

WAKACJE ZE SMARTFONEM

PORADNIK DLA RODZICÓW



An abstract painting with vibrant, expressive brushstrokes in shades of teal, blue, orange, and pink. In the center, a hand holds a black smartphone, which displays a dark, abstract image. The overall composition is dynamic and artistic, with the text overlaid on the right side.

WSTĘP

Wakacje to czas odpoczynku, przygód i wspólnych chwil – zarówno offline, jak i online. W dzisiejszym świecie trudno sobie wyobrazić wyjazd bez smartfona, zdjęć z podróży wrzucanych na Instagram, ulubionych filmików na YouTube czy krótkich relacji na TikToku. Dla dzieci i młodzieży internet to nie tylko rozrywka, ale też sposób na kontakt z rówieśnikami i wyrażanie siebie. Dla rodziców – często źródło obaw o bezpieczeństwo. Choć cyfrowy świat ułatwia życie i uprzyjemnia wypoczynek, niesie też pewne zagrożenia, o których warto pamiętać.

Zachęcamy do lektury poradnika wakacyjnego, który powstał właśnie z myślą o rodzicach i dzieciach, po to, by pomóc bezpiecznie korzystać z technologii podczas wakacyjnych wyjazdów.

Podpowiemy, jak rozmawiać z dziećmi o odpowiedzialnym korzystaniu z mediów społecznościowych, jak zadbać o ochronę danych osobowych i nie stać się łatwym celem dla cyberprzestępców. Wyjaśnimy, jakie aplikacje warto mieć w telefonie, jakie ustawienia mogą się przydać w podróży i co zrobić w przypadku kradzieży urządzenia za granicą. Zajmiemy się również tematem kontroli rodzicielskiej – jak ją ustawić, by zapewnić dzieciom bezpieczeństwo online, nie odbierając im przy tym swobody. Na koniec podpowiemy, jak dzielić się wakacyjnymi wspomnieniami w sieci, zachowując przy tym prywatność i rozsądek.

Wierzimy, że świadome podejście do cyfrowych narzędzi sprawi, że wakacje będą nie tylko udane, ale i bezpieczne – zarówno dla dzieci, jak i dorosłych.

JAK ZADBAĆ O CYFROWY BALANS I BEZPIECZEŃSTWO DZIECKA?

Wakacje to upragniony czas relaksu, odpoczynku i przygód - ale też okres, gdy dzieci spędzają więcej czasu online. Dobrze przeczytaliście:) Więcej wolnego, to więcej gier, filmików na YouTube, TikToku i kontaktów z rówieśnikami przez internet.

Dla dziecka to codzienność. Dla rodzica - wyzwanie. Jak zachować cyfrowy balans, zadbać o bezpieczeństwo online, a przy tym nie popsuć relacji zakazami i podejrzliwością?

1. Zadbajcie wspólnie o cyfrową równowagę

Wprowadź rytuały offline

Wspólne śniadanie bez telefonów, wieczorna gra planszowa, wyprawa w góry bez powiadomień. To nie musi być całodniowy „detoks cyfrowy”. Wystarczy kilka zasad dotyczących korzystania z telefonu i zaplanowanie stałych momentów offline, by dziecko nie czuło, że „ciągle coś traci”. Można się umówić, że po wspólnym wyjściu na plażę czy zwiedzaniu, będzie godzina na ulubione gry i aplikacje. Dzieci lepiej reagują na jasne zasady niż na zakazy bez uzasadnienia.

Wakacyjny dziennik zamiast relacji na żywo

Zachęć dziecko do dokumentowania wakacji w zeszycie lub albumie. Rysunki, zdjęcia z aparatu natychmiastowego, zasuszone liście czy bilety z podróży -





to nie tylko świetna pamiątka, ale i alternatywa dla ciągłego publikowania w internecie.

Bądź wzorem

Jeśli sam przeglądasz telefon przy stole, Twoje prośby o odkładanie ekranów nie będą wiarygodne. Cyfrowa równowaga zaczyna się od dorosłych. Ustalcie partnerskie zasady korzystania z urządzeń elektronicznych podczas wakacji i bądźcie konsekwentni.

2. TikTok i YouTube – bezpieczne publikowanie i oglądanie

Rozmawiaj, nie oceniaj

Zamiast „znów tylko TikTok?!”, zapytaj: „Co ostatnio oglądałeś ciekawego?”, „Który filmik Cię rozbawił?”. Zamiast zamykać temat, otwórz przestrzeń do rozmowy, to dobre sposoby, by rozpocząć rozmowę bez oceniania. Dzięki temu dziecko poczuje, że nie chcesz go kontrolować, ale jesteś ciekawy jego świata.

Wyjaśnij, czym jest hejt i jak na niego reagować

Wakacyjne publikacje często są bardziej swobodne, radosne, ale to nie oznacza, że dzieci są chronione przed hejtem. Powiedz dziecku, że może spotkać się z nieprzyjemnymi komentarzami – i to niekoniecznie dlatego, że zrobiło coś złe. Naucz je, że warto ignorować hejterów, blokować nieprzyjaznych użytkowników i zgłaszać nieodpowiednie treści. Przypomnij, że zawsze może się do Ciebie zwrócić – bez obawy, że „będzie miało kłopoty”.

