(CYBER)BEZPIECZNE
ŚWIĘTA Z OSE

ose it-szkoła

ose OGÓLNOPOLSKA SIEĆ EDUKACYJNA

Grudzień to dla nas wyjątkowy czas – organizujemy rodzinne spotkania, kupujemy prezenty, składamy życzenia i świętujemy Boże Narodzenie. Co zrobić, by Gwiazdka wiązała się jedynie z radością i wspaniałą, rodzinną atmosferą, a niekoniecznie z cyfrowymi kłopotami? Przygotowaliśmy dla Was wyjątkowy poradnik, który pomoże Wam ustrzec się przed zagrożeniami online w okresie świątecznym. Skorzystajcie z porad Ogólnopolskiej Sieci Edukacyjnej (OSE) i bądźcie bezpieczni w internecie!

W święta odbieramy wiele SMS-ów, telefonów i elektronicznych kartek z życzeniami. Uważajcie i nie dajcie się złapać w pułapkę phishingu!

Cyberprzestępcy nie śpią i stale wymyślają nowe sposoby na wyłudzenie naszych danych i środków z kont bankowych. Bywa, że podszywają się pod znane instytucje czy firmy – chcą uśpić naszą czujność i skłonić do kliknięcia w niebezpieczny link czy pobrania zainfekowanego załącznika.

Jak chronić się przed oszustami? Zwracajcie szczególną uwagę na elektroniczne kartki z życzeniami (phishing), SMS-y z prośbą o dopłatę do paczki czy natychmiastowe uregulowanie zaległej faktury (smishing) oraz podejrzane telefony, np. z banku (vishing). Przyglądajcie się też samej wiadomości – jeżeli zawiera błędy językowe i manipulujące komunikaty (np. „podaj dane w ciągu 24 godzin") oraz jest skierowana do ogólnego odbiorcy (np. „Szanowny Kliencie"), najprawdopodobniej została wysłana przez oszusta.

Uważajcie też na wiadomości, które rzekomo pochodzą od Waszych znajomych, jednak ani ton wypowiedzi, ani używane zwroty nie pasują do nadawców. Upewnijcie się, czy to faktycznie znajomy spróbował się z Wami kontaktować – choćby dzwoniąc do niego.

Jeśli otrzymacie podejrzaną wiadomość, zachowajcie ostrożność: nie klikajcie w żadne linki i nie dokonujcie płatności, zgłoście się też do CERT Polska za pomocą formularza, a podejrzany SMS prześlijcie na numer **799 448 084**.

Więcej porad znajdziecie w aktualnościach na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: świąteczny phishing" i „Bezpiecznicw sieci z OSE: phishing".

Internet nie zna granic! Kontaktując się z bliskimi za pomocą komunikatorów czy wideokonferencji, musicie jednak pamiętać o podstawowych zasadach bezpieczeństwa.

