



UKE

KIESZONKOWY

PORADNIK

WAKACYJNY

DLA RODZICÓW

Spis treści

Wstęp: Letnia wolność pod cyfrową lupą

Rozdział 1: Domowa nuda i smartfon jako „niania” - jak nie stracić kontroli?

Rozdział 2: Sztuczna inteligencja (AI) na wakacjach - nowe oblicze cyfrowego ryzyka

Rozdział 3: Niewidzialne pułapki w telefonie - na co polują cyberprzestępcy?

Rozdział 4: Sharenting i cyfrowy ślad - kiedy dumni rodzice nieświadomie szkodzą dzieciom

Rozdział 5: Cyfrowy portfel nastolatka - wakacyjne kieszonkowe i bezpieczne płatności

Rozdział 6: Zgubiony lub skradziony telefon za granicą - plan awaryjny krok po kroku

Rozdział 7: Cyfrowy niezbędnik podróżnika - aplikacje i ustawienia, które warto znać przed wyjazdem

Rozdział 8: Wakacyjny kontrakt cyfrowy

Podsumowanie: Wspólny powrót do realu

Letnia wolność pod cyfrową lupą

Wakacje to czas odpoczynku, przygód i wspólnych chwil, zarówno offline, jak i online. Kiedy jednak wybrzmiewa ostatni dzwonek szkolny, dla nas rodziców, zaczyna się logistyczny maraton. Podczas gdy my musimy normalnie pracować, dzieci zostają w domach lub wyjeżdżają na obozy z ogromną ilością wolnego czasu, którego nie organizuje już plan lekcji.

W dzisiejszym świecie trudno sobie wyobrazić wakacje bez smartfona, zdjęć z podróży wrzucanych na Instagram, 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 z myślą o rodzicach i dzieciach, po to, by pomóc bezpiecznie korzystać z technologii podczas wakacji. Podpowiemy, jak rozmawiać o odpowiedzialnym korzystaniu z sieci, jak zadbać o ochronę danych, kontrolować czas przed ekranem bez odbierania dzieciom swobody oraz jak uważać na najnowsze zagrożenia związane ze sztuczną inteligencją.



1. Domowa nuda i smartfon jako *niania*, czyli jak nie stracić kontroli?

Dobrze to znacie: "Mamo, tato, nudzę się!". W pośpiechu, pomiędzy jednym mailem z pracy a drugim, najłatwiej jest machnąć ręką i pozwolić dziecku na "kilka minut" z telefonem. Problem polega na tym, że w wakacje te minuty błyskawicznie zamieniają się w długie godziny.

Algorytmy zatrzymywania uwagi

Wakacyjny brak rutyny sprawia, że dzieci bezwiednie wpadają w pętlę algorytmów serwisów społecznościowych, które są zaprojektowane tak, by maksymalnie przykuwać uwagę i utrudniać odłożenie ekranu.

FOMO (Lęk przed wykluczeniem)

Brak codziennego widywania znajomych z klasy nasila potrzebę ciągłego odświeżania aplikacji. Dzieci czują przymus bycia online, by nie ominął ich żaden wakacyjny trend czy wewnętrzny żart grupy rówieśniczej.

Wakacyjne wyzwania (Challenges)

Nuda rodzi ryzykowne pomysły. Niektóre wakacyjne wyzwania na TikToku mogą być bardzo ryzykowne, np. zachęcają do skakania z niebezpiecznych wysokości do wody, uciekania przed ochroniarzami czy niszczenia mienia.

Zadbajcie wspólnie o cyfrową równowagę i wprowadźcie rytuały offline. Ustalcie stałe momenty bez telefonów, np. wspólne śniadanie, wieczorna gra planszowa czy wyprawa rowerowa bez powiadomień. Nie musicie od razu wprowadzać całodniowego „detoksu cyfrowego”. Wystarczy umówić się, że po wspólnym wyjściu na spacer lub wykonaniu obowiązków domowych, dziecko ma swoją określoną godzinę na ulubione gry i aplikacje. Dzieci znacznie lepiej reagują na jasne, partnerskie zasady niż na nagłe zakazy bez uzasadnienia.