Co publikować, a czego unikać?

Pomóż dziecku zrozumieć, że publikowanie lokalizacji, zdjęć w stroju kąpielowym czy filmików z pokoju hotelowego to ryzyko utraty prywatności. Nawet „zabawa w nagrywanie” może prowadzić do problemów. Wspólnie ustalcie granice – np. że nie wrzucamy filmików z lokalizacją domku letniskowego, z informacją o tym, że cała rodzina jest na wyjeździe. Przypomnij, że raz wrzucone treści mogą zostać w sieci na zawsze, nawet jeśli je usunie.

Zasada: „Najpierw pokaż, potem wrzucaj” - w szczególności u młodszych dzieci.

Porozmawiajcie o trendach i wyzwaniach

Niektóry wakacyjny „challenge” lub trend na TikToku może być ryzykowny - np. zachęcać do skakania z wysokości do wody, uciekania przed ochroniarzem w miejscu publicznym czy przesadnego obnażania się. Zainteresuj się, co jest teraz popularne wśród młodszych użytkowników i porozmawiaj o konsekwencjach - fizycznych, prawnych, psychicznych. Nie oceniaj - pytaj: „A co Ty o tym myślisz?”, „Czy uważasz, że to bezpieczne?”.

Zadbajcie wspólnie o ustawienia prywatności

W wakacyjnym pośpiechu dzieci mogą wrzucać filmy bez sprawdzania, czy konto jest prywatne, czy lokalizacja jest ukryta, albo kto może komentować ich treści. Warto raz na jakiś czas wspólnie przejrzeć ustawienia konta:

- Kto może zobaczyć profil
- Kto może komentować
- Czy lokalizacja jest włączona
- Czy historia oglądania jest chroniona





Dzieci często nie mają świadomości, że np. dodanie tagu z nazwą hotelu zdradza ich aktualną lokalizację.

Ustalcie zasady nagrywania innych osób

Wakacyjne filmiki często pokazują innych – znajomych z kolonii, przypadkowych turystów, a nawet obsługę hotelową. Wytłumacz dziecku, że nie każdy chce być nagrywany, że prawo do prywatności dotyczy każdego. Zachęć, by przed publikacją filmów z innymi osobami dziecko pytało o zgodę, szczególnie jeśli są to dzieci lub osoby niepełnoletnie.

- Naucz zasad prywatności i reagowania
- Kto może komentować i oglądać
- Jak zgłaszać nieodpowiednie treści
- Kiedy zablokować użytkownika
- Dlaczego nie wolno odpowiadać obcym

To wszystko można omówić spokojnie, zanim wydarzy się coś trudnego.

3. Gry online i internetowi „znajomi z wakacji”

Gry są super – ale z umiarem

Wakacje to czas, gdy dzieci grają więcej. To naturalne. Ale warto ustalić czas grania i miejsce (np. nie w czasie posiłków, nie do późnej nocy). Zainteresuj się, w co dziecko gra – może to być okazja do wspólnej zabawy albo poznania jego świata.

Uwaga na „nowych kolegów z sieci”

W wielu grach dzieci spotykają rówieśników – ale i nieznajomych dorosłych, którzy udają dzieci. Porozmawiajcie o zasadzie:

„Nie podaję dokładnego imienia, wieku, szkoły, numeru telefonu ani miejsca pobytu”

Ustalcie, że jeśli ktoś proponuje spotkanie, przesyła dziwne wiadomości, prosi o zdjęcia – dziecko zawsze **ma** powiedzieć o tym rodzicom. Nawet, jeśli boi się, że „zrobiło coś nie tak”.

Zasada 3P w kontaktach online: **Pytaj – Pokaż – Powiedz**

- Pytaj, jeśli nie wiesz, kto to.
- Pokaż rodzicowi lub opiekunowi.
- Powiedz, jeśli coś Cię zaniepokoiło.

Zaufanie + zasady = bezpieczne wakacje online

Nie musisz znać wszystkich trendów z TikToka ani przechodzić każdej gry. Wystarczy, że będziesz obecny, zainteresowany i otwarty na rozmowę.

- Zamiast kontrolować – rozmawiaj.
- Zamiast zakazywać – ustal zasady.
- Zamiast oceniać – ucz mądrej obecności w sieci.

Wakacje to idealny czas, by dziecko nauczyło się świadomie korzystać z technologii. A Ty możesz być w tym jego najlepszym przewodnikiem.



An artistic illustration of two children, a girl and a boy, looking at a smartphone together. The background is a vibrant, abstract composition of brushstrokes in shades of blue, orange, and white. The children are positioned in the foreground, with the girl on the left and the boy on the right. The smartphone is held in the center, displaying a landscape image. The overall mood is creative and digital.

