności oraz zachowaniem równowagi pomiędzy światem online i offline. Coraz częściej mówi się o higienie cyfrowej, czyli świadomym i odpowiedzialnym korzystaniu z technologii w taki sposób, by wspierały one rozwój i codzienne funkcjonowanie, a nie szkodziły zdrowiu fizycznemu, psychicznemu i relacjom społecznym.

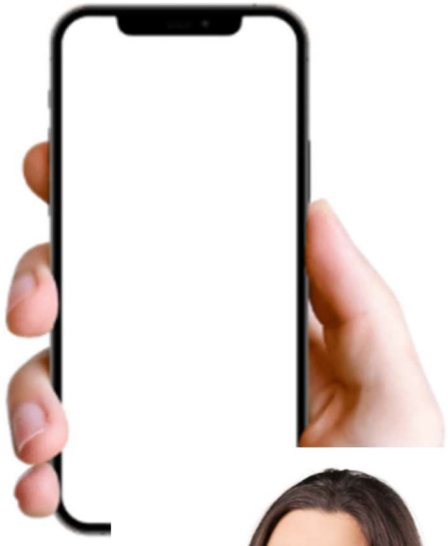
Celem tego podręcznika jest wsparcie uczniów, nauczycieli, rodziców i edukatorów w budowaniu świadomych postaw młodych użytkowników Internetu. Publikacja pokazuje, jak uczyć dzieci i młodzież mądrego korzystania z sieci, kontrolowania czasu ekranowego, bezpiecznego udostępniania informacji oraz rozpoznawania zagrożeń cyfrowych – takich jak phishing, wyłudzanie danych czy dezinformacja. Omawia także rolę mediów społecznościowych, ich możliwości i ograniczenia wiekowe, a przede wszystkim uczy, jak chronić prywatność i zachować równowagę między życiem cyfrowym a realnym.

Znajdziesz tu zarówno przystępne wyjaśnienia kluczowych pojęć i zagrożeń, jak i praktyczne narzędzia dydaktyczne, wskazówki dla dzieci i rodziców oraz przegląd przydatnych aplikacji i portali do weryfikacji informacji. Dzięki nim możliwe jest prowadzenie atrakcyjnych zajęć w szkołach i w grupach młodzieżowych, które nie tylko przekazują wiedzę, ale także kształtują krytyczne myślenie, odpowiedzialność i umiejętność bezpiecznego poruszania się w Internecie.

Mamy nadzieję, że ten podręcznik stanie się dla Ciebie praktycznym przewodnikiem, inspiracją do rozmów o bezpieczeństwie cyfrowym i źródłem pomysłów na nowoczesne lekcje, które łączą naukę z aktywnością i refleksją nad świadomym korzystaniem z technologii.

Bezpieczne korzystanie z Internetu

Higiena cyfrowa



Internet jest niezbędny w nauce, pracy i rozrywce, ale jego nadmiar szkodzi zdrowiu i relacjom. Higiena cyfrowa to świadome dbanie o równowagę między światem online a offline. Polega na planowaniu czasu przed ekranem, wybieraniu wartościowych treści, dbaniu o bezpieczeństwo i zdrowie fizyczne.

Zbyt długie korzystanie z sieci powoduje zmęczenie oczu, bóle pleców, problemy ze snem, spadek koncentracji, rozdrażnienie, a nawet uzależnienie i izolację społeczną. Aby temu zapobiec, warto wprowadzić kilka prostych zasad. Należy ustalać limity czasu online, robić przerwy co 45–60 minut i stosować regułę 20-20-20: co 20 minut przez 20 sekund patrzeć w dal. Dobrze jest odkładać telefon przed snem, ograniczać powiadomienia i media społecznościowe, utrzymywać prawidłową postawę ciała oraz używać filtrów światła niebieskiego.Pomocne są narzędzia takie jak aplikacje do kontroli czasu ekranowego (np. Digital Wellbeing, Screen Time) czy tryby skupienia, a rodzice mogą korzystać z funkcji kontroli rodzicielskiej. Ważne jest też dawanie dobrego przykładu dzieciom – wspólne ustalenie zasad (np. brak telefonów przy posiłkach) i zachęcanie do aktywności offline

sprzyja zdrowym nawykom. Higiena cyfrowa nie oznacza rezygnacji z technologii, lecz mądre korzystanie z niej. Świadome planowanie czasu, robienie przerw, dbałość o zdrowie i unikanie nadmiaru bodźców pozwala w pełni korzystać z Internetu, zachowując równowagę między życiem online i offline.

Poniższe tabele przedstawiają zalecane proporcje między aktywnością fizyczną, czasem spędzanym w bezruchu oraz korzystaniem z ekranów w zależności od wieku dziecka. Uwzględniają one zarówno potrzeby rozwojowe najmłodszych, jak i zasady zdrowej higieny cyfrowej. Dzięki nim rodzice, nauczyciele i opiekunowie mogą świadomie kształtować codzienny rytm dnia, dbając o prawidłowy sen, odpowiednią ilość ruchu oraz ograniczanie czasu spędzanego przed ekranem.

Zalecany czas ekranowy u dzieci poniżej 5 roku życia według Światowej Organizacji Zdrowia (WHO)

Wiek	Zalecenia
0-1 rok	Kilka razy dziennie różne aktywności; dla niechodzących co najmniej 30 min leżenia na brzuszku. Nie dłużej niż 1 h ciągłego przebywania w wózku/krzesełku/nosidle. **Czas ekranowy niewskazany** – zamiast tego zaleca się czytanie i opowiadanie. Sen: 0–3 mies. 14–17 h/dobę; 4–11 mies. 12–16 h.

1-2 lata	Co najmniej 180 min aktywności o różnej intensywności w ciągu dnia. Nie dłużej niż 1 h przebywania w bezruchu. 1 r.ż. – bez czasu ekranowego; 2 r.ż. – **co najwyżej 1 h/dzień** wysokojakościowego czasu ekranowego z opiekunem (mniej = lepiej) . Czytanie i opowiadanie z opiekunem. Sen: 11–14 h/dobę z drzemkami, stałe pory snu.
3-4 lata	Co najmniej 180 min aktywności, w tym co najmniej 60 min umiarkowanej lub dużej intensywności. Nie dłużej niż 1 h przebywania w bezruchu. Czas ekranowy **co najwyżej 1 h/dzień** (mniej = lepiej). Czytanie i opowiadanie z opiekunem. Sen: 10–13 h/dobę (może być drzemka), stałe pory snu.

Źródło: Guidelines On Physical Activity, Sedentary Behaviour And Sleep For Children Under 5 Years Of Age
https://iris.who.int/server/api/core/bitstreams/60a1cbaa-2bef-4251-9557-e52ce22112b3/content

FUNDACJA DAJEMY DZIECIOM SIŁĘ

Zalecane zasady korzystania z Internetu rekomendowane przez Fundację Dajemy Dzieciom Siłę

Wiek	Zalecenia	Komentarz
Do 2 roku życia	Kontakt z ekranem niezalecany	Dopuszczalna aktywność np. wideokonferencja z rodzicem lub bliską osobą.
3-5 lat	Kontakt z ekranem okazjonalny	Czas ekranowy okazjonalny, ekran nieinteraktywny (np. bajki a nie gry. Obecność dorosłego wymagana. Zalecane 2–3 dni w tygodniu bez czasu ekranowego.

