KWIECIEŃ 2026 | NR 1

2B SAFE

TWÓJ PRZEWODNIK PO CYFROWYM ŚWIECIE

OFICJALNA PUBLIKACJA UCZNIÓW XIII LICEUM OGÓLNOKSZTAŁCĄCEGO W RADOMIU
Z ZAKRESU CYBERBEZPIECZEŃASTWA, NOWYCH TECHNOLOGII I SPOŁECZNOŚCI
W INTERNECIE.

Cyberbezpieczeństwo to klucz do bezpiecznego korzystania z Internetu i ochrony naszych danych każdego dnia.

Jeśli doświadczasz cyberprzemocy lub widzisz ją w swoim otoczeniu – nie milcz. Szukaj pomocy u dorosłych lub zadzwoń pod bezpłatny numer 116 111 - Telefon Zaufania dla Dzieci i Młodzieży

ŹRÓDŁO:GOOGLE

ŹRÓDŁO:GOOGLE

TRAGICZNA HISTORIA MEGAN MEIER – GDY CYBERPRZEMOC PROWADZI DO TRAGEDII

AUTOR: JULITA MIELNICZUK || ŹRÓDŁO: TVN

W dzisiejszych czasach Internet jest ważną częścią życia młodych ludzi. Umożliwia komunikację i poznawanie nowych osób, ale niestety może być także miejscem cyberprzemocy. Jednym z najbardziej tragicznych przykładów jej skutków jest historia Megan Meier.

Megan była trzynastoletnią dziewczyną z Missouri w Stanach Zjednoczonych. W 2006 roku poznała w Internecie chłopaka o imieniu „Josh Evans" na portalu MySpace. Na początku ich rozmowy były miłe, a chłopak szybko zdobył jej zaufanie.

Po pewnym czasie „Josh" zaczął wysyłać Megan obraźliwe wiadomości. W jednej z nich napisał, że „świat byłby lepszym miejscem bez niej". Dziewczyna bardzo to przeżyła i niedługo potem odebrała sobie życie.

Później okazało się, że „Josh Evans" był fałszywym profilem stworzonym przez dorosłą sąsiadkę Megan, Lori Drew. Historia ta wstrząsnęła opinią publiczną i zwróciła uwagę na poważny problem cyberprzemocy. Pokazuje ona, **jak bardzo słowa w Internecie mogą ranić i jak ważne jest okazywanie szacunku innym w sieci.**

FAŁSZYWE ZBIÓRKI NA CHORE DZIECI – OSZUŚCI WYŁUDZILI MILIONY

AUTOR:VIKTORIA ROMANENKO ||ŹRÓDŁO:ONET

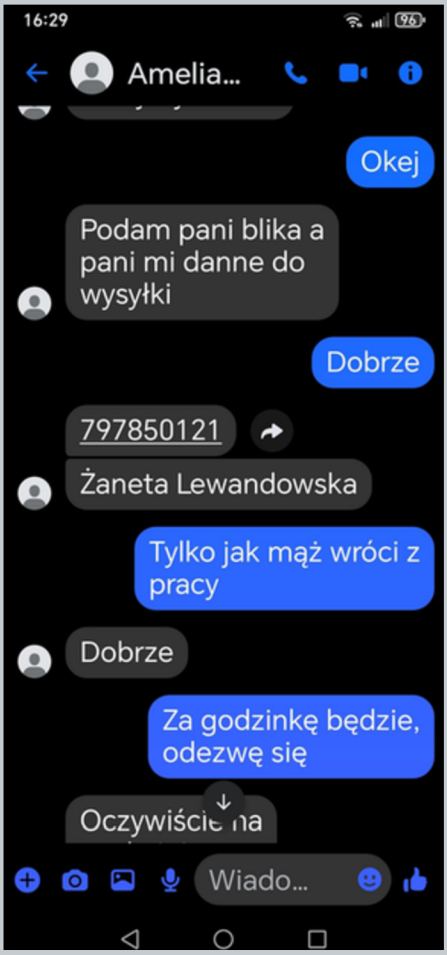
Policja rozbiła grupę przestępczą, która przez kilka lat zbierała pieniądze na rzekome leczenie chorych dzieci. Zbiórki okazały się fałszywe, a większość pieniędzy nigdy nie trafiała do potrzebujących.