2. Sztuczna inteligencja na wakacjach, czyli nowe oblicze cyfrowego ryzyka

Świat technologii pędzi naprzód, a internetowi oszuści zyskali zupełnie nowe, zaawansowane narzędzia oparte na sztucznej inteligencji. Warto poznać te mechanizmy, zanim uderzą w naszą rodzinę.

Klonowanie głosu (Voice Scam)

Oszuści potrafią wykorzystać krótkie próbki dźwiękowe (np. z filmiku, który Wasze dziecko wrzuciło na publiczny profil). Za pomocą programów AI są w stanie idealnie sklonować głos syna lub córki. Następnie dzwonią do rodziców lub dziadków, symulując płacz i dramatyczną sytuację: "Mamo, miałem wypadek, pilnie potrzebuję pieniędzy".

Manipulacja wizerunkiem (Deepfake)

Zdjęcia dzieci mogą być bez ich wiedzy przerobione przez algorytmy AI w nieodpowiednie, kompromitujące lub nawet pornograficzne materiały (tzw. deepnude). W czasie wakacji, gdy młodzież robi masę zdjęć, takie przerobione grafiki stają się groźnym narzędziem szantażu rówieśniczego i cyberbullyingu.

Emocjonalne boty AI

Samotne dni w domu sprzyjają szukaniu kontaktu z chatbotami AI udającymi realnych ludzi. Boty te potrafią manipulować emocjonalnie młodym człowiekiem, stopniowo wyciągając od niego wrażliwe informacje o rodzinie, adresie domowym czy statusie materialnym.

Wprowadźcie rodzinne *hasło ratunkowe* i rozmawiajcie o manipulacjach AI. Ustalcie jedno tajne, unikalne słowo lub frazę znaną wyłącznie członkom najbliższej rodziny (np. *ZielonaPapuga2026*). Nauczcie dziecko i dziadków, że jeśli ktokolwiek zadzwoni i podając się za krewnego, będzie prosił o nagłą pomoc finansową lub podanie danych, należy bezwzględnie zażądać podania hasła ratunkowego. Jeśli rozmówca go nie zna, to próba oszustwa.



3. Niewidzialne pułapki w telefonie - na co polują cyberprzestępcy?

Brak nadzoru nauczycieli i rozluźnienie dyscypliny przez rodziców to idealne warunki dla cyberprzestępców. Polują oni na nieuwagę najmłodszych użytkowników sieci, którzy w wakacje grają znacznie więcej.

Oszustwa na mikropłatności

Gry takie jak Roblox, Fortnite czy Minecraft wciągają w wakacje mocniej niż zwykle. Dzieci, chcąc zdobyć unikalne przedmioty (skiny), dają się nabrać na fałszywe strony oferujące „darmowe generatory walut”. Efekt? Wyłudzenie haseł do kont lub podpięcie karty płatniczej rodzica i gigantyczne rachunki.

Niebezpieczne aplikacje

Szukając nowych gier, młodzież niekiedy pobiera programy z niesprawdzonych źródeł. Zanim zainstalujecie nową aplikację, sprawdźcie, kto ją stworzył i jakie ma opinie w oficjalnym sklepie. Nie zezwalajcie aplikacjom na dostęp do kontaktów, zdjęć czy lokalizacji, jeśli nie są one niezbędne do ich działania.

Fałszywi znajomi w grach sieciowych

W grach online dzieci stale spotykają rówieśników, ale i nieznanym dorosłych, którzy udają dzieci. Próbuje oni zdobyć zaufanie dziecka, wyciągać prywatne dane lub namawiać na spotkania w świecie realnym.