PORADY UKE

1. Ustal stałe momenty bez ekranów, np. podczas posiłków czy wspólnych wyjść.
2. Pytaj dziecko z ciekawością o to, co ogląda, zamiast je oceniać.
3. Ustal, że młodsze dzieci pokazują Ci treści przed ich publikacją w internecie.
4. Naucz dziecko, by nie publikowało lokalizacji ani szczegółów dotyczących wyjazdu.
5. Powiedz dziecku, że ma prawo blokować i zgłaszać nieodpowiednie treści oraz zawsze może zwrócić się do Ciebie.
6. Zainteresuj się grami dziecka i sprawdź, z kim gra i rozmawia.
7. Wytłumacz, że nie powinno podawać nieznajomym swojego imienia, wieku czy miejsca pobytu.
8. Uzgodnij dzienny limit czasu online i przypominajcie sobie nawzajem o przerwach.
9. Pokaż dziecku dobry przykład, sam odkładając telefon w ważnych chwilach.
10. Stwórz z dzieckiem prosty kodeks cyfrowy, który określa zasady korzystania z internetu w wakacje.



WAKACJE BEZ RYZYKA – CHROŃ SWOJE DANE

Wakacje to czas odpoczynku i oderwania od codziennych obowiązków, ale także moment, w którym tracimy czujność – również w kwestii bezpieczeństwa cyfrowego. Nie tylko na dzieci czyhają zagrożenia, na Ciebie też. Korzystanie z internetu w podróży, udostępnianie zdjęć czy rezerwacje przez aplikacje niesie ze sobą ryzyko. Cyberprzestępcy doskonale wiedzą, że urlop to idealna okazja, by wykorzystać naszą nieostrożność. Dlatego warto pamiętać o kilku podstawowych zasadach, które pomogą zabezpieczyć dane osobowe i uniknąć przykrych niespodzianek.

Zagrożenia zaczynają się już na etapie rezerwacji wakacji. Korzystanie z niezweryfikowanych stron internetowych może prowadzić do wyłudzenia danych karty płatniczej lub danych osobowych. Przed zrobieniem rezerwacji sprawdź adres domeny, wiarygodność serwisu, opinie innych użytkowników.

Kolejne ryzyko to korzystanie z otwartych sieci Wi-Fi na lotniskach, w hotelach, czy kawiarniach. Choć są wygodne i pozwolą zaoszczędzić GB, to cyberprzestępcy mogą tworzyć fałszywe punkty dostępowe Wi-Fi. Takie hotspoty umożliwiają przechwycenie części danych przesyłanych przez użytkowników. W takich warunkach najlepiej, aby dziecko unikało logowania się do bankowości internetowej, poczty czy innych serwisów wymagających podania hasła. Jeśli już musi skorzystać z publicznej sieci, warto użyć VPN, który szyfruje przesyłane dane i utrudnia ich przechwycenie.

Nadmierne i nieostrożne publikowanie w mediach społecznościowych nie dotyczy tylko dzieci. Publikowanie informacji o tym, że jesteś poza domem to zaproszenie dla złodziei nie tylko cyfrowych, ale i tych okradających fizycznie.

Nie publikuj zdjęć, na których są:

- dane osobowe,
- dokumenty rejestracyjne samochodu,
- karty pokładowe,
- adresy,
- numery pokoi hotelowych.

Z pozoru niewinne szczegóły mogą zostać wykorzystane do przestępstwa lub nieprzyjemnego żartu.

Podczas wyjazdu wiele osób korzysta z nawigacji, zakupów czy rezerwacji usług. Zanim zainstalujesz nową aplikację sprawdź, kto ją stworzył i jakie ma opinie w sklepie z aplikacjami. Nie zezwalaj aplikacjom na dostęp do kontaktów, zdjęć czy lokalizacji, jeśli nie są one niezbędne do działania aplikacji.

- Instaluj aplikacje tylko z legalnych, oficjalnych sklepów.

Pamiętaj o zabezpieczeniu samego urządzenia.

Po powrocie z wakacji sprawdź aktywność na kontach bankowych i portalach społecznościowych. Nawet jeśli podczas wyjazdu wszystko przebiegało bez zakłóceń, upewnij się, że nikt nie wykorzystał Twojej nieobecności do przejęcia kontroli nad danymi czy finansami.

Bezpieczne wakacje to nie tylko kwestia zamknięcia domu i spakowania apteczki. To także troska o dane osobowe, które są równie cenne jak portfel czy paszport.

PORADY UKE:

1. Unikajcie publicznych sieci Wi-Fi bez VPN – szczególnie do logowania się do banków, maili czy portali społecznościowych.
2. Nie publikujcie zdjęć ujawniających dane osobowe – np. kart pokładowych, numerów pokoi czy lokalizacji w czasie rzeczywistym.
3. Instalujcie aplikacje tylko z oficjalnych źródeł – zawsze sprawdzajcie uprawnienia aplikacji i opinie w sklepie.



CYFROWY NIEZBĘDNIK PODRÓŻNIKA – APLIKACJE I USTAWIENIA, KTÓRE WARTO ZNAĆ

Dzięki odpowiednim aplikacjom i ustawieniom nasze urządzenia mobilne mogą zastąpić przewodniki, mapy, słowniki, a nawet lokalnych przewoźników. Dla wielu rodziców „odpoczynek” z dzieckiem to przygoda pełna emocji, ale też wyzwań.

Jedną z najważniejszych kwestii podczas wyjazdu jest planowanie trasy i punktów postoju. Mapy online takie jak Google, Waze, Apple Maps, OpenStreetMap itp. pozwalają dziś nie tylko znaleźć drogę do hotelu, ale też podpowiedzą, gdzie znajdują się place zabaw, toalety publiczne czy przyjazne rodzinom restauracje.