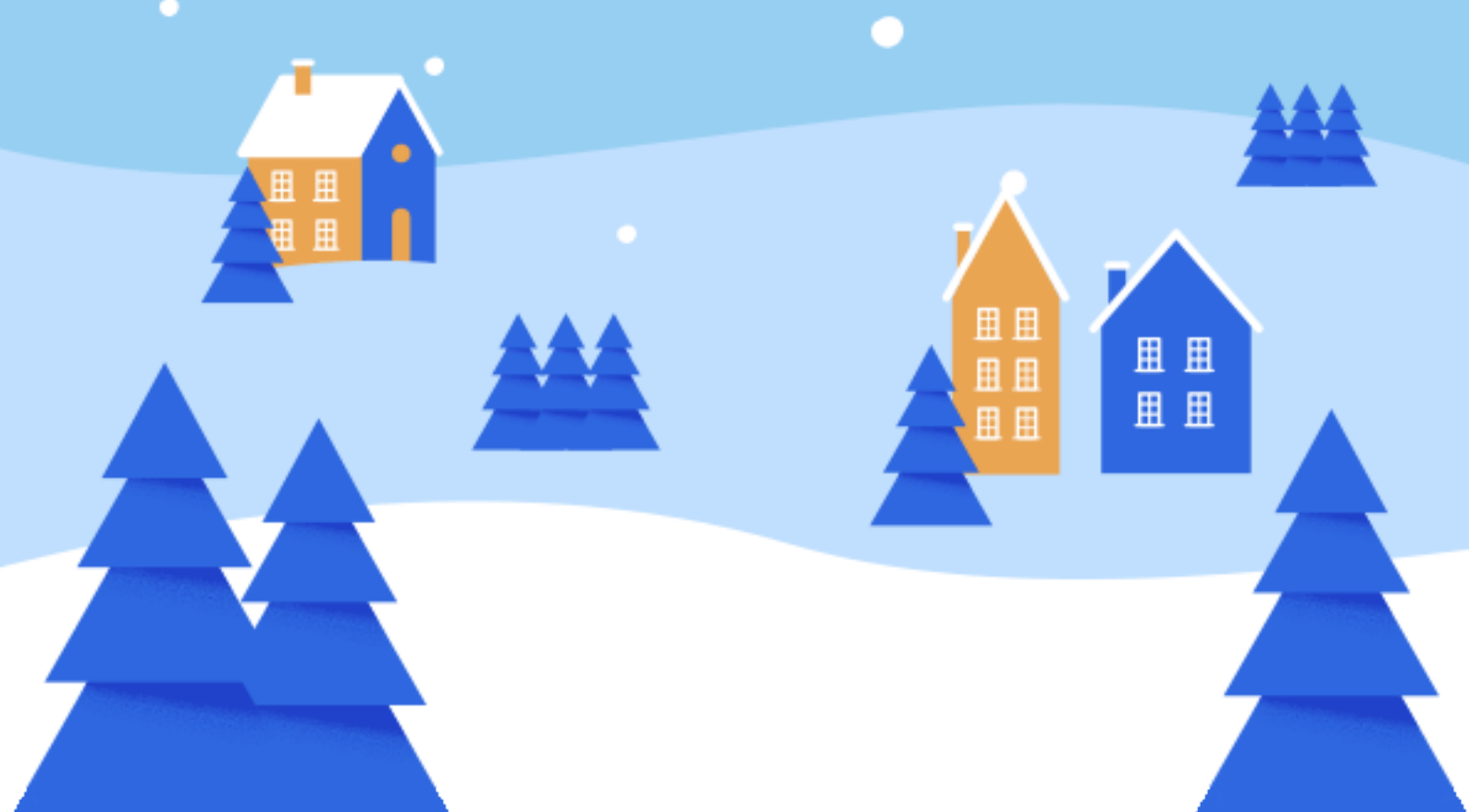
W święta „wszyscy wszystkim ślą życzenia” i na szczęście nie musimy już polegać tylko na papierowych kartkach. Dzięki komunikatorom internetowym i oprogramowaniu umożliwiającemu nawiązywanie rozmów wideo możemy być bliżej z przyjaciółmi i rodziną, nawet jeśli w rzeczywistości dzielą nas tysiące kilometrów.

Aby jednak kontakty te były bezpieczne, musicie pamiętać przede wszystkim o bieżącym aktualizowaniu komunikatorów zainstalowanych na komputerach, tabletach czy smartfonach. To kluczowe dla bezpieczeństwa połączenia, tak samo jak korzystanie jedynie z aplikacji udostępnionych do pobrania w oficjalnych źródłach.

Nie bez znaczenia jest także zasada ograniczonego zaufania: nie klikajcie bezrefleksyjnie we wszystkie linki, które dostaniecie w wiadomościach, uważajcie też na podejrzane załączniki i prośby o dołączenie do grona znajomych wysyłane przez obce osoby. W rozmowie przy użyciu komunikatorów nigdy nie podawajcie też poufnych informacji – danych osobowych, loginów i haseł, kodów BLIK czy numerów kont bankowych.

Prowadząc wideorozmowę, nie możecie zapominać o ochronie swojej prywatności. Zasłaniajcie obiektyw kamery, gdy jej nie używacie, a także sprawdzajcie… co macie za plecami. Usuńcie z tła wszystko, co może zawierać osobiste informacje. Pamiętajcie też o netykiecie!

Szczegółowe porady dotyczące komunikatorów i rozmów wideo znajdziecie w naszych aktualnościach na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: komunikatory internetowe” i „Bezpieczni w sieci z OSE: wideokonferencje”.