6-9 lat	Do 1 h dziennie (2 godz. okazjonalnie, np. w weekend)	Zalecany podział na krótsze sesje oraz przerwy. Konieczna kontrola i dobór treści przez opiekuna. Zalecane 2–3 dni w tygodniu bez czasu ekranowego.
10-12 lat	Do 2 h dziennie	Czas ekranowy nie powinien stanowić więcej niż 30 % czasu wolnego dziecka. Zalecane 1-2 dni w tygodniu bez czasu ekranowego.
13-15 lat	Do 30% czasu wolnego dziennie np. 2h oraz 4h w weekendy	Czas ekranowy nie powinien stanowić więcej niż 30 % czasu wolnego dziecka. Elastyczne dostosowanie do potrzeb np. jednego dnia mniej innego więcej.
Powyżej 15 lat	Do 30% czasu wolnego dziennie np. 2h oraz 4h w weekendy	Czas przed ekranem nie powinien być nagrodą ani karą. Powinien być traktowany jako jedna z aktywności, która – jak każda – ma swoje miejsce i czas.

Źródło: Fundacja Dajemy Dzieciom Siłę: Domowe Zasady Ekranowe
https://domowezasadyekranowe.fdds.pl/zasady/ograniczaj-czas-przed-ekranem/?utm_source=chatgpt.com

Korzystanie z mediów społecznościowych

Media społecznościowe stały się jednym z głównych narzędzi komunikacji, rozrywki i zdobywania informacji. Dzięki nim możemy utrzymywać kontakt z rodziną i znajomymi, dzielić się zdjęciami, filmami, własnymi opiniami, a także poznawać nowe osoby i śledzić wydarzenia ze świata. Najpopularniejsze platformy mają różne funkcje i grupy odbiorców. Facebook służy głównie do kontaktu ze znajomymi, tworzenia wydarzeń i grup tematycznych, a jego użytkownikami są zarówno dorośli, jak i starsza młodzież. Instagram skupia się na zdjęciach i krótkich filmach, a TikTok na dynamicznych, krótkich nagraniach wideo, które szczególnie przyciągają nastolatków. YouTube to największa platforma wideo, oferująca zarówno treści edukacyjne, jak i rozrywkowe, natomiast Snapchat pozwala na przesyłanie zdjęć i filmów znikających po określonym czasie. X (dawniej Twitter) służy do szybkiego przekazywania informacji i opinii, często wykorzystywany jest przez dziennikarzy i osoby publiczne. LinkedIn to z kolei platforma skierowana do dorosłych użytkowników i środowiska biznesowego.

Większość serwisów społecznościowych ustala minimalny wiek użytkownika na 13 lat, co wynika z przepisów o ochronie prywatności dzieci w Internecie (COPPA w USA, RODO w Europie). Facebook, Instagram, TikTok, Snapchat, X czy LinkedIn pozwalają na założenie konta od 13. roku życia, a w przypadku osób poniżej 16 lat w niektórych krajach wymagana jest zgoda rodziców. YouTube również wymaga ukończenia 13 lat, choć dla młodszych dzieci przewidziano

specjalną aplikację YouTube Kids, umożliwiającą bezpieczniejsze oglądanie treści pod kontrolą opiekuna.

Korzystanie z mediów społecznościowych niesie ze sobą wiele zagrożeń. Jednym z nich jest uzależnienie od Internetu, które objawia się nieustannym sprawdzaniem powiadomień i trudnością w oderwaniu się od ekranu. Częstym problemem jest hejt i cyberprzemoc, czyli obraźliwe komentarze, ośmieszanie czy wykluczanie w sieci, które mogą wpływać na samoocenę i zdrowie psychiczne. W mediach społecznościowych łatwo też trafić na nieprawdziwe informacje i teorie spiskowe, które mogą wprowadzać w błąd. Istnieje również ryzyko kontaktu z nieznajomymi, którzy mogą podszywać się pod kogoś innego w celu manipulacji lub oszustwa. Publikowanie prywatnych danych, zdjęć czy lokalizacji zwiększa ryzyko utraty prywatności lub kradzieży tożsamości. Niektóre treści, takie jak przemoc, pornografia czy niebezpieczne wyzwania, mogą być szkodliwe dla rozwoju dzieci i młodzieży.

Aby korzystać z mediów społecznościowych w sposób bezpieczny, warto przestrzegać kilku zasad. Przede wszystkim należy dbać o prywatność – nie podawać adresu, numeru telefonu ani miejsca pobytu, a ustawienia konta ustawić tak, by dostęp do publikowanych treści mieli jedynie zaufani znajomi. Warto publikować z rozwagą, pamiętając, że wszystko, co trafi do sieci, może zostać zapisane lub wykorzystane bez zgody autora. Ważne jest stosowanie silnych, unikalnych haseł i włączanie uwierzytelniania dwuetapowego. Nie powinno się przyjmować zaproszeń od obcych osób, a w przypadku hejtu lub nękania – blokować sprawców i zgłaszać ich administratorom serwisu lub osobom dorosłym. Istotne jest także ograniczanie czasu spędzanego online i wprowadzanie przerw od ekranu, aby zachować równowagę między światem cyfrowym a realnym. Przy przeglądaniu treści warto zachować krytyczne myślenie i sprawdzać informacje w kilku

źródłach. Jeśli coś w Internecie wzbudza niepokój lub niepewność, warto porozmawiać z rodzicem, nauczycielem lub inną zaufaną osobą.

Świadome i bezpieczne korzystanie z mediów społecznościowych pozwala czerpać z nich korzyści – utrzymywać kontakt z innymi, rozwijać zainteresowania czy zdobywać wiedzę – jednocześnie chroniąc prywatność, zdrowie psychiczne i czas potrzebny na inne ważne aktywności. Odpowiedzialne podejście, znajomość ograniczeń wiekowych oraz stosowanie zasad bezpieczeństwa pomagają korzystać z Internetu mądrze i bez szkody dla siebie.

Pamiętaj:

- **Ustaw konto jako prywatne** i ogranicz widoczność postów tylko dla znajomych.
- **Nie udostępniaj danych osobowych** – adresu, szkoły, numeru telefonu, miejsca pobytu.
- **Publikuj z rozwagą** – zdjęcia i komentarze mogą pozostać w sieci na zawsze.
- **Stosuj silne, unikalne hasła** i włącz weryfikację dwuetapową.
- **Nie dodawaj obcych osób** – akceptuj zaproszenia tylko od znanych Ci ludzi.
- **Reaguj na hejt i nękanie** – blokuj agresywnych użytkowników, zgłaszaj nieodpowiednie treści.
- **Ogranicz czas spędzany w sieci** – rób przerwy i ustal limity dla aplikacji.
- **Sprawdzaj informacje** – weryfikuj źródła, aby nie dać się wprowadzić w błąd.
- **Nie klikaj podejrzanych linków** – unikniesz wirusów i kradzieży danych.
- **Rozmawiaj z dorosłymi** – jeśli coś Cię zaniepokoi, zgłoś to rodzicowi lub nauczycielowi.

Ćwiczenia

1. Zgodnie z zasadami opracowanymi przez Fundację Dajemy Dzieciom Siłę, dziecko w wieku 11 lat może korzystać z ekranu przez jaki czas dziennie?

.....

.....

2. Zgodnie z zasadami opracowanymi przez Fundację Dajemy Dzieciom Siłę, maksymalnie jaki procent wolnego czasu można spędzać przed ekranem?