- Przed wyjazdem pobierz mapę wybranego obszaru, by w razie braku zasięgu mieć dostęp do potrzebnych informacji offline.

Kolejnym problem dla wielu podróżujących jest bariera językowa. Aplikacje tłumaczące, nie tylko umożliwiają przetłumaczenie wypowiedzi rozmówcy, ale też pozwalają skierować kamerę telefonu na napis lub ulotkę i zobaczyć ich tłumaczenie. W sytuacjach, gdy trzeba się dogadać szybko i skutecznie, to prawdziwy ratunek.

- Pobierz pakiet językowy, co umożliwi tłumaczenie bez połączenia z internetem. Zaoszczędzisz transfer i zwiększysz bezpieczeństwo, gdy dane nie będą przesyłane przez sieć.

Nie można zapomnieć o kwestiach finansowych. Korzystanie z aplikacji, ułatwia płacenie kartą za granicą, bez wysokich prowizji i ryzyka blokady karty przez bank. Dodatkowo dzięki przelicznikom walut można od razu zorientować się, ile naprawdę kosztuje sok w lokalnej kawiarni. A mając dziecko przy sobie, każda chwila zaoszczędzona na szukaniu bankomatu ma znaczenie.

- Nawet jeśli używasz płatności mobilnych, zabierz ze sobą fizyczną kartę i gotówkę. W niektórych rejonach świata mogą być problemy z realizacją płatności zbliżeniowych lub płatności cyfrowymi portfelami.

Smartfon to dziś centrum dowodzenia całej podróży. Utrata telefonu, awaria aplikacji, kradzież danych, czy brak dostępu do internetu w kluczowym momencie, potrafią skutecznie zepsuć nawet najlepiej zaplanowany wyjazd. Dlatego warto pomyśleć o cyfrowych zabezpieczeniach, które dadzą nam większy spokój.

- Zabezpiecz dostęp za pomocą kodu, odcisku palca lub rozpoznawania twarzy. To podstawowa bariera ochronna w przypadku zgubienia lub kradzieży.
- Aktywuj usługę „znajdź mój telefon”, która pozwala zlokalizować zgubione urządzenie, a w razie potrzeby – zdalnie je zablokować lub wyczyścić dane.
- Twórz kopie zapasowe zdjęć, kontaktów i dokumentów – najlepiej w chmurze, dzięki czemu nawet utrata telefonu nie oznacza utraty wspomnień ani ważnych informacji.
- Korzystaj z VPN, szczególnie gdy logujesz się do kont bankowych.
- Tak jak swój telefon, zabezpiecz urządzenia dziecka. Dodatkowo skorzystaj z aplikacji kontroli rodzicielskiej.





Zanim ruszymy w drogę, warto również poświęcić chwilę na techniczne przygotowanie. Przydadzą się: aktualizacja systemu, pobranie potrzebnych aplikacji i map, aktywacja roamingu danych lub zakup karty eSIM, naładowany powerbank i uniwersalna ładowarka.

Odpowiednie przygotowanie nie wyeliminuje każdego ryzyka, ale znacząco je zmniejszy. Dobrze przygotowany cyfrowy niezbędnik to nie tylko wygoda, ale i bezpieczeństwo. Bo najlepsze wspomnienia rodzą się tam, gdzie technologia daje nam swobodę bycia tu i teraz – razem.

PORADY UKE:

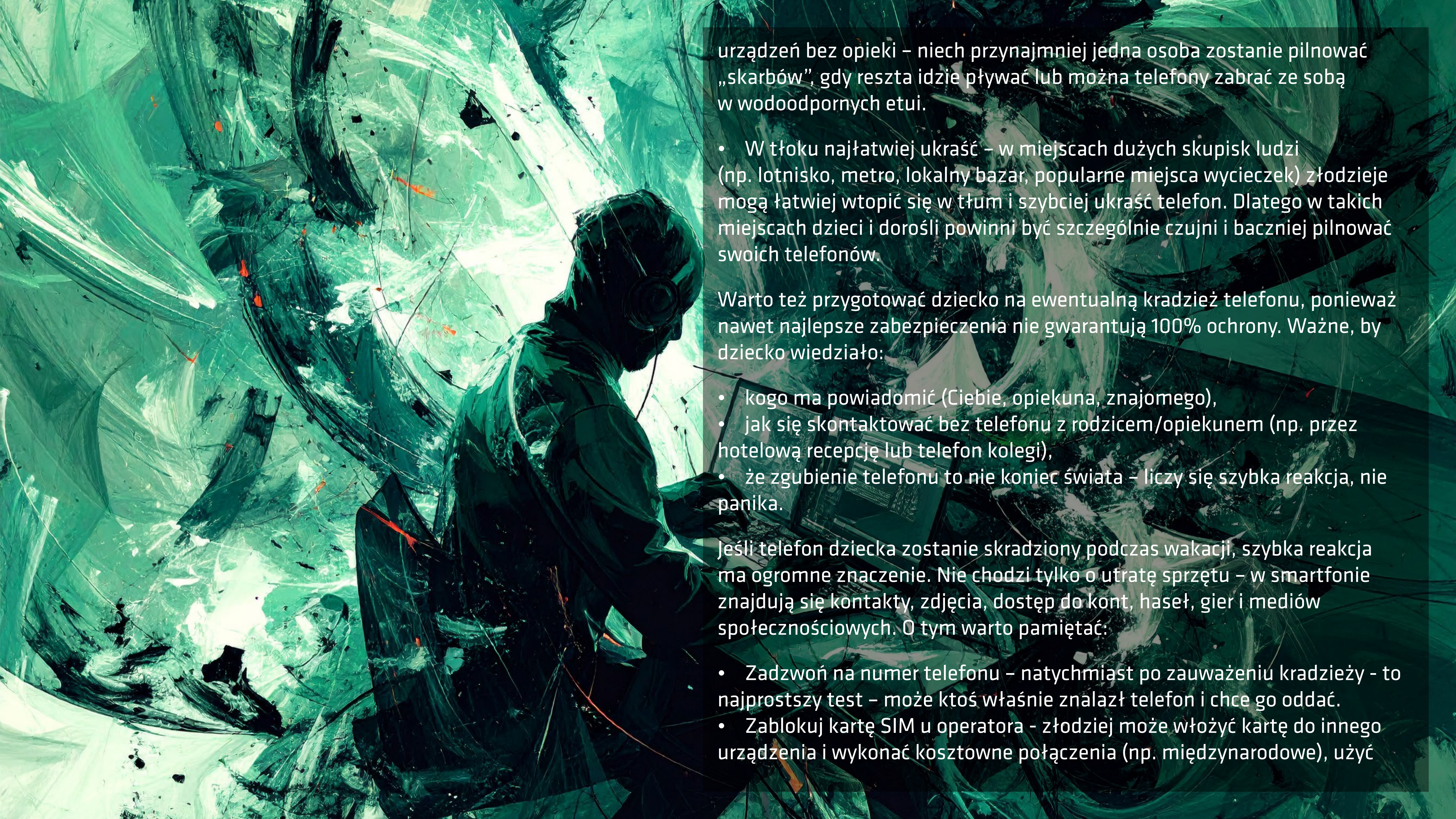
1. Pobierzcie mapy i słowniki offline przed wyjazdem – zwiększysz wygodę i bezpieczeństwo w razie braku dostępu do internetu.
2. Zabezpieczcie telefon hasłem, odciskiem palca lub twarzą – aktywuj funkcje lokalizacji i zdalnej blokady w razie zgubienia lub kradzieży.
3. Włączcie kontrolę rodzicielską i róbcie kopie zapasowe danych – zapewni to bezpieczeństwo dziecka i spokój rodzica.

KRADZIEŻ TELEFONU ZA GRANICĄ – CO ZROBIĆ, BY ZABLOKOWAĆ USŁUGI I CHRONIĆ DANE?

Wakacje to czas beztroski – ale również okres, w którym rośnie ryzyko kradzieży, zwłaszcza w miejscach turystycznych. Telefon to jeden z najczęściej kradzionych przedmiotów – ma wartość finansową oraz jest źródłem wielu danych. Dlatego dobrze, aby dzieci wiedziały jak mogą chronić swoje telefony przed złodziejami. Dotyczy to też Ciebie:)

- Nie trzymaj telefonu „na wierzchu” – zostawianie telefonu na stole w restauracji, na ręczniku na plaży, w tylnej kieszeni spodni czy trzymanie w ręku podczas spaceru zdecydowanie ułatwia „pracę” złodziejowi.
- Unikaj „okazji” dla złodzieja – bardzo często złodzieje działają w duecie: jedna osoba odwraca uwagę (np. zadaje pytanie, upuszcza coś), druga kradnie telefon.
- Stosuj akcesoria utrudniające kradzież – telefony, które nie są w jakiś sposób przypięte do dziecka są łatwiejsze do skradzenia. Telefon na smyczy, w etui na pasku czy schowany w nerce z przodu uniemożliwiają szybka kradzież.
- Nad wodą działaj zespołowo – bardzo często telefony są zostawiane na ręczniku (lub pod nim), kiedy rodzice z dziećmi idą do wody – złodzieje o tym wiedzą i czyhają na takie okazje. Dobrze jest wówczas nie zostawiać





urządzeń bez opieki – niech przynajmniej jedna osoba zostanie pilnować „skarbów”, gdy reszta idzie pływać lub można telefony zabrać ze sobą w wodoodpornych etui.

- W tłoku najłatwiej ukraść – w miejscach dużych skupisk ludzi (np. lotnisko, metro, lokalny bazar, popularne miejsca wycieczek) złodzieje mogą łatwiej wtopić się w tłum i szybciej ukraść telefon. Dlatego w takich miejscach dzieci i dorośli powinni być szczególnie czujni i bacznie pilnować swoich telefonów.

Warto też przygotować dziecko na ewentualną kradzież telefonu, ponieważ nawet najlepsze zabezpieczenia nie gwarantują 100% ochrony. Ważne, by dziecko wiedziało:

- kogo ma powiadomić (Ciebie, opiekuna, znajomego),
- jak się skontaktować bez telefonu z rodzicem/opiekunem (np. przez hotelową recepcję lub telefon kolegi),
- że zgubienie telefonu to nie koniec świata – liczy się szybka reakcja, nie panika.

