



WIARYGODNOŚĆ INFORMACJI W ERZE FAKE NEWS

CO TO JEST DEZINFORMACJA?

Dezinformacja to celowe szerzenie fałszywych lub wprowadzających w błąd informacji, mające na celu manipulację opinią publiczną lub wprowadzenie chaosu. Może przybierać różne formy: od zmanipulowanych zdjęć i filmów po nieprawdziwe artykuły i posty w mediach społecznościowych.

Jak sobie z nią poradzić i jakie są kluczowe umiejętności w walce z Dezinformacją w erze cyfrowej?



Po pierwsze *KRYTYCZNE MYŚLENIE*, Zadawaj pytania: Kto jest autorem? Jakie są inne źródła potwierdzające te informacje? Po drugie *UMIEJĘTNOŚĆ WERYFIKOWANIA FAKTÓW*: Korzystaj z narzędzi takich jak FactCheck.org, Snopes, aby potwierdzić prawdziwość informacji. Warto również sprawdzać daty publikacji w jakim dana informacja się pojawiła i czy na pewno jest ona aktualna. Po trzecie *ANALIZA ŹRÓDEŁ*: jest to kluczowa umiejętność, upewnij się, że źródło jest uznawane za sprawdzone i rzetelne. Po czwarte: *MECHANIZM MANIPULACJI*: bądź świadomy technik manipulacji, takich jak selektywne przedstawienie faktów



NARZĘDZIA DO WALKI

Aby skutecznie walczyć z dezinformacją, warto korzystać z kilku przydatnych narzędzi.

Narzędzia do weryfikacji obrazów, takie jak Google Reverse Image Search, pozwalają sprawdzić, czy dany obraz został użyty w różnych kontekstach lub czy jest zmanipulowany.

Wtyczki i rozszerzenia przeglądarki, takie jak NewsGuard czy Media Bias/Fact Check, pomagają ocenić wiarygodność stron internetowych i artykułów, dostarczając informacji na temat ich rzetelności.

Platformy monitorujące fake news, jak FactCheck.org czy The Poynter Institute, oferują aktualne informacje na temat rozprzestrzeniania się fałszywych wiadomości, co pozwala na bieżąco śledzić i weryfikować podejrzane treści.

Edukacja medialna jest równie istotna kursy online i warsztaty dotyczące rozpoznawania dezinformacji pomagają rozwijać umiejętności krytycznego myślenia i weryfikacji faktów, co wzmacnia zdolność do rozpoznawania i unikania fałszywych informacji.





JAK ROZPOZNAĆ ZAGROŻENIA I SIĘ IM SPRZECIWIĆ?

W dobie cyfrowej rewolucji, obok rosnącej liczby fałszywych informacji, pojawiły się również nowoczesne formy oszustw i kradzieży tożsamości, które stają się coraz bardziej powszechne.

Zrozumienie, jak rozpoznać te zagrożenia oraz jak się przed nimi chronić, jest kluczowe w utrzymaniu bezpieczeństwa osobistego i finansowego. Jakie są najnowsze oszustwa i kradzieże tożsamości, a także jak skutecznie sobie z nimi radzić?



Oszustwa BLIK i Inne Metody Wyłudzenia Pieniędzy

BLIK, system płatności mobilnych, który zdobył ogromną popularność w Polsce, jest również celem różnego rodzaju oszustw. Oszuści stosują kilka technik, aby wyłudzić pieniądze:

- **Phishing:** Oszuści mogą podszywać się pod banki lub instytucje finansowe i prosić o przestanie kodu BLIK lub danych logowania. Mogą to robić poprzez fałszywe e-maile, SMS-y lub nawet rozmowy telefoniczne.
- **Fałszywe aplikacje:** podszywanie się pod legalne aplikacje BLIK, które po zainstalowaniu mogą kraść dane użytkownika lub narażać go na inne rodzaje oszustw.



JAK SIĘ CHRONIĆ?

Nigdy nie podawaj kodu BLIK ani danych logowania przez telefon, e-mail lub SMS, banki i instytucje finansowe nigdy nie proszą o takie informacje w ten sposób.

Używaj zabezpieczeń telefonu takie jak hasła, odciski palców lub rozpoznawanie twarzy, aby utrudnić dostęp osobom trzecim.

Regularnie aktualizuj oprogramowanie i aplikacje – zapewnia to ochronę przed znanymi lukami bezpieczeństwa.