 **Zastosujcie zasadę 3P i włączcie kontrolę rodzicielską. Wyłumaczcie dziecku, by w kontaktach online nigdy nie podawało nieznanym swojego dokładnego imienia, wieku, szkoły, numeru telefonu ani miejsca pobytu.**

 **Pytaj, jeśli nie wiesz, kto do Ciebie pisze.
Pokaż rodzicowi, opiekunowi każdą dziwną wiadomość.
Powiedz, jeśli coś Cię zaniepokoiło lub ktoś prosi Cię o zdjęcia.**

UKE



4. Sharenting i cyfrowy ślad – kiedy dumni rodzice nieświadomie szkodzą dzieciom

Bezpieczeństwo cyfrowe naszych dzieci w okresie letnim zależy w równej mierze od zachowania nas samych - dorosłych. Wakacje to jeden z najbardziej „instagramowych” okresów w roku, a zjawisko sharentingu (nadmiernego dzielenia się życiem dzieci w sieci) osiąga wtedy apogeum.

Plażowe kadry pod lupą przestępców

Wiele osób wrzuca do sieci zdjęcia dzieci na plaży, w basenie czy w letnich, skąpych ubraniach. Taki obrazek dla rodzica jest „śladki”, ale dla obcych osób, może mieć zupełnie inny wydźwięk. Zdjęcia te mogą zostać zapisane i trafić w niepowołane ręce w mrocznych zakątkach internetu.

Publikowanie dokumentów i świadectw

Koniec roku szkolnego to plaga wrzucania zdjęć świadectw z czerwonym paskiem. Wraz z pochwałą udostępniane są pełne dane osobowe dziecka: imię, nazwisko, data urodzenia, klasa i nazwa szkoły. To kopalnia wiedzy dla oszustów budujących cyfrowy profil dziecka.

Geolokalizacja w czasie rzeczywistym

Oznaczając hotel, plażę czy kurort w czasie, gdy tam przebywamy, pokazujemy przestępcom nasz dokładny plan dnia oraz informujemy, że nasz dom stoi pusty.

Ustalcie zasady nagrywania innych osób i pytajcie dziecko o zgodę na publikację. Wprowadźcie w domu żelazną zasadę: nie publikujemy zdjęć dzieci w sytuacjach prywatnych, intymnych (w kostiumie kąpielowym, przy jedzeniu czy podczas snu). Zawsze pytajcie swoje dziecko o zgodę na wrzucenie zdjęcia do sieci, jeśli jest już w wieku, w którym może ją świadomie wyrazić. Co więcej, ustalcie zasady nagrywania innych osób. Wy tłumaczcie dziecku, że kręcąc wakacyjne filmiki na TikToka czy YouTube, nie wolno nagrywać i publikować wizerunku znajomych z kolonii, obsługi hotelowej czy przypadkowych turystów bez ich wyraźnej zgody. Każdy ma prawo do prywatności.

5. Cyfrowy portfel nastolatka – wakacyjne kieszonkowe i bezpieczne płatności

Wakacje sprzyjają pierwszym samodzielnym zakupom dzieci czy to na gofry podczas kolonii, czy na nowe cyfrowe dodatki w grach. Coraz częściej tradycyjne banknoty zastępujemy dziecku płatnościami telefonem, kartą przedpłaconą lub BLIK-iem. To wygodne, ale wymaga edukacji finansowej.

Fałszywe zbiórki i loterie

W okresie letnim się zalewają fałszywe reklamy obiecujące szybki zysk, tanie smartfony za symboliczną złotówkę czy konkursy organizowane przez rzekomych influencerów. Dzieci, chcąc wykazać się samodzielnością, potrafią stracić całe swoje kieszonkowe.

Przechwytywanie danych kart płatniczych

Korzystanie przez młodzież z niezweryfikowanych stron internetowych lub klikanie w linki z SMS-ów (np. o rzekomej dopłacie do paczki z wakacyjnymi ubraniami) może prowadzić do utraty oszczędności życia z konta rodzica, jeśli karta jest podpięta pod wspólny profil.

Publiczne sieci Wi-Fi a bankowość

Korzystanie z otwartych, darmowych sieci Wi-Fi na lotniskach, w hotelach czy kawiarniach w niektórych krajach niesie ryzyko. Cyberprzestępcy tworzą fałszywe punkty dostępowe, by przechwytywać loginy i hasła.