Jeśli telefon dziecka zostanie skradziony podczas wakacji, szybka reakcja ma ogromne znaczenie. Nie chodzi tylko o utratę sprzętu – w smartfonie znajdują się kontakty, zdjęcia, dostęp do kont, haseł, gier i mediów społecznościowych. O tym warto pamiętać:

- Zadzwoń na numer telefonu – natychmiast po zauważeniu kradzieży - to najprostszy test – może ktoś właśnie znalazł telefon i chce go oddać.
- Zablokuj kartę SIM u operatora - złodziej może włożyć kartę do innego urządzenia i wykonać kosztowne połączenia (np. międzynarodowe), użyć



numeru telefonu do potwierdzenia logowania (np. do kont bankowych lub portali społecznościowych). Skontaktuj się z operatorem, zgłoś kradzież i zablokuj kartę SIM.

- Zlokalizuj i zablokuj telefon zdalnie - jeśli urządzenie ma włączone odpowiednie funkcje telefonu, ma włączoną lokalizację i internet to możesz sprawdzić, gdzie się znajduje, zablokować je na odległość i usunąć wszystkie dane zdalnie.
- Zmień hasła do kont powiązanych z telefonem - zmień hasło do konta Google lub Apple ID – to główne konta, do którego przypisane są telefony. Zmień hasła do aplikacji: Gmail, Instagram, Snapchat, TikTok, Discord itp. Jeśli dziecko lub Ty korzystacie z menedżera haseł – natychmiast zmień dane logowania.
- Wyloguj urządzenie z usług zdalnie - po zmianie hasła część aplikacji automatycznie przestanie działać, ale warto dodatkowo wylogować urządzenie z konta Google i usunąć urządzenie z listy Apple ID.
- Zablokuj urządzenie przez numer IMEI - operator może zablokować urządzenie, by nie dało się go używać w sieci (nawet z inną kartą SIM). Zgłoś kradzież telefonu do operatora i poproś o zablokowanie IMEI.

PORADY UKE:

1. Przygotujcie swoje telefony przed wyjazdem - włącz funkcję lokalizacji, zabezpiecz ekran hasłem, ustaw możliwość zdalnego zablokowania i zapisz numer IMEI. Dzięki temu w razie kradzieży będziesz mógł szybko zareagować.
2. Ucz dziecko, by nie nosiło telefonu „na widoku” - telefon powinien być zawsze schowany – najlepiej w nerce, wewnętrznej kieszeni lub przypięty smyczką. To prosty nawyk, który realnie zmniejsza ryzyko kradzieży.
3. Działaj od razu po utracie telefonu - zablokuj kartę SIM u operatora, zlokalizuj i zablokuj urządzenie zdalnie (przez iCloud lub Google), zmień hasła do kont dziecka. Im szybciej zadziałasz, tym mniej szkód powstanie.



DZIECI ONLINE PODCZAS WAKACJI – JAK USTAWIĆ KONTROLĘ RODZICIELSKĄ W TELEFONIE I TABLECIE?

W czasie wakacji rośnie ryzyko, że dzieci natkną się na treści nieodpowiednie dla ich wieku, przypadkiem zrobią zakupy w aplikacjach albo po prostu poświęcą zbyt wiele godzin na cyfrową rozrywkę. Dlatego wakacje to idealny moment, by wybrać narzędzia kontroli rodzicielskiej.

Dlaczego warto włączyć kontrolę rodzicielską

Wbrew pozorom kontrola rodzicielska nie służy do szpiegowania dziecka, lecz do budowania bezpiecznej przestrzeni w internecie. Pozwala filtrować treści, ograniczać czas korzystania z urządzeń, a także monitorować aktywność dziecka – wszystko po to, by chronić jego rozwój psychiczny i emocjonalny a także dbać o jego bezpieczeństwo. Odpowiednie ustawienia pomagają też unikać sytuacji, w których dziecko może nieświadomie przekazać swoje dane osobowe lub natrafić na nieodpowiednie kontakty online.

Jak skonfigurować kontrolę rodzicielską w telefonie lub tablecie

Proces zależy od rodzaju urządzenia – najczęściej mówimy tu o systemach Android i iOS. Na obu platformach dostępne są wbudowane rozwiązania,

które pozwalają rodzicom mieć większą kontrolę nad tym, co dziecko robi w sieci.

System operacyjny Android oferuje kilka warstw kontroli rodzicielskiej, zarówno wbudowanych, jak i dostępnych poprzez oficjalne narzędzia Google. Rodzic zakłada swoje konto na wybranej przez siebie aplikacji, a następnie łączy z nim konto dziecka. W ten sposób można zarządzać aplikacjami instalowanymi na telefonie, ustalać limity czasowe dla poszczególnych programów, a także ustawić godziny, w których urządzenie automatycznie się blokuje (np. po godzinie 21:00). Co ważne, można też monitorować lokalizację dziecka, jeśli ma ono telefon przy sobie.