Lubimy uwieczniać wyjątkowe, świąteczne chwile na zdjęciach. Zanim jednak zdecydujecie się podzielić nimi w sieci, dwa razy się zastanówcie. Czy zdjęcie lub filmik przedstawiający Wasze dziecko go nie ośmiesza?

Sharenting – bo o nim mowa – to niebezpieczne zjawisko polegające na nieroztropnym dokumentowaniu życia swojego dziecka w internecie. Klikając „Udostępnij", musicie mieć świadomość, że pozornie niewinna fotka lub śmieszny filmik mogą niespodziewanie obiec internet, trafić w niepowołane ręce lub sprawić, że dziecko stanie się w przyszłości obiektem hejtu, a nawet ofiarą cyberprzemocy.

Warto wiedzieć, że materiały z wizerunkiem dziecka, upublicznione np. w mediach społecznościowych, często zdradzają więcej, niż powinny: są opatrywane komentarzami zawierającymi zbyt wiele szczegółów (takich jak imię dziecka, wiek, data urodzin czy nazwa jego szkoły lub przedszkola).

Czy to znaczy, że nie wolno dzielić się zdjęciami swoich dzieci w internecie? Można to robić, ale z głową, pamiętając, że w tym przypadku mniej znaczy więcej. Sprawdzajcie ustawienia prywatności i udostępniajcie materiały tylko znajomym, zrezygnujcie z publikowania zdjęć dzieci rozebranych do kąpieli lub umorusanych jedzeniem i za każdym razem zastanówcie się, czy jednym nieprzemyślanym postem nie skompromitujecie swojej pociechy – zarówno dziś, jak i za kilkanaście lat. A przede wszystkim: zawsze pytajcie o zgodę przed opublikowaniem zdjęcia czy filmiku! W ten sposób nauczycie dziecko, że ma prawo do prywatności i ochrony własnego wizerunku.

Więcej wskazówek znajdziecie w poradniku „Sharenting i wizerunek dziecka w sieci" i kursie e-learningowym „Sharenting. Czy warto mieć rodzinny album w sieci" dostępnych na platformie OSE IT Szkoła oraz aktualności na ose.gov.pl: „Dzielisz się zdjęciem dziecka w sieci? Rób to z głową!".

W święta chętniej niż zwykle dzielimy się z potrzebującymi tym, co mamy. Niestety – oszuści potrafią to wykorzystać… Uważajcie na naciągaczy i zawsze weryfikujcie organizatora zbiórki!

„Na leczenie", „na zwierzaka", „na Ukrainę" – to najczęstsze cele zbiórek, z jakimi mamy do czynienia w internecie. Jako społeczeństwo coraz bardziej angażujemy się w pomoc potrzebującym, musimy więc wiedzieć, że możemy natknąć się na oszustów.

Przestępcy grają na naszych emocjach i bez mrugnięcia okiem wykorzystują różne metody – wyszukują w internecie zdjęcia chorych dzieci i zwierząt, podrabiają dokumentację medyczną, w swoje zbiórki angażują celebrytów. Wszystko po to, by wyłudzić od nas pieniądze.

To oczywiście nie znaczy, że powinniśmy zrezygnować z udziału w akcjach charytatywnych! Jeżeli chcecie komuś pomóc, wybierajcie zaufane platformy organizujące zbiórki (tam również zdarzają się próby oszustw, jednak organizatorzy zrzutek są szczegółowo weryfikowani) oraz miejcie oczy i uszy szeroko otwarte. Sprawdzajcie, jak długo istnieje organizacja, która prowadzi zbiórkę, szukajcie jej regulaminu, terminu rozpoczęcia i zakończenia. Koniecznie zajrzyjcie też na stronę zbiorki.gov.pl, gdzie prowadzony jest rejestr zbiórek publicznych organizowanych na terenie kraju.

A może chcecie wrzucić pieniądze do puszki? Spójrzcie więc czujnie na osobę prowadzącą zbiórkę. Powinna być ona wyposażona w identyfikator zawierający imię i nazwisko, nazwę zbiórki, jej cel i numer, a także informacje o organizatorze.

Jeśli macie podejrzenia co do legalności jakiejś zbiórki pieniędzy, zgłoście tę sprawę na policję.

Chcecie kupić na prezent grę komputerową? Wybierzcie taką, która będzie odpowiednia dla Waszego dziecka. Kierujcie się oznaczeniami PEGI – znajdziecie je na pudełku.