Przestępcy **wykorzystywali emocjonalne historie oraz zdjęcia chorych dzieci, aby wzbudzić współczucie i zachęcić ludzi do wpłat**. W niektórych przypadkach posługiwali się nawet wizerunkiem dziecka, które już zmarło, aby ich działania wyglądały bardziej wiarygodnie. Grupa działała od 2016 roku i w tym czasie zebrała prawie 15 milionów złotych od darczyńców, jednak na rzeczywistą pomoc przeznaczono tylko niewielką część tej kwoty.

W sprawie zatrzymano kilka osób podejrzanych o udział w zorganizowanej grupie przestępczej, pranie pieniędzy oraz oszustwa. Podejrzanym grozi nawet do 12 lat więzienia.

Ta sytuacja pokazuje, jak ważne jest sprawdzanie wiarygodności zbiórek charytatywnych przed przekazaniem pieniędzy.

ŹRÓDŁO:CHAT GPT



ŹRÓDŁO: FACEBOOK

UWAGA NA OSZUSTWO „METODĄ NA BLIK"!

AUTOR: DAWID PAWELEC || ŹRÓDŁO: HREJTERZY

Coraz częściej dochodzi do oszustw internetowych związanych z płatnościami BLIK. Przestępcy podszywają się pod naszych znajomych i próbują wyłudzić pieniądze. Oszust przejmuje konto na portalu społecznościowym i pisze do znajomych tej osoby, udając ją, a następnie prosi o pilną pomoc finansową i przesłanie kodu BLIK. Gdy ktoś wyśle kod i zatwierdzi transakcję w aplikacji bankowej, przestępca wypłaca pieniądze z bankomatu, a niestety takie środki bardzo trudno odzyskać. Najczęstsze wiadomości od oszustów to na przykład: „Hej, możesz mi szybko wysłać BLIK? Oddam wieczorem.", „Brakuje mi 100 zł, pomożesz?", „Jestem w sklepie i nie działa mi karta." czy „Muszę pilnie zapłacić za zamówienie." Aby się chronić, zawsze zadzwoń do znajomego i upewnij się, że to naprawdę on, nie wysyłaj kodu BLIK przez komunikatory bez pewności, dokładnie sprawdzaj, co potwierdzasz w aplikacji bankowej oraz chroń swoje konta, używając silnych haseł i logowania dwustopniowego.

Pamiętaj, że kod BLIK działa jak gotówka – jeśli go podasz, możesz stracić swoje pieniądze, dlatego zachowaj czujność i nie daj się oszukać.

Jeśli otrzymasz prośbę o BLIK-a z nieznanego numeru lub podejrzewasz, że mogło dojść do próby oszustwa, niezwłocznie skontaktuj się ze swoim bankiem. Pracownicy infolinii pomogą Ci zabezpieczyć konto i podpowiedzą, jakie kroki podjąć dalej.

OSZUSTWO TELEFONICZNE Z UŻYCIEM AI – NOWA METODA CYBERPRZESTĘPCÓW

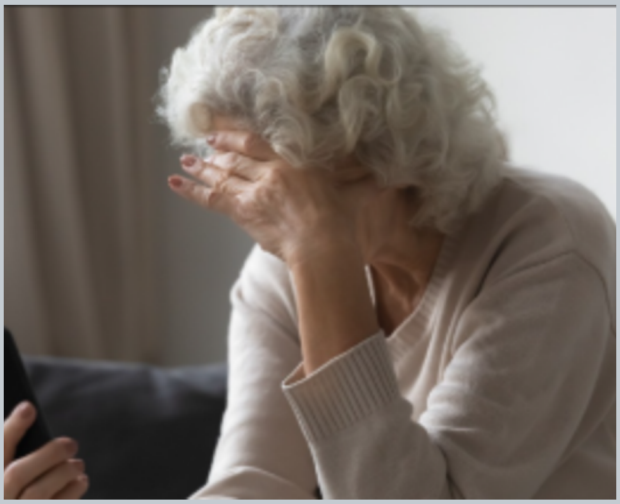
AUTOR:BARBARA ZWIERZCHOWSKA || ŹRÓDŁO: ONET

Cyberprzestępcy coraz skuteczniej wykorzystują technologię klonowania głosu przez AI, aby wyłudzać pieniądze metodą na bliską osobę w potrzebie.