.....

.....

3. Na czym polega zasada 20-20-20?

.....

.....

4. Od jakiego wielu można legalnie założyć konto na FB?

.....

.....

5. Jakich danych nie powinieneś publikować w mediach społecznościowych?

.....

.....

Cyberzagrożenia i ochrona danych osobowych

Tworzenie bezpiecznych haseł

Współczesny świat w coraz większym stopniu opiera się na technologiach cyfrowych. Korzystamy z Internetu w nauce, pracy, rozrywce, kontaktach z innymi ludźmi, a także do załatwiania codziennych spraw, takich jak zakupy czy bankowość. To ogromne udogodnienie, ale jednocześnie niesie ze sobą ryzyko. Każde nasze kliknięcie, hasło czy przesłana informacja może stać się celem cyberprzestępców.

Szczególnie ważna jest ochrona danych osobowych (np. imienia, nazwiska, adresu, numeru PESEL, loginów, numerów kart płatniczych) oraz haseł, które pełnią rolę kluczy do naszych kont w sieci. Utrata kontroli nad nimi może prowadzić do kradzieży pieniędzy, podszywania się pod nas czy utraty prywatności. Z związku z tym przestrzegaj następujących zasad tworzenia haseł:

- Hasło powinno mieć minimum 12 znaków i zawierać litery małe i wielkie, cyfry oraz znaki specjalne.
- Należy unikać oczywistych kombinacji, takich jak *123456*, *qwerty* czy imię plus rok urodzenia.
- Dla każdego konta powinno się stosować inne hasło – dzięki temu wyciek z jednego serwisu nie narazi nas na utratę wszystkich danych.
- Warto korzystać z menedżerów haseł, które bezpiecznie przechowują i generują skomplikowane hasła.
- W miarę możliwości należy włączać uwierzytelnianie dwuskładnikowe (2FA), np. kod SMS lub aplikację mobilną.

Phishing

Phishing to podszywanie się pod zaufane instytucje w celu wyłudzenia danych (np. bank, szkołę, portale społecznościowe).

Przykłady wyłudzeń:

- e-mail od „banku" z prośbą o zalogowanie się przez link,
- SMS z informacją o dopłacie kilku złotych do paczki,
- SMS z informacją „Twoja paczka jest opóźniona, kliknij w link aby ją śledzić"
- ogłoszenie sprzedażowe z linkiem do „potwierdzenia płatności".

Jak się bronić:

- nie klikaj w podejrzane linki,
- sprawdzaj adres strony i certyfikat (bezpieczne strony posiadają certyfikat SSL, rozpoznasz je kłódce przy adresie oraz początku „https://" zamiast „http://"),
- nigdy nie podawaj haseł przez SMS czy e-mail.

Wyłudzenia danych osobowych (Identity Theft)

Częstym problemem jest kradzież danych osobowych, w szczególności numeru PESEL oraz danych z dowodu osobistego i użycie ich do zaciągania zobowiązań lub podszywania się pod ofiarę.

Przykłady wyłudzeń:

- konto na Facebooku założone na cudze dane,
- pożyczka wzięta na cudzy PESEL,
- podszywanie się pod ucznia lub nauczyciela.

Jak się bronić:

- nie publikuj swoich wrażliwych danych w sieci,
- chroń dokumenty tożsamości (nie wysyłaj skanu dowodu osobistego bez pewności, że jest to bezpieczne i konieczne),
- zastrzeż swój numer PESEL (np. w aplikacji mObywatel), co zapobiega wzięciu pożyczki na twoje dane osobowe

Ransomware

Ransomware jest to złośliwe oprogramowanie szyfrujące pliki i blokujące dostęp do komputera w celu wyłudzenia okupu.

Przykłady wyłudzeń:

- podczas gry online otrzymujesz od innego gracza wiadomość o niesamowitej promocji; wystarczy jedynie zainstalować upgrade na swoim komputerze; instalacja programu kończy się zablokowaniem dostępu do komputera i żądaniem okupu,
- instalujesz potrzeby program z niepewnego źródła; po jego zainstalowaniu dostęp do Twojego komputera jest zablokowany po czym otrzymujesz żądanie okupu.

Jak się bronić:

- rób kopie zapasowe, najważniejszych plików na Twoim komputerze,
- nie otwieraj podejrzanych załączników,
- nigdy nie instaluj oprogramowania z niepewnych i nielegalnych źródeł,
- aktualizuj system i używaj antywirusa.

Man in the Middle (MitM)

Man in the Middle jest to podsłuchiwanie połączeń między użytkownikiem a serwisem, najczęściej bankiem. MitM ma miejsce na przykład podczas prób połączenia z bankiem w niezabezpieczonych sieciach Wi-Fi, czy też przez prośbę o interwencję, podczas której przestępca podsłuchuje rozmowę użytkownika z bankiem, który weryfikuje jego tożsamość.

Przykłady wyłudzeń:

- prośba o kontakt z bankiem przez „konsultanta-przestępcę”
- fałszywe Wi-Fi, przez którą przestępca przechwytuje hasła i dane osobowe.

Jak się bronić:

- unikaj logowania do banku w publicznych sieciach,
- używaj VPN,
- sprawdzaj czy strony posiadają certyfikat bezpieczeństwa SSL (strony posiadają symbol kłódki oraz zaczynają się od: https://).

CEO Fraud

CEO Fraud jest to podszywanie się pod dyrektora, przełożonego firmy lub też podszywanie się pod urzędnika w celu wyłudzenia danych lub pieniędzy.

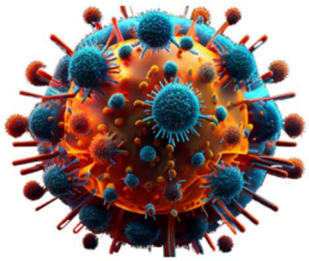
Przykłady wyłudzeń:

- e-mail „od dyrektora szkoły” z prośbą o pilny przelew na wycieczkę dziecka,
- wiadomość od urzędnika Urzędu Skarbowego z informacją o konieczności zapłaty zaległego podatku,
- wiadomość podszywająca się pod prezesa firmy, ze zleceniem zaległego przelewu do kontrahenta.

Jak się bronić:

- zawsze weryfikuj nadawcę,
- przy „pilnych” poleceniach przelewów potwierdź konieczność wykonania płatności osobiście lub telefonicznie tzn. zadzwoń na numer telefonu znajdujący się na oficjalnej stronie internetowej instytucji (telefon podany w wiadomości może być nieprawdziwym telefonem do oszusta),
- nie przekazuj poufnych danych wyłącznie na podstawie e-maila.

Niebezpieczne oprogramowanie



Niebezpieczne oprogramowanie spowalniające działanie systemu, zawierające oprogramowanie szpiegowskie czy też korzystające z mocy obliczeniowej komputera najczęściej instalowane jest wraz z oprogramowaniem z nielegalnych lub niepewnych źródeł.

Przykłady wyłudzeń:

- darmowa gra wykradająca dane,
- aplikacja podszywająca się pod aplikację bankową.

Jak się bronić:

- pobieraj aplikacje i programy tylko z oficjalnych sklepów,
- kontroluj uprawnienia aplikacji.

Próby wyłudzenia środków finansowych i szantaże

Oszuści coraz częściej wykorzystują szybkie płatności (np. BLIK) oraz silne emocje, podszywając się pod znajomych czy instytucje. Często stosują też szantaż, aby wymusić przelew.