KRADZIEŻ TOŻSAMOŚCI

Kradzież tożsamości to poważne zagrożenie, które może prowadzić do finansowych i osobistych problemów. Oszuści mogą używać różnych metod, aby zdobyć dane osobowe, takie jak numery PESEL, numery kart kredytowych, czy dane kont bankowych:

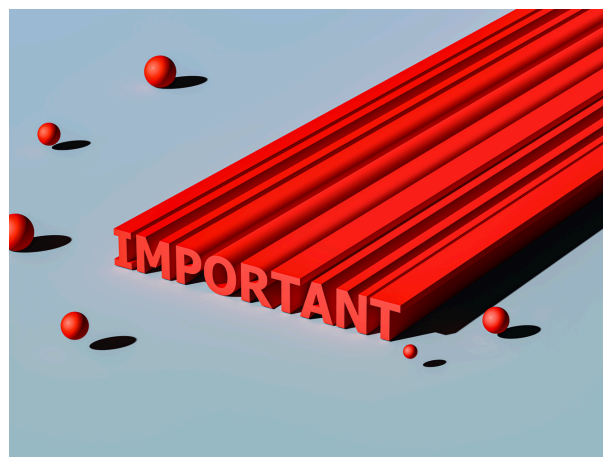
W jaki sposób dochodzi do kradzieży tożsamości? Na przykład poprzez skimming jest to technika polegająca na instalowaniu urządzeń do kopiowania danych z kart kredytowych w terminalach lub bankomatach. Następnym sposobem jest wyłudzenie informacji, poprzez rozmowy telefoniczne, przedstawiając się jako przedstawiciel bankowy

CO ROBIĆ?

Przede wszystkim unikaj podawania danych osobowych przez telefon lub e-mail, jeśli nie jesteś pewien tożsamości osoby po drugiej stronie. Regularnie sprawdzaj konto bankowe, aby szybko wykryć jakiegokolwiek nieautoryzowane transakcje lub otwarcie konta na twoje nazwisko. Używaj oprogramowania antywirusowego i dbaj o aktualizacje systemu operacyjnego. Ustaw silne hasła i zmieniaj je regularnie.

PAMIĘTAJ!

Po pierwsze edukuj siebie i innych o dezinformacji i oszustwach. Wiedza na temat najnowszych technik i narzędzi zabezpieczających może pomóc w ochronie przed fałszywymi informacjami i oszustwami. Po drugie bądź ostrożny z e-mailami i wiadomościami od nieznanых nadawców. Nie klikaj w podejrzane linki ani nie pobieraj załączników, które mogą być próbą phishingu. Po trzecie i jedno z ważniejszych - używaj silnych haseł i zabezpieczeń na swoich urządzeniach. Regularnie zmieniaj hasła i korzystaj z uwierzytelniania dwuetapowego, jeśli to możliwe.



Po czwarte sprawdzaj źródła informacji przed uwierzeniem lub udostępnieniem. Korzystaj z narzędzi do weryfikacji faktów i upewnij się, że informacje pochodzą z wiarygodnych źródeł. Piąte, NIGDY nie podawaj kodu BLIK ani danych logowania przez telefon, e-mail lub SMS. Banki nigdy nie proszą o takie informacje w ten sposób. Ostatnim punktem, ale nie najmniej ważnym jest Instalowanie i aktualizowanie oprogramowania antywirusowego, aby chronić swoje urządzenia przed zagrożeniami i złośliwym oprogramowaniem.



PODZIEL SIĘ WIEDZĄ!

Zachęcamy Cię do podzielenia się tym artykułem z rodziną, przyjaciółmi i współpracownikami. Dezinformacja to poważne zagrożenie, które może wpływać na każdego z nas, a wspólna edukacja to klucz do budowania bardziej świadomego społeczeństwa.

Artykuł ten został napisany na podstawie naszych własnych doświadczeń oraz aktywnego udziału w mobilnościach projektu „Wiarygodność Informacji w Erze Fake News” Sfinansowanego ze środków UE . Dzięki zdobytej wiedzy i praktyce, mamy nadzieję dostarczyć Ci narzędzi i wskazówek, które pomogą w rozpoznawaniu i zwalczaniu fałszywych informacji.



Podziel się tym artykułem, aby pomóc innym zrozumieć zagrożenia związane z dezinformacją i nauczyć ich, jak skutecznie się przed nimi chronić. Razem możemy stworzyć bardziej odporną na fałszywe informacje społeczność!