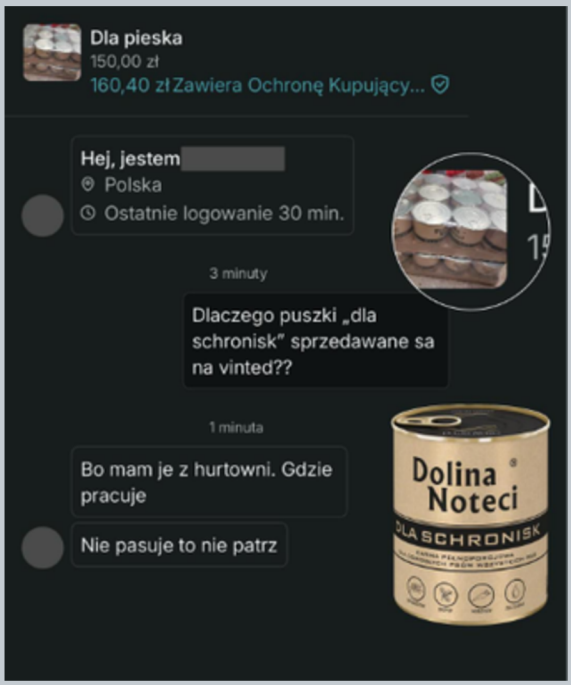
Cały proceder zaczyna się od zdobycia krótkiej próbki głosu, którą oszuści kradną z filmów w mediach społecznościowych lub nagrań z rozmów telefonicznych, a następnie przy pomocy sztucznej inteligencji tworzą niemal identyczną kopię barwy głosu i sposobu mówienia ofiary.

Uzbrojony w taki klon przestępca dzwoni do członka rodziny, udając dziecko lub wnuka, który rzekomo spowodował wypadek lub ma poważne problemy z prawem, i pod ogromną presją czasu błaga o szybki przelew lub podanie kodów do płatności. Ponieważ głos brzmi niezwykle wiarygodnie i jest przepełniony emocjami, takimi jak płacz czy panika, ofiara często działa instynktownie i traci czujność, wierząc, że naprawdę ratuje bliską osobę.

Najlepszą obroną przed tym zagrożeniem jest natychmiastowe rozłączenie się i samodzielne oddzwonienie na znany nam numer telefonu tej osoby, a także ustalenie z rodziną unikalnego hasła bezpieczeństwa, które pozwoli w kilka sekund zweryfikować tożsamość rozmówcy i uniknąć utraty oszczędności.



ŹRÓDŁO: ONET



ŹRÓDŁO:INSTAGRAM

KARMA DLA SCHRONISK SPRZEDAWANA W INTERNECIE

AUTOR: NATALIA FERT || ŹRÓDŁO: INSTAGRAM

Firma Dolina Noteci poinformowała o niepokojącej sytuacji związanej z pomocą dla zwierząt. Co roku przekazuje ona duże ilości karmy do schronisk i fundacji, aby wspierać bezdomne psy i koty.

Karma ta jest dawana za darmo i specjalnie oznaczona napisem „dla schronisk". Niestety okazało się, że ktoś wystawił takie puszki na sprzedaż w internecie, m.in. na platformie Vinted.

Firma podkreśla, że taka karma powinna trafiać wyłącznie do potrzebujących zwierząt, a nie być sprzedawana. W tej sytuacji pomoc przeznaczona dla schronisk została odebrana psom, które jej potrzebują.

Producent poprosił internautów, aby zgłaszali takie oferty sprzedaży. Dzięki temu można sprawdzić, skąd pochodzi karma i zapobiec podobnym sytuacjom w przyszłości.

KAMERY W DOMU

AUTOR: MAGDA WIROWSKA || ŹRÓDŁO: GOOGLE

Coraz więcej osób instaluje w swoich domach kamery, na przykład do monitorowania mieszkania, dzieci lub zwierząt. Urządzenia te mają zwiększać poczucie bezpieczeństwa, jednak jeśli nie są odpowiednio zabezpieczone, mogą stać się celem cyberprzestępców.