W przypadku urządzeń z systemem iOS, takich jak iPhone czy iPad, Apple oferuje funkcję Czas przed ekranem. Po aktywacji tej opcji, w ustawieniach, rodzic może zdefiniować limity czasowe na aplikacje (np. gry, media społecznościowe), zablokować dostęp do nieodpowiednich stron internetowych oraz kontrolować zakupy w App Store. Możliwe jest również ustawienie tzw. „czasu bez urządzenia” – czyli godzin, w których dziecko nie powinno korzystać z tabletu czy telefonu.

Poza systemowymi rozwiązaniami, są aplikacje, które oferują bardziej zaawansowane możliwości. Pozwalają one nie tylko monitorować aktywność online, ale również analizować, ile czasu dziecko spędza w konkretnych aplikacjach, blokować dostęp do niektórych treści (np. przemoc, pornografia), a nawet prowadzić zdalną kontrolę nad urządzeniem z poziomu aplikacji rodzica. Dodatkowo usługi kontroli rodzicielskiej oferują również dostawcy usług komunikacji elektronicznej.



The background of the entire slide is an abstract digital artwork. It features a woman's profile in the upper left, looking down. The background is a complex web of dark blue and black lines, with some orange and yellow highlights, suggesting a digital or networked environment.

PORADY UKE:

1. Skonfigurujcie kontrolę rodzicielską jeszcze przed wakacjami – użyjcie narzędzi w systemie Android, iOS lub aplikacji zewnętrznych.
2. Ustalcie limity czasu i dostęp do treści – blokujcie aplikacje nieodpowiednie wiekowo oraz ustawcie „czas offline”.
3. Rozmawiajcie z dziećmi o tym, dlaczego są ograniczenia – budujcie zaufanie i edukujcie, zamiast tylko blokować.

Wybierając narzędzie kontroli zwróć uwagę:

- Cena vs funkcje
- Profilowanie urządzeń – możliwość tworzenia wielu profili i zarządzanie kilkoma urządzeniami
- Bezpieczeństwo urządzeń, np. dodatkowa ochrona antywirusowa
- Powiadomienia i raporty – dostęp do historii aktywności i prób dostępu do zablokowanych treści

Wprowadzenie kontroli rodzicielskiej to jedno, ale ważniejsze jest prowadzenie dialogu z dzieckiem. Dobrze, gdy dziecko rozumie, dlaczego pewne treści są zablokowane, dlaczego jego czas przed ekranem jest ograniczany i jak powinno korzystać z internetu w sposób odpowiedzialny. Taka rozmowa buduje zaufanie i uczy samodzielnego podejmowania właściwych decyzji w przyszłości.

Wakacje nie muszą oznaczać braku zasad – zwłaszcza gdy chodzi o bezpieczeństwo dzieci online. Dobrze skonfigurowana kontrola rodzicielska może być cennym wsparciem dla rodziców, którzy chcą zadbać o zdrową cyfrową równowagę swoich pociech. Warto poświęcić chwilę na ustawienie tych narzędzi i regularnie wracać do tematu korzystania z technologii w rozmowach z dzieckiem.

WAKACYJNE ZDJĘCIA W SIECI – ŁADNE WSPOMNIENIA CZY RYZYKOWNA INFORMACJA?

Wakacje to jeden z najbardziej „instagramowych” okresów w roku. Słońce, plaża, malownicze widoki – to aż prosi się o zdjęcie. Ale zanim wrzucimy fotkę z palmą, selfie z drinkiem czy story z apartamentu, warto zastanowić się czy wszystkim powinieneś się dzielić. Daj dobry przykład swoim dzieciom.

Wakacje zaczynają się od świadectw z czerwonym paskiem

Koniec roku szkolnego to publikowanie przez rodziców w mediach społecznościowych świadectw z czerwonym paskiem, , często bez zastanowienia, że wraz z pochwałą za dobre wyniki szkolne udostępniane są też dane osobowe dziecka: imię, nazwisko, data urodzenia, nazwa szkoły, klasa. Choć intencją rodziców jest zazwyczaj duma i radość, to warto zadać sobie pytanie, czy za kilka lat ich dziecko – już jako nastolatek lub dorosły – będzie zadowolone z tego, że jego życie od najmłodszych lat było relacjonowane publicznie. Sharenting, czyli nadmierne dzielenie się informacjami o dzieciach w internecie, może prowadzić do naruszenia prywatności, utraty kontroli nad własnym wizerunkiem, a nawet do poważniejszych zagrożeń, takich jak kradzież tożsamości czy cyberprzemoc. Zanim więc klikniemy ,opublikuj’, warto zapytać nie tylko siebie, ale i swoje dziecko: czy naprawdę chce, żeby cały świat widział jego świadectwo?





- Nigdy nie publikuj w sieci danych osobowych dziecka. Jeśli chcesz się pochwalić jego sukcesem rób to w sposób, który nie narazi dziecka na potencjalne niebezpieczeństwo.

Zdjęcia dzieci w kostiumach kąpielowych? Lepiej nie

Wiele osób wrzuca do sieci zdjęcia dzieci na plaży, w basenie, w letnich ubraniach, w sytuacjach prywatnych czy półnagich. Taki obrazek dla rodzica może być „słodki”, ale dla obcych – może mieć zupełnie inny wydźwięk. Natomiast za kilka lat, dla Twojego nastolatka, „urocza fotka z dziś”, może być źródłem wstydu i upokorzenia.