Przykłady wyłudzeń:

- SMS lub wiadomość na Messengerze od znajomego: *„Hej, zabrakło mi 50 zł na zakupach, prześlij mi proszę BLIK”*.
- podszywanie się pod ZAiKS lub inną instytucję: *„Szanowna Pani, podczas lekcji korzystała Pani z utworów muzycznych objętych prawami autorskimi. Proszę o wpłatę 400 zł w celu uregulowania zobowiązań wynikających z ZAiKS. W przeciwnym wypadku zostanie wobec Pani wszczęte postępowanie sądowe”*.
- próby szantażu: *„Zgraliśmy pliki z Twojego telefonu. Przelej 1000 zł na wskazany rachunek, albo zdjęcia zostaną rozesłane do wszystkich Twoich znajomych”*.

Jak się bronić:

- zawsze kontaktuj się bezpośrednio ze znajomym, zanim przelejesz pieniądze,
- nie ufaj nagłym prośbom o płatność – szczególnie, gdy pojawia się presja czasu,
- ignoruj i zgłaszaj szantaże – instytucje publiczne nie żądają wpłat przez SMS czy komunikatory,
- w razie podejrzenia oszustwa lub szantażu poinformuj rodziców, nauczyciela lub policję.

Podsumowanie

Zasady bezpiecznego korzystania z Internetu

- Chroń dane osobowe i hasła, stosuj silne zabezpieczenia.
- Stosuj zasadę ograniczonego zaufania wobec wiadomości i próśb o pieniądze.
- Zawsze weryfikuj nadawcę i instytucję, zanim podejmiesz działanie.
- Regularnie aktualizuj oprogramowanie i rób kopie zapasowe danych.
- Korzystaj z oficjalnych źródeł aplikacji i serwisów.
- Pamiętaj, że cyberprzestępcy często wykorzystują emocje – pośpiech, strach czy chęć pomocy. Nigdy nie ulegaj presji.

Ćwiczenia

Poniżej znajdują się screeny wiadomości zawierających próby wyłudzenia danych. Uzasadnij, dlaczego jest to oszustwo.

1.

Od: "Allegro Raty Od.nowa" <play2@mailersenderabd.com>
Data: 30 września 2020 o 03:40:15 CEST
Do:
Temat: Potwierdzenie wysłania wniosku o kredyt na zakupy Raty Od.nowa

allegro

Witaj

Zaakceptuj swoją prośbę o przyznanie kredytu Raty Od.nowa.

Przypominamy, że wniosek o przyznanie kredytu Raty Od.nowa został wysłany prawidłowo. Zanim wypełniony formularz zostanie przesłany do banku udzielającego pożyczki potrzebujemy dodatkowej weryfikacji email.

Przejdź do wniosku

Decyzja jest podejmowana przez bank lub pośrednika pożyczkowego niezwłocznie po odebraniu formularza. Prawdopodobnie odbierzesz ją do kilku minut od dostarczenia wypełnionego formularza. W przypadku, kiedy nie jest możliwe podjęcie decyzji natychmiast, otrzymasz ją w możliwie najkrótszym czasie, a Allegro prześle Tobie e-mail z informacją o decyzji o kredycie ratalnym.

2.

File Edit View Go Message Tools Help

Get Messages | Write | Chat | Address Book | Tag

From DHL Express Cargo <delivery@dhl.com> | Reply | Reply All | Forward | More

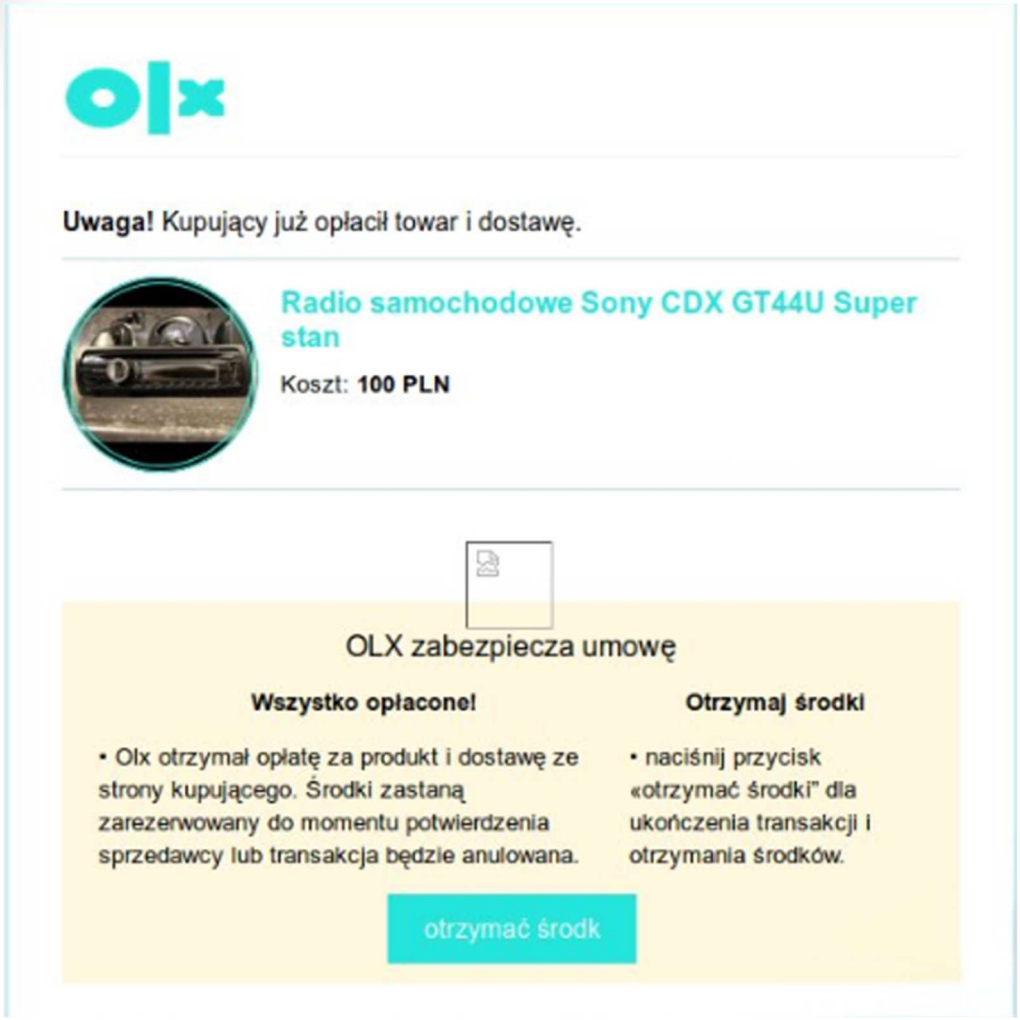
Subject **DOSTAWA DHL CARGO** 09:56

PACZKI NUMBER: DHL119040
DATA PRZYJAZDU: wtorek 3 sierpnia 2021 r.