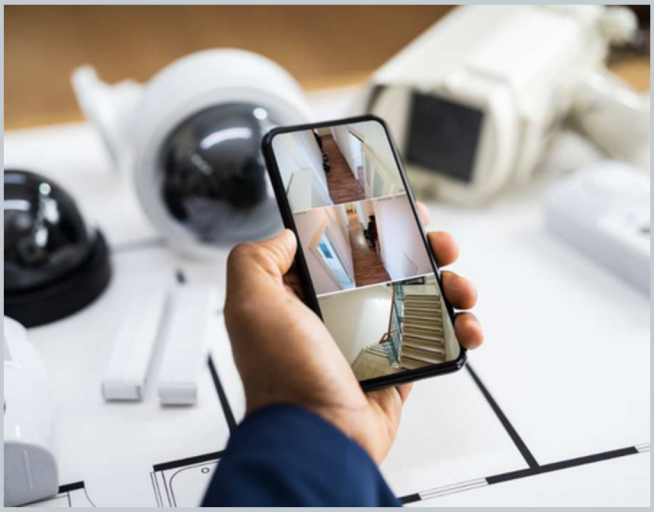
Zagrożenie polega na tym, że hakerzy potrafią przejmować dostęp do kamer IP i oglądać obraz z prywatnych mieszkań. W Internecie można znaleźć nawet oferty sprzedaży dostępu do takich przejętych kamer, a nagrania z nich bywają publikowane w sieci. W efekcie osoby niepowołane mogą podglądać codzienne życie domowników, co stanowi poważne naruszenie prywatności.

Do takich sytuacji najczęściej dochodzi z powodu błędów użytkowników. Wiele osób nie zmienia fabrycznych haseł, stosuje proste zabezpieczenia lub nie aktualizuje oprogramowania urządzeń. To sprawia, że cyberprzestępcy mogą stosunkowo łatwo uzyskać dostęp do kamer i innych urządzeń typu smart w domu.

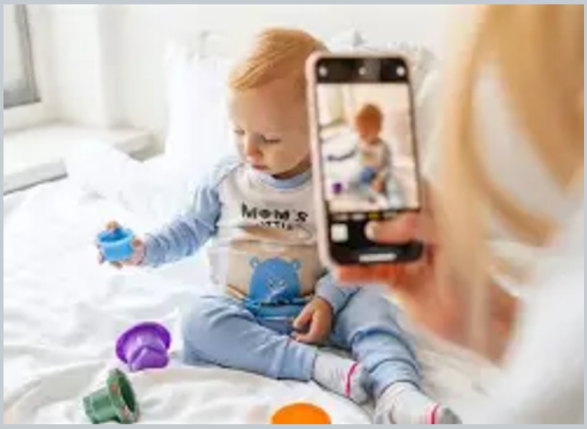
Przejęcie kamery może prowadzić do poważnych konsekwencji, takich jak naruszenie prywatności, możliwość obserwowania codziennego życia domowników oraz publikowanie lub sprzedaż nagrań w internecie.

Aby się przed tym chronić, należy stosować podstawowe zasady bezpieczeństwa cyfrowego. Warto ustawiać silne i unikalne hasła, regularnie aktualizować oprogramowanie oraz kontrolować, kto ma dostęp do urządzeń.

Kamery mogą poprawić bezpieczeństwo domu, ale tylko wtedy, gdy są odpowiednio zabezpieczone. Brak podstawowych zasad cyberbezpieczeństwa może sprawić, że zamiast chronić, staną się narzędziem do naruszania prywatności domowników.



ŹRÓDŁO: GOOGLE



ŹRÓDŁO:GOOGLE

SHARENTING – CZY TO W PORZĄDKU?

AUTOR: LENA DUDEK || ŹRÓDŁO:FACEBOOK

Czy dzieci mogą brać świadomie udział w social mediach rodziców? Gdzie wyznaczymy barierę wiekową świadomej zgody? A może w relacji rodzic-dziecko, nie ma miejsca na w pełni dobrowolną zgodę, bo każde dziecko chce zadowolić rodziców? Czy dziecko może ocenić, co to znaczy 100, 1000, 100 tysięcy wyświetleń? Czy to moralne zarabiać na wizerunku dziecka? Jedno zdjęcie nie czyni sharentingu, ale czy relacjonowanie codziennego życia nie odziera dziecka z prywatności?