Zablokujcie publiczne Wi-Fi dla operacji finansowych i wdróżcie powiadomienia o płatnościach. Nauczcie dziecko, że podczas korzystania z publicznych sieci Wi-Fi w kurortach ryzykowne jest logowanie się do bankowości elektronicznej, poczty e-mail czy wpisywanie haseł do gier. Jeśli zaistnieje pilna potrzeba logowania, dziecko musi wyłączyć Wi-Fi i przejść na własny pakiet danych (roaming) lub użyć szyfrowanego połączenia VPN. Dodatkowo na koncie lub karcie dziecka ustawcie niskie limity dziennych transakcji oraz włączcie powiadomienia SMS/push na swoim telefonie o każdym wydatku.



6. Zgubiony lub skradziony telefon za granicą - plan awaryjny krok po kroku

Telefon w podróży to nasze centrum dowodzenia, ale w zatłoczonych miejscach turystycznych (bazarach, metrze, plażach) drastycznie rośnie ryzyko kradzieży lub zgubienia sprzętu. Urządzenie ma nie tylko wartość finansową, ale przede wszystkim jest źródłem naszych prywatnych danych, haseł i wspomnień.

Złodziejskie patenty na plaży i w tłumie

Bardzo często złodzieje działają w duetach, jedna osoba odwraca uwagę (pyta o drogę, coś upuszcza), a druga kradnie telefon leżący na kawiarnianym stoliku czy wystający z tylnej kieszeni spodni. Często zostawiamy też sprzęt bez opieki na ręczniku, idąc całą rodziną kąpać się w morzu.

Ryzyko braku szybkiej reakcji

Jeśli smartfon nie zostanie zablokowany natychmiast po kradzieży, złodziej może wykorzystać kartę SIM do wykonania bardzo kosztownych połączeń międzynarodowych lub użyć numeru do autoryzacji logowań w banku.

Przygotujcie urządzenia przed wyjazdem i nauczcie dziecko procedury awaryjnej. Przed wyjazdem zabezpieczcie ekrany wszystkich telefonów kodem PIN, odciskiem palca lub biometrią twarzy. Włączcie funkcję lokalizacji oraz usługę zdalnego blokowania i czyszczenia danych (np. Znajdź mój iPhone/Find My Device Google). Zapiszcie też numer IMEI urządzenia. Nauczcie dziecko, że zgubienie telefonu to nie koniec świata i nie należy panikować, ale natychmiast zgłosić to Wam lub opiekunowi na kolonii. **W przypadku utraty sprzętu działajcie od razu: zablokujcie kartę SIM u operatora, zablokujcie telefon zdalnie i zmieńcie hasła do kont głównych (Google, Apple ID) oraz aplikacji społecznościowych.**

Dostawcy usług telekomunikacyjnych mają obowiązek uniemożliwienia korzystania w swojej sieci ze skradzionych lub zagubionych urządzeń końcowych, takich jak telefony, tablety i modemy. Najczęściej stosowaną metodą jest identyfikacja urządzeń na podstawie numeru IMEI, który jest unikalnym identyfikatorem nadawanym każdemu urządzeniu mobilnemu.

Pamiętaj! Dostawca zablokuje urządzenie, jeśli zgłosisz kradzież w odpowiednim trybie. Zgłaszanie kradzieży podlega przepisom Kodeksu postępowania karnego dotyczącym zawiadomienia o przestępstwie. Osoba poszkodowana powinna uzyskać poświadczenie zgłoszenia kradzieży. Blokowane są również urządzenia zgubione przez abonenta. Składając wniosek o zablokowanie skradzionego/zgubionego telefonu musisz przedstawić dostawcy dowód kupna lub inne dane jednoznacznie potwierdzające, że to Twoja własność.

UKE



7. Cyfrowy niezbędnik podróżnika – aplikacje i ustawienia, które warto znać przed wyjazdem

Odpowiednie przygotowanie technologiczne przed urlopem potrafi uratować nas z niejednej opresji, zaoszczędzić sporo nerwów, pieniędzy oraz gigabajtów transferu za granicą.