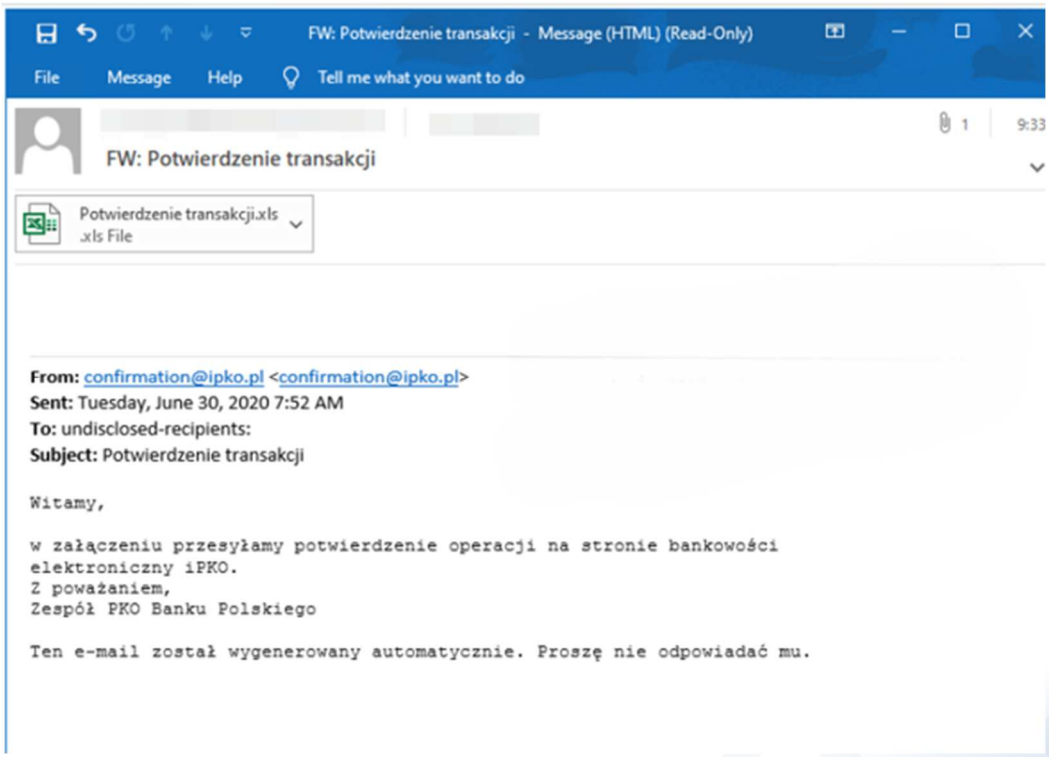
DHL ON DEMAND DELIVERY

Szanowny Kliencie,
Twoja przesyłka dotarła do biura. nasz courier nie był w stanie dostarczyć go na Twój adres z powodu błędnego adresu podanego przez naszego klienta.
Aby odebrać przesyłkę, udaj się do jednego z naszych najbliższych biur i pokaż ten pokwitowanie.
KLIKNIJ W DODATEK, ABY POBRAĆ I WYDRUKOWAĆ PARAGON.
Z wyrazami szacunku,
Zespół DHL

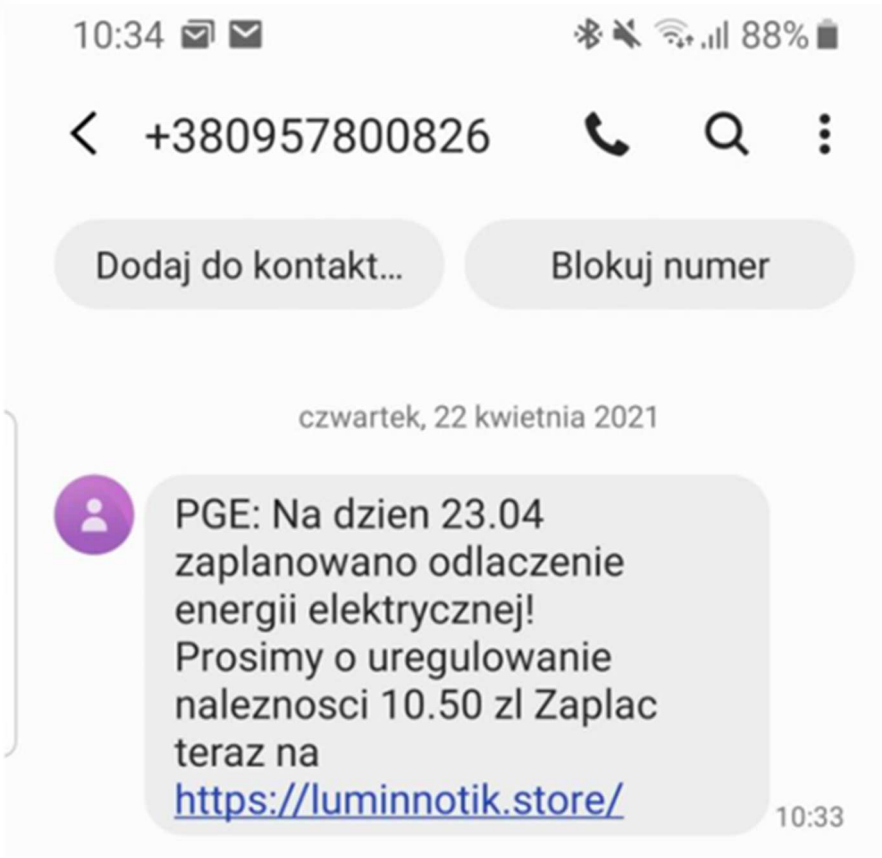
3.


olx
Uwaga! Kupujący już opłacił towar i dostawę.
Radio samochodowe Sony CDX GT44U Super stan
Koszt: 100 PLN
OLX zabezpiecza umowę
Wszystko opłacone!
• Olx otrzymał opłatę za produkt i dostawę ze strony kupującego. Środki zastaną zarezerwowany do momentu potwierdzenia sprzedawcy lub transakcja będzie anulowana.
Otrzymaj środki
• naciśnij przycisk «otrzymać środki" dla ukończenia transakcji i otrzymania środków.
otrzymać środk

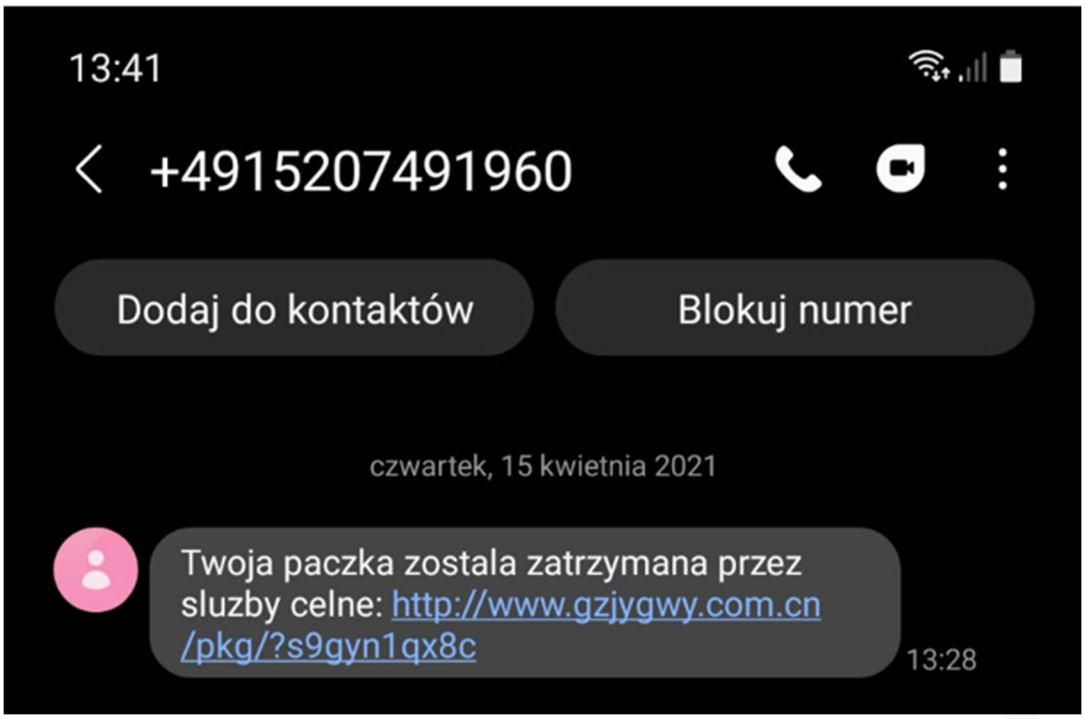
4.