Cyfrowy ślad zostaje na zawsze. Niedługo luksusem będzie, kiedy wchodząc w dorosłość ktoś będzie miał "czystą kartę" w sieci.

Bardzo chciałabym prawnego uregulowania kwestii zarabiania na sharentingu - myślę, że gdyby nie szły za tym pieniądze, a konta opierające się na wiezunku dzieci były postrzegane przez firmy jako "ryzykowne", to również mniej rodziców by się na to decydowało.

OSZUSTWA NA OLX - JAK SIĘ CHRONIĆ

AUTOR: LENA DUDEK || ŹRÓDŁO: OSZUSTWA.INFO

Oszustwa na OLX polegają najczęściej na podszywaniu się pod kupujących lub serwis i wyłudzaniu danych oraz pieniędzy. Przestępcy kontaktują się przez SMS, e-mail lub komunikatory i wysyłają fałszywe linki do stron przypominających OLX. Następnie próbują nakłonić ofiarę do podania danych karty, kodów SMS lub danych logowania, tłumacząc, że jest to potrzebne do odebrania płatności.

Popularnym sposobem jest także wysyłanie fałszywych potwierdzeń przelewu, aby sprzedający uwierzył, że pieniądze zostały wysłane i jak najszybciej nadał paczkę. W rzeczywistości przelew nie istnieje, a sprzedający traci zarówno towar, jak i pieniądze.

Aby uniknąć oszustwa, należy pamiętać, że OLX nie wymaga podawania danych karty do otrzymania pieniędzy, nie klikać w podejrzane linki oraz zawsze sprawdzać faktyczny wpływ środków na konto bankowe. Ważne jest też, aby nie działać pod presją czasu i zachować ostrożność przy każdej transakcji.

ŹRÓDŁO: OSZUSTWO.INFO

PROBLEM NIELEGALNYCH TREŚCI W INTERNECIE

AUTOR: DAGMARA MAZUR-POSUNIAK || ŹRÓDŁO: BBC

Współczesny Internet daje ogromne możliwości komunikacji i zdobywania informacji, jednak wiąże się również z poważnymi zagrożeniami. Jednym z nich jest rozpowszechnianie nielegalnych i szkodliwych materiałów, które mogą krzywdzić innych ludzi.

Według śledztwa przeprowadzonego przez BBC News, osoby, które doświadczyły przemocy w dzieciństwie, wciąż zmagają się z faktem, że materiały związane z ich krzywdą mogą nadal krążyć w sieci. Jedna z ofiar zwróciła się do Elon Musk, właściciela platformy X, z prośbą o skuteczniejsze działania w celu usuwania takich treści.

Platformy społecznościowe deklarują, że walka z nielegalnymi materiałami jest ich priorytetem i podkreślają, że stosują zasadę „zerowej tolerancji". Mimo to problem nadal istnieje, a tego typu treści mogą być rozpowszechniane i sprzedawane w różnych częściach świata.

Eksperci zwracają uwagę, że takie działania nie tylko łamią prawo, ale także powodują dalsze cierpienie osób pokrzywdzonych. **Dlatego tak ważne jest odpowiedzialne korzystanie z internetu, zgłaszanie niebezpiecznych treści oraz wspólne dbanie o bezpieczeństwo w sieci.**

ŹRÓDŁO: BBC

Imię : _____

OVERSHERING

Wykreśl słowa związane z oversheringiem

I	S	Ź	B	F	L	Ć	P	D	X	T	Ą
H	Ż	L	E	Ę	Ł	Q	W	Q	A	X	Ż
A	R	M	Z	Q	Ś	Ę	W	O	L	N	Ę
Y	Ó	R	P	Q	Ą	B	D	Q	Ć	Z	E
Ą	Ś	G	I	Ó	F	S	Z	V	B	N	Z
F	R	C	E	R	P	Z	I	Z	H	P	Ż
O	N	D	C	Z	U	C	E	R	Q	R	H
Ć	F	R	Z	I	B	Z	C	T	K	O	Ś
D	J	Ź	E	Q	L	E	I	X	V	B	Ł
X	I	Ę	Ń	O	I	G	Ń	Ń	B	L	K
T	H	J	S	Ź	C	Ó	S	K	Ę	E	Ą
Ń	L	G	T	J	Z	Ł	T	Ś	D	M	L
H	V	C	W	X	N	Y	W	E	H	Y	Q
Y	Ó	M	O	Ż	E	Z	O	D	T	H	E

_____ _____ _____

_____ _____ _____

Overshering to nadmierne dzielenie się prywatnymi informacjami (np. o sobie, swoich emocjach czy życiu) w sytuacjach, gdzie nie jest to odpowiednie lub potrzebne, np. w internecie albo wobec obcych osób.