Pułapka braku zasięgu

Poleganie wyłącznie na nawigacji działającej online może nas zgubić w lasach, górach lub na zagranicznych bezdrożach, gdzie nagle stracimy zasięg sieci komórkowej.

Bariera językowa w kryzysowej sytuacji

Brak możliwości szybkiego przetłumaczenia menu, rozkładu jazdy czy tablicy informacyjnej w obcym kraju bywa ogromnym utrudnieniem w podróżowaniu z dziećmi.

Juice Jacking (Złośliwe ładowarki)

Podłączanie telefonu do darmowych, publicznych portów USB na lotniskach czy dworcach kolejowych za pomocą samego kabla niesie ryzyko infekcji złośliwym oprogramowaniem. Specjalnie zmodyfikowane gniazda USB potrafią potajemnie zgrywać dane z podłączonych smartfonów.



8. Wakacyjny kontrakt cyfrowy

Aby wakacyjne porady nie pozostały jedynie teorią, stwórzcie z dzieckiem prosty, przejrzysty Wakacyjny Kodeks Cyfrowy, który określi sztywne, ale partnerskie reguły gry na czas letnich miesięcy.

Zasada Najpierw pokaż, potem wrzucaj

Chroni młodsze dzieci przed publikacją wizerunku bez przemyślenia konsekwencji.

Strefy wolne od ekranów

Telefony odkładamy całkowicie podczas posiłków oraz wspólnych wyjść do restauracji czy na plażę.

Zablokowana lokalizacja

Wyłączamy funkcję GPS dla aplikacji społecznościowych i nie oznaczamy miejsc pobytu w czasie rzeczywistym.

Zgłaszanie zamiast ukrywania

Dziecko ma prawo zablokować hejtera i zgłosić każdą nieodpowiednią treść rodzicowi bez obaw o karę.

Opóźniona publikacja wspomnień

Zdjęcia z wakacji wrzucamy na profile społecznościowe dopiero po powrocie z wyjazdu.

Instalacja aplikacji tylko z oficjalnych sklepów

Gry i aplikacje pobieramy wyłącznie za zgodą rodzica z Google Play lub App Store.

Ochrona prywatności rówieśników

Nie nagrywamy i nie publikujemy innych osób bez ich wyraźnej zgody.

Złoty balans (Czas offline)

Ustalamy dzienny limit czasu przed ekranem, dbając o regularne przerwy na ruch na świeżym powietrzu.

Kopia zapasowa przed wyjazdem

Wszystkie zdjęcia, kontakty i dokumenty przed podróżą zgrywamy do chmury lub na dysk zewnętrzny.

Dobry przykład idzie z góry

Rodzic sam odkłada telefon w ważnych, rodzinnych momentach wyjazdu.



UKE

Wspólny powrót do realu

Najważniejszym wnioskiem, jaki powinien płynąć z lektury tego poradnika, nie jest bezwzględny zakaz korzystania z technologii i całkowite odcięcie dziecka od sieci. **Internet, smartfony oraz narzędzia sztucznej inteligencji to naturalne środowisko współczesnego młodego pokolenia.**

Najlepsze wakacyjne wspomnienia rodzą się tam, gdzie technologia daje nam swobodę bycia tu i teraz - razem. Po przeczytaniu tego poradnika, zatrzymajcie się na chwilę i przyjrzyjcie własnym nawykom. Upewnijcie się, że Wasze dzieci wiedzą, że mogą przyjść do Was z każdym, nawet najtrudniejszym problemem. Czasem wystarczy jedno spokojne zdanie: „Jestem po Twojej stronie, rozwiążemy to razem”, by otworzyć przestrzeń do mądrego dialogu, który ochroni nasze pociechy skuteczniej niż jakakolwiek blokada systemowa.

Życzymy bezpiecznego, spokojnego i pełnego wspaniałych, rodzinnych przygód wypoczynku!