FW: Potwierdzenie transakcji - Message (HTML) (Read-Only)
File
Message
Help
Tell me what you want to do
1
9:33
FW: Potwierdzenie transakcji
Potwierdzenie transakcji.xls
.xls File
From: confirmation@ipko.pl <confirmation@ipko.pl>
Sent: Tuesday, June 30, 2020 7:52 AM
To: undisclosed-recipients:
Subject: Potwierdzenie transakcji
Witamy,
w załączeniu przesyłamy potwierdzenie operacji na stronie bankowości elektroniczny iPKO.
Z poważaniem,
Zespół PKO Banku Polskiego
Ten e-mail został wygenerowany automatycznie. Proszę nie odpowiadać mu.

5.


10:34
88%
+380957800826
Dodaj do kontakt...
Blokuj numer
czwartek, 22 kwietnia 2021
PGE: Na dzien 23.04 zaplanowano odlaczenie energii elektrycznej! Prosimy o uregulowanie naleznosci 10.50 zl Zaplac teraz na https://luminnotik.store/
10:33

6.


13:41
+4915207491960
Dodaj do kontaktów
Blokuj numer
czwartek, 15 kwietnia 2021
Twoja paczka zostala zatrzymana przez sluzby celne: http://www.gzjygwy.com.cn/pkg/?s9gyn1qx8c
13:28

7.


21:42
27%
POLICJA
Usuń
wtorek, 30 marca 2021
Masz nie oplacony mandat karny.
W dniu 31.03.2021 twoj mandat
zostanie przekazany do komornika z
tytulu zaleglosci 10.00 PLN
Oplac teraz www.placimy24.
87669

Dezinformacja – zagrożenia i sposoby obrony

Wprowadzenie w temat

Żyjemy w epoce natłoku informacji, gdzie wiadomości docierają do nas błyskawicznie poprzez media tradycyjne i internetowe. Ten nieograniczony dostęp do treści niesie jednak ryzyko zetknięcia się z fałszywymi przekazami – fake newsami i dezinformacją. Zbyt szybki rozwój technologii spowodował, że odbiorcy coraz częściej czują się zagubieni w gąszczu wiadomości, a brak odpowiednich umiejętności krytycznego myślenia sprawia, że łatwo ulegają manipulacji.

Dezinformacja nie tylko wpływa na indywidualne wybory – np. decyzje zakupowe czy zdrowotne – lecz także na postawy społeczne i polityczne. Może prowadzić do polaryzacji społecznej, podsycania emocji czy wzmacniania podziałów w społeczeństwie. Dlatego zrozumienie mechanizmów dezinformacji i rozwijanie kompetencji informacyjnych jest dziś jedną z kluczowych umiejętności obywatelskich.

Pojęcia związane z dezinformacją

- **Fałszywe informacje (False News)** – ogólne określenie na wszystkie treści nieprawdziwe w mediach (plotki, fake newsy, propaganda, clickbaity, scam, phishing)
- **Fake news** – wiadomości całkowicie lub częściowo zmyślone, podszywające się pod prawdziwe informacje. Mogą być intencjonalne (dla zysku, wpływu politycznego) albo nieintencjonalne (rozpowszechniane przez użytkowników bez świadomości).
- **Dezinformacja intencjonalna (disinformation)** – celowe tworzenie fałszywych treści, aby wprowadzić odbiorców w błąd, zmanipulować lub osiągnąć zysk.

- **Dezinformacja niezamierzona (misinformation)** – powielanie fałszywych treści w dobrej wierze, np. udostępnienie przez znajomego niezweryfikowanego artykułu.
- **Złośliwe wiadomości (malinformation)** – prawdziwe treści ujawnione w złej intencji, np. publikacja prywatnej korespondencji lub informacji wrażliwych
- **Propaganda** – systematyczne oddziaływanie informacyjne, którego celem jest utrwalenie określonych postaw i poglądów w społeczeństwie. Wykorzystuje emocje, symbole, manipulację faktami
- **Manipulacja** – wywieranie wpływu na jednostki lub grupy w sposób ukryty, tak aby nieświadomie realizowały cele manipulatora. Często przybiera formę półprawd, teorii spiskowych czy sztucznego wzbudzania emocji.
- **Clickbait** – nagłówek lub tytuł skonstruowany tak, by przyciągnąć uwagę i kliknięcia, często oderwany od rzeczywistej treści artykułu.
- **Scam / Phishing** – oszustwo internetowe mające na celu zdobycie poufnych danych (np. numerów kart, loginów).
- **Plotka** – niesprawdzona, często sensacyjna wiadomość, która szybko się rozprzestrzenia, choć może nie mieć żadnych podstaw w faktach.
- **Treści pseudonaukowe** – komunikaty powołujące się na rzekome badania czy ekspertów, które w rzeczywistości nie mają podstaw naukowych.
- **Teorie spiskowe** – narracje zakładające ukryte działania grup lub organizacji kontrolujących świat, zwykle bez dowodów.
- **Bańka informacyjna (filter bubble)** – sytuacja, w której algorytmy mediów społecznościowych i wyszukiwarek pokazują użytkownikowi treści zgodne z jego wcześniejszymi poglądami, wzmacniając polaryzację.
- **Efekt echa (echo chamber)** – mechanizm, w którym użytkownik otoczony jest tylko informacjami zgodnymi z jego przekonaniami, przez co nabiera przeświadczenia, że jego pogląd jest powszechny i jedynie słuszny.
- **Boty i cyborgi** – automatyczne konta lub sieci kont sterowane przez ludzi, rozpowszechniające masowo treści dezinformacyjne
- **Trolle internetowe** – osoby publikujące kontrowersyjne lub fałszywe treści w celu wywołania emocji, chaosu i zamętu

Zagrożenia związane z dezinformacją

Dezinformacja stanowi jedno z największych wyzwań współczesnego świata, ponieważ wpływa zarówno na życie jednostek, jak i całych społeczeństw. Jej skutki widoczne są w wielu obszarach – od polityki, przez zdrowie publiczne, aż po relacje społeczne i gospodarkę. Najbardziej oczywistym zagrożeniem jest utrata zaufania do mediów, instytucji państwowych i nauki. Jeśli odbiorcy wielokrotnie spotykają się z fałszywymi treściami, zaczynają wątpić nawet w informacje prawdziwe, co prowadzi do chaosu informacyjnego i poczucia, że „nie wiadomo, komu wierzyć". Dezinformacja może być także wykorzystywana do manipulacji politycznej – fałszywe wiadomości o kandydatach czy partiach wpływają na decyzje wyborcze, pogłębiają polaryzację i osłabiają demokrację. W wymiarze społecznym dezinformacja często gra na emocjach – strachu, gniewie, poczuciu zagrożenia – co prowadzi do konfliktów i radykalizacji poglądów. Może także osłabiać więzi społeczne, podważać solidarność i wzmacniać podziały między grupami. Wreszcie, dezinformacja niesie zagrożenia ekonomiczne: fałszywe treści mogą powodować panikę na rynkach, wpływać na decyzje konsumentów, a także sprzyjać oszustwom finansowym i kradzieży danych. Wszystkie te zagrożenia łączy wspólny mianownik – osłabianie zaufania i zdolności społeczeństwa do podejmowania świadomych, racjonalnych decyzji.