FILTRY AI „BEAUTY STANDARD"
W SOCIAL MEDIACH

Pułapka Perfekcji

TO, CO WIDZISZ NA INSTAGRAMIE,
CZĘSTO NIE JEST RZECZYWISTOŚCIĄ

1.Nie porównuj się do filtra.
2.Perfekcja z internetu często nie istnieje.
3.Bądź sobą, nie algorytmem.

Czy wiesz, że do 13. roku życia przeciętne dziecko "vlogujących" rodziców ma w sieci tysiące zdjęć i godzin nagrań, na które nigdy NIE WYRAZIŁO ZGODY?

- **UTRACONA PRYWATNOŚĆ:** DOMOWE PIELESZE STAJĄ SIĘ PLANEM ZDJĘCIOWYM.
- **CYFROWY ŚLAD:** CZY TWOJE DZIECKO PODZIĘKUJE CI ZA TEN FILM ZA 10 LAT?
- **BRAK GRANIC:** GDZIE KOŃCZY SIĘ MIŁOŚĆ, A ZACZYNA WALKA O ZASIĘGI?

MOJE ŻYCIE TO NIE TWÓJ CONTENT.

CATFISH ALERT

SPRAWDŹ ZANIM UWIERZYSZ W INTERNETOWĄ MIŁOŚĆ

Love scamming to oszustwo, w któym fałszywe profile budują relacje emocjonalne, by wyłudzić pieniądze. Catfishing to jego forma- manipulacja uczuciami i ożsamością. Pamiętaj nigdy nie daj się osobie którą znas tylko online i weryfikuj informacje,

DIGITAL KIDNAPPING

Twoje dziecko jest celem. Chroń jego prywatność w sieci.

To kradzież zdjęć dziecka z internetu (np. z Facebooka, Instagrama, TikToka) **i wykorzystywanie ich przez obce osoby bez zgody rodziców.**

Oszuści:

- **tworzą fałszywe profile,**
- **podszywają się pod rodziców,**
- **publikują zdjęcia jako „swoje dziecko",**
- **używają zdjęć do oszustw lub manipulacji.**

PAMIĘTAJ

- Nie udostępniaj zdjęć osób bez ich zgody
- Ustaw profil jako prywatny
- Ogranicz widoczność zdjęć tylko dla znajomych
- Nie ufaj nieznanym osobom
- Uważaj na zdjęcia w stroju kąpielowym lub bieliźnie
- Regularnie sprawdzaj, kto obserwuje Twoje konto

PRACE UCZNIÓW KLAS TRZECICH

NAJWAŻNIEJSZE NUMERY

Gov.pl

ZGŁOŚ PRZESTĘPSTWO

Cert.pl

ZGŁOŚ PRZESTĘPSTWO

112 – numer alarmowy

800 120 002 – Niebieska Linia

116 111 – telefon zaufania dla dzieci i młodzieży

800 12 12 12 – telefon Rzecznika Praw Dziecka

800 112 800 –telefon dla ofiar przemocy

Redaktor naczelny: Giulia Piaseczny
Zastępca redaktora: Wiktoria Błaszczyk
Zespół redakcyjny: Alina Aleksienko, Marlena Bujak, Lena Dudek, Natalia Fert, Patrycja Frączek, Dawid Leszczyk, Jakub Maciejewski, Julita Mielniczuk, Marceli Mizera, Dawid Pawelec, Victoriia Romanenko, Magda Wirowska, Barbara Zwierzchowska
Opiekun merytoryczny: Dagmara Mazur-Posuniak
Skład i łamanie: Lena Czajka, Dagmara Mazur-Posuniak
Dane kontaktowe: 2besafe@13liceum.eu