Nie mamy wpływu, kto zobaczy nasze zdjęcie, zapisze je, przekaże dalej. W skrajnych przypadkach fotografie dzieci trafiają w niepowołane ręce. Zdjęcia dzieci mogą być również przerobione przez AI w pornograficzne deepfake. Brzmi jak scenariusz z filmu? Niestety, to realne ryzyko. Według raportu Australian Institute of Criminology (AIC) z 2024 r., prawie 7% osób, które opublikowały zdjęcia dzieci w Internecie, otrzymało prośby o materiały związane z wykorzystywaniem dzieci. Udostępnianie zdjęcia lub informacji o dzieciach wiązało się ze znacznie zwiększonym prawdopodobieństwem zadawania pytań o charakterze seksualnym na temat dzieci, a także proszenia, wywierania nacisku lub oferowania zapłaty za seksualne zdjęcia dzieci.

Geolokalizacja – niechciany tropiciel

Wiele platform społecznościowych automatycznie zapisuje lokalizację zdjęcia – nawet jeśli my jej nie oznaczymy. Jeśli mamy włączony GPS w telefonie i nie wyłączyliśmy tej funkcji w ustawieniach aplikacji, każde zdjęcie może zawierać informacje, gdzie dokładnie zostało zrobione. Po co ułatwiać komuś śledzenie naszych tras?

Oznaczając hotel, miasto, restaurację czy plażę – w czasie, gdy tam przebywamy –

pokazujemy nie tylko, gdzie jesteśmy, ale często też z kim, z jakimi dziećmi, jak długo tam będziemy i kiedy wrócimy. To z pozoru tylko migawka, ale dla kogoś, kto zbiera dane, może być bezcenna. W skrajnych przypadkach pokazujemy przestępcy nasz plan dnia.

Cyfrowy ślad, który zostaje na zawsze

Wakacyjne zdjęcia to piękne wspomnienia – ale pamiętajmy, że internet nie zapomina. To, co dziś jest beztróskim kadrem z podróży, za kilka lat może być powodem do zażenowania. Szczególnie dla dzieci, które dorastają i nie chcą, by ich zdjęcia w piżamie z maskotką były publicznie dostępne.

Dodatkowo – każde zdjęcie buduje nasz cyfrowy profil. Nawet jeśli nie mamy nic do ukrycia, z czasem może to wpływać na to, jak jesteśmy postrzegani przez pracodawcę, znajomych, szkołę dziecka.

Zasady bezpiecznego dzielenia się wakacjami w sieci

- Opóźnij publikację – wrzucaj zdjęcia dopiero po powrocie.
- Zamazuj dane osobowe – na biletach, kartach hotelowych, dokumentach.
- Nie oznaczaj lokalizacji w czasie rzeczywistym.
- Nie pokazuj dzieci w sytuacjach prywatnych lub intymnych (np. w kostiumie, w łóżku, przy jedzeniu).
- Zadbaj o ustawienia prywatności – niech Twoje zdjęcia widzą tylko zaufani znajomi.
- Zawsze pytaj dziecko o zgodę, jeśli jest w wieku, w którym może ją świadomie wyrazić.

Wakacje są od tego, by odpoczywać i kolekcjonować wspomnienia. Internet nie musi wiedzieć, gdzie jesteśmy, co jemy i jak wyglądał każdy dzień naszego wyjazdu. Czasem mniej znaczy bezpieczniej – i mądrzej.

PORADY UKE:

1. Nie publikujcie zdjęć dzieci w kostiumach, w łóżku, przy jedzeniu – to może naruszać prywatność lub zostać źle wykorzystane.
2. Wyłączcie geolokalizację zdjęć i opóźniajcie publikację – nie pokazujcie na bieżąco, gdzie jesteście i jak długo.
3. Zanim opublikujesz zdjęcie dziecka – zapytaj o zgodę – zwłaszcza gdy dziecko ma już możliwość świadomego wyboru.



PODSUMOWANIE

Po przeczytaniu tego poradnika warto zrobić jeszcze kilka rzeczy:

Zatrzymaj się na chwilę i przyjrzyj swoim nawykom. Czy publikujesz więcej niż chcesz? Czy zawsze pytasz dziecko o zgodę, zanim pokażesz je w sieci?

Sprawdź, czy dzieci wiedzą, że mogą przyjść do Ciebie z każdym problemem – również tym z internetu. Czasem wystarczy jedno zdanie, które pokaże, że jesteś po ich stronie.

Omów z innymi dorosłymi w rodzinie lub gronie znajomych, jak wspólnie możecie wspierać dzieci w cyfrowym świecie. Dziadkowie, opiekunowie czy starsze rodzeństwo też mają wpływ na to, jakie zasady obowiązują w domu czy na wyjeździe.

Ten poradnik to początek rozmowy – nie jej koniec. Technologie będą się zmieniać, ale wartości, które przekazujemy dzieciom, pozostają te same: szacunek, odpowiedzialność i uważność. Niech te wartości towarzyszą Wam także w czasie letniego wypoczynku – w realu i online.

Życzymy udanego, bezpiecznego i pełnego dobrych wspomnień wypoczynku dla dzieci i ich opiekunów!



CIK.UKE.GOV.PL

Urząd Komunikacji Elektronicznej

UKE