Twórcy dezinformacji

Dezinformacja nie powstaje sama z siebie – za każdym fałszywym newsem, zmanipulowanym zdjęciem czy teorią spiskową stoją konkretni twórcy i mechanizmy. Mogą to być zarówno wyspecjalizowane instytucje i grupy działające na zlecenie państw, jak i pojedyncze osoby, które z różnych powodów decydują się rozpowszechniać nieprawdziwe informacje. Część z nich działa świadomie, dążąc do osiągnięcia celów politycznych, finansowych lub propagandowych, inni natomiast nieświadomie powielają treści, które wydają im się wiarygodne. Zrozumienie, kto i w jaki sposób tworzy oraz rozpowszechnia dezinformację, pozwala lepiej bronić się przed jej skutkami i rozwijać krytyczne podejście do docierających do nas wiadomości.

Piramida twórców dezinformacji

Na szczycie piramidy znajdują się operatorzy cyberpropagandy, czyli wyspecjalizowane jednostki – najczęściej powiązane z państwowymi służbami bezpieczeństwa – które planują i tworzą całe narracje propagandowe. To oni odpowiadają za strategiczne kampanie dezinformacyjne, zwane wojną informacyjną, których celem jest polaryzacja społeczeństwa, osłabienie przeciwnika i destabilizacja życia publicznego.

Niżej w hierarchii działają media i narzędzia dystrybucji treści. Są to portale informacyjne lub pseudoinformacyjne, często finansowane przez organizacje prowadzące działania propagandowe. W tej grupie mieszczą się także agenci wpływu oraz tzw. brygady sieciowe, które zajmują się masową produkcją i powielaniem spreparowanych wiadomości, aby zwiększyć ich zasięg i dotrzeć do jak największej liczby odbiorców.

Kolejnym poziomem są osoby publiczne i zwykli użytkownicy, którzy – świadomie lub nieświadomie – powielają fałszywe narracje. Mogą to być politycy, dziennikarze, celebryci, ale również uczniowie czy seniorzy. Ich rola jest bardzo istotna, ponieważ udostępniając niezweryfikowane treści w mediach społecznościowych, nadają im pozory wiarygodności.

Na samym dole piramidy znajdują się konsumenci fałszywych wiadomości, czyli odbiorcy, którzy bezrefleksyjnie przyjmują zasłyszane treści i rozpowszechniają je dalej, np. udostępniając posty w mediach społecznościowych czy przekazując informacje znajomym. Często tworzą też własne warianty dezinformacji, np. w formie memów, komentarzy czy przeróbek zdjęć.

Dodatkowym elementem wzmacniającym cały proces są boty i trolle internetowe. Boty to automatyczne konta w mediach społecznościowych, które masowo powielają fałszywe treści, zwiększając ich zasięg. Trolle natomiast to osoby, które celowo wywołują kłótnie, publikują prowokacyjne komentarze lub szerzą kontrowersyjne treści, aby wprowadzić chaos i zamęt w dyskusjach.

Rysunek 2. Kategorie twórców fake newsów. Opracowanie K. Rosińskiej na podstawie: Gu L., Kropotov V., Yarochkin F. (2017). The fake news machine: How propagandists abuse the Internet and manipulate the public. TrendMicro. https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf

Cechy fake newsa

Choć fałszywe informacje mogą przybierać różne formy, wszystkie mają pewne wspólne elementy. Należą do nich: autor lub osoba powielająca treść, potencjalni odbiorcy, kontekst społeczny, a także sama zawartość komunikatu. Analizując te składniki, można wyodrębnić cechy typowe dla fake newsów.

1. Pierwszym elementem jest twórca lub rozpowszechniający wiadomość. Fałszywe treści mogą być generowane zarówno przez bardzo aktywnych użytkowników Internetu, chętnie zabierających głos w dyskusjach i udzielających się społecznie, jak i przez fikcyjne konta czy boty. Te ostatnie zazwyczaj obserwują znacznie więcej profili, niż same mają obserwujących.
2. Drugim elementem są potencjalne ofiary, czyli osoby narażone na oddziaływanie fake newsów. Fałszywe treści zwykle nawiązują do realnych potrzeb lub lęków odbiorców, np. wiadomości medyczne kierowane do seniorów. Rozprzestrzeniają się one szczególnie w grupach tematycznych i w mediach społecznościowych, które wykorzystują psychologiczne skłonności użytkowników i ich relacje z innymi, aby budować zaufanie do przekazu.
3. Trzecim składnikiem jest kontekst społeczny. Fake newsy rozchodzą się wielokrotnie szybciej niż wiadomości prawdziwe – badania wskazują, że nawet sześć razy szybciej. Zyskują ogromną popularność w Internecie: są masowo udostępniane, komentowane i lajkowane, zwłaszcza w środowiskach o jednolitym lub skrajnie spolaryzowanym światopoglądzie.

4. Ostatnim elementem jest sama treść. Charakteryzuje się ona zwykle polaryzowaniem odbiorców, aktualnością, kontrowersyjnością, wywoływaniem silnych emocji oraz przekonywującym językiem. Pod względem formy fake newsy można rozpoznać po krzykliwych nagłówkach pisanych wielkimi literami, częstym użyciu znaków zapytania i wykrzykników,

rozpoczynaniu tytułu od liczby, obecności słów wzbudzających skrajne emocje czy słów negujących. Często zawierają one dużą liczbę grafik, emotikonów, hashtagów, a także podejrzane linki – puste, nietypowe lub z zaszyfrowanym adresem URL.

Dlaczego ulegamy dezinformacji

Uleganie dezinformacji to zjawisko złożone, które łączy w sobie mechanizmy psychologiczne, społeczne i technologiczne. Przede wszystkim ogromną rolę odgrywa sposób działania mediów społecznościowych. Każdy użytkownik, który polubi lub udostępni daną treść, staje się powielaczem, czyli osobą wzmacniającą jej wiarygodność w oczach innych. Polubienia i udostępnienia pełnią funkcję „pieczęci autentyczności" – jeśli coś widzimy u znajomego, zyskuje to większą moc przekonywania.

Naukowcy z Uniwersytetu Princeton dowiedli, że powielanie nieprawdziwych treści wynika w dużej mierze z nawyków, które kształtują algorytmy platform społecznościowych. Każde udostępnienie nagradzane jest większym zasięgiem, komentarzami i reakcjami, co zachęca użytkowników do dzielenia się treściami kontrowersyjnymi i emocjonalnymi – niezależnie od ich prawdziwości. System ten niejako premiuje szybkie i nieprzemyślane kliknięcia zamiast refleksji nad treścią.

Efekt ten potęguje zjawisko „społecznego dowodu słuszności", opisane przez Roberta Cialdiniego. Jeśli wiele osób udostępnia daną wiadomość, podświadomie uznajemy, że musi być ona prawdziwa, bo „tylu ludzi nie może się mylić". W rzeczywistości to właśnie masowe powielanie sprawia, że fałszywe treści wydają się bardziej wiarygodne niż są w istocie. W sieci działa też efekt echa – kiedy użytkownicy funkcjonują w bańkach informacyjnych, otoczeni wyłącznie podobnymi poglądami, fałszywe wiadomości stają się jeszcze mocniej ugruntowane.

Kolejnym powodem, dla którego łatwo ulegamy dezinformacji, są tzw. heurystyki poznawcze, czyli uproszczone sposoby oceniania rzeczywistości. Gdy nie mamy czasu lub wiedzy, aby sprawdzić wszystkie fakty, opieramy się na prostych przesłankach: emocjach (lęku, gniewie), potwierdzeniu własnych przekonań, autorytecie czy konformizmie. To dlatego wiadomości publikowane przez celebrytów czy znane osoby zyskują dodatkową wiarygodność – stereotypowo zakładamy, że „skoro odnieśli sukces, to wiedzą lepiej".

Znaczenie ma też psychologia perswazji: odpowiednio skonstruowane nagłówki, wzbudzanie strachu, poczucia zagrożenia lub przeciwnie – nadziei, wpływają na nasz osąd bardziej niż suche fakty. Dodatkowo internetowa anonimowość sprawia, że użytkownicy nie czują odpowiedzialności za to, co udostępniają czy komentują, a to jeszcze bardziej ułatwia rozprzestrzenianie fałszywych informacji.

Wszystkie te czynniki razem powodują, że dezinformacja rozchodzi się błyskawicznie, a jej skutki są bardzo poważne – od błędnych decyzji jednostek po wpływ na całe społeczeństwa.

Walka z dezinformacją

Portale weryfikujące informacje

Portale fact-checkingowe są narzędziem, które każdy użytkownik Internetu może wykorzystać, aby sprawdzić wiarygodność informacji. W praktyce korzystanie z nich jest bardzo proste: wystarczy wejść na stronę wybranego portalu i skorzystać z wyszukiwarki lub przeglądać już opublikowane analizy i dementi. Jeśli trafimy na wiadomość budzącą wątpliwości, możemy ją zgłosić do weryfikacji – np. poprzez formularz (Demagog, Fakenews.pl), wtyczkę przeglądarkową

(FakeHunter) czy specjalne sekcje raportowania. Wyniki sprawdzeń publikowane są w formie artykułów, raportów lub krótkich notatek z wyjaśnieniem i podaniem źródeł. Niektóre portale, jak Demagog czy NASK, oferują także materiały edukacyjne i kursy, które uczą rozpoznawania manipulacji i krytycznej analizy treści. Z kolei inicjatywy międzynarodowe, takie jak EU vs Disinfo czy polski Disinfo Digest, pozwalają śledzić bieżące kampanie dezinformacyjne i zrozumieć szerszy kontekst fałszywych narracji. Dzięki temu każdy internauta może szybko sprawdzić, czy dana wiadomość jest prawdziwa, i nie przyczyniać się do rozpowszechniania nieprawdziwych treści. Zapoznaj się z najbardziej popularnymi portalami:

- FakeHunter (PAP): Umożliwia każdemu zgłaszanie wątpliwych treści, które następnie są weryfikowane przez społecznych wolontariuszy i ekspertów – https://fakehunter.pap.pl
- Demagog: Specjalizuje się w sprawdzaniu wypowiedzi polityków i edukowaniu społeczeństwa w zakresie krytycznego myślenia – https://demagog.org.pl
- Fakenews.pl: Publikuje analizy i dementi fake newsów z różnych dziedzin życia, od polityki po zdrowie i technologię – https://fakenews.pl
- NASK „Weryfikuje”: Monitoruje i analizuje kampanie dezinformacyjne, wskazując trendy i zagrożenia dla bezpieczeństwa informacyjnego Polski – https://www.nask.pl/weryfikuje
- EU vs Disinfo (UE): Projekt Unii Europejskiej, który dokumentuje i obala prokremlowską dezinformację oraz publikuje analizy narracji propagandowych – https://euvsdisinfo.eu
- Disinfo Digest: Polski portal prezentujący analizy i omówienia bieżących kampanii dezinformacyjnych w kraju i za granicą – https://disinfodigest.pl

Programy weryfikujące informację

W erze mediów społecznościowych i natychmiastowego dostępu do wiadomości coraz trudniej odróżnić prawdę od fałszu. Z pomocą przychodzą programy i narzędzia do weryfikacji informacji, które pozwalają sprawdzić źródło, autentyczność i kontekst treści napotkanych w Internecie. Dzięki nim możesz upewnić się, czy dana wiadomość, zdjęcie lub film nie są manipulacją ani elementem kampanii dezinformacyjnej.

Oto niektóre z nich:

1. DomainTools Whois Lookup
   - Opis: Narzędzie pozwalające sprawdzić dane rejestracyjne domeny (np. kiedy domena została zarejestrowana, kto jest jej właścicielem, jakie są serwery DNS itp.), co pomaga ustalić, kto stoi za daną stroną internetową.
   - Link: https://whois.domaintools.com/

2. Google Lens / Google Images (wyszukiwanie obrazem)
   - Opis: Pozwala użyć zdjęcia lub obrazu jako zapytania — można znaleźć skąd pochodzi obraz, czy był używany wcześniej, porównać wersje, odkryć manipulacje graficzne.
   - Link: https://lens.google/

3. TinEye (obrazy wsteczne)
   - Opis: Wyszukiwarka obrazem wstecznym — użytkownik przesyła obraz, a TinEye próbuje znaleźć wersje tego obrazu w Internecie (również edytowane), co pomaga wykryć, czy obraz został zmanipulowany lub używany dawniej w innym kontekście.
   - Link: https://www.tineye.com/

4. InVID & WeVerify Verification Plugin

- Opis: Wtyczka do przeglądarki, która łączy narzędzia do analizy obrazów i wideo — m.in. rozbijanie filmów na klatki („keyframes”), sprawdzanie metadanych, wyszukiwanie odwrotne obrazów, analiza kontekstu zdjęć i wideo, porównywanie wersji i wykrywanie manipulacji.
- Link: https://www.invid-project.eu/tools-and-services/invid-verification-plugin/

5. NewsGuard

- Opis: Rozszerzenie przeglądarki, które ocenia wiarygodność źródeł informacji — przypisuje stronom ocenę, wyświetla ikony obok linków, oferuje tzw. „Nutrition Label” z informacjami o właścicielu, historii, transparentności, liczbie błędów itp. Niektóre funkcje są płatne.
- Link: https://www.newsguardtech.com/how-it-works/

KOMITET DO SPRAW POŻYTKU PUBLICZNEGO

Narodowy Instytut Wolności
Centrum Rozwoju Społeczeństwa Obywatelskiego

Rządowy Program Wsparcia Organizacji Pozarządowych
Moc Małych Społeczności

ESCUELA

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI – CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO W RAMACH RZĄDOWEGO PROGRAMU WSPARCIA ORGANIZACJI POZARZĄDOWYCH MOC MAŁYCH SPOŁECZNOŚCI