Gry komputerowe mają wiele zalet: pomagają zdobywać praktyczne umiejętności, rozwijać zainteresowania, wzmacniać kompetencje społeczne, a także budować wieloletnie przyjaźnie. Zanim jednak zapakujecie grę w świąteczny papier i położycie ją pod choinkę, wybierzcie mądrze!

Polecamy kierowanie się wskazaniami ogólnoeuropejskiego systemu klasyfikacji gier PEGI (Pan-European Game Information). Trzeba pamiętać, że rating PEGI podaje jedynie informację, czy gra jest właściwa dla danego wieku, nie uwzględnia natomiast poziomu jej trudności – jako PEGI 3 może być oceniona np. trudna gra ekonomiczna, ponieważ nie zawiera treści nieodpowiednich dla dzieci.

Informacje o grze są w systemie PEGI podawane na dwa sposoby: w formie pięciu oznaczeń wiekowych (PEGI 3, PEGI 7, PEGI 12, PEGI 16 i PEGI 18) oraz ośmiu deskryptorów treści, czyli oznaczeń zawartości gry (Violence – sceny przemocy, Bad language – wulgaryzmy, Fear – obrazy lub dźwięki, które mogą przestraszyć dziecko, Gambling – elementy hazardowe, Sex – treści o charakterze seksualnym, Drugs – narkotyki i inne używki, Discrimination – stereotypy, In-game purchases – mikropłatności). Te pierwsze znajdują się na opakowaniu gry z obu stron, natomiast drugie – z tyłu pudełka.

Znajomość oznaczeń w systemie PEGI może pomóc w doborze gry odpowiedniej do wieku i możliwości poznawczych dziecka. To jednak nie wszystko! Aby czas spędzony z grą był bezpieczny, potrzebna jest także rozmowa z młodym graczem i wspólne ustalenie zasad.

Szczegółowe informacje znajdziecie w poradniku „Nastolatki i gry cyfrowe” oraz aktualnościach „Gra pod choinkę? Poradnik Świętego Mikołaja” i „Gry – dobra czy bezwartościowa rozrywka”. Pomocnych materiałów szukajcie na naszej platformie e-learningowej OSE IT Szkoła i na stronie ose.gov.pl.

Prezent na ostatnią chwilę? Uważajcie na wyjątkowe okazje i fałszywe sklepy internetowe. Jeśli coś wyda Wam się podejrzane, zróbcie zakupy gdzie indziej!

Polubiliśmy sklepy internetowe i często – zwłaszcza przed świętami – decydujemy się na zakupy online. Wygoda, oszczędność czasu, możliwość porównania wielu ofert, korzystne ceny… Same zalety? Niekoniecznie. Okazuje się bowiem, że kupując prezenty, możemy wpaść w sidła oszustów. Niestety o wielu pułapkach dowiemy się dopiero wtedy, gdy bez końca będziemy czekać na zamówioną paczkę lub gdy jej zawartość będzie bardzo różnić się od oczekiwanej.

Tak jak w przypadku innych zagrożeń w sieci zbawienny okaże się zdrowy rozsądek. Niech nie zwiodą Was „wyjątkowe oferty dostępne tylko dziś", „megarabaty" i przeceny na cały asortyment sklepu! Zanim wrzucicie coś do internetowego koszyka, poszukajcie podstawowych informacji na stronie sklepu: danych kontaktowych (w tym formularza), numeru NIP i numeru wpisu do Krajowego Rejestru Sądowego (KRS), a także regulaminu, informacji o sposobach dostawy, formach płatności czy warunkach zwrotu towaru. Przed dokonaniem zakupu zapoznajcie się też z opiniami na temat sklepu i sprzedawcy. Waszą czujność powinny wzbudzić wyłącznie pozytywne oceny dodane w podobnym okresie.

Gdy podejmiecie już decyzję i przejdziecie do strony płatności, sprawdźcie wszystko dwa razy. Jeśli zauważyliście literówki (np. w adresie) lub cokolwiek wzbudzi Wasze podejrzenia – czym prędzej zrezygnujcie z transakcji.

Zakupy w fałszywym sklepie możecie zgłosić na stronie incydent.cert.pl oraz na policji, poinformujcie o tym też swój bank. Jeśli za swoje zakupy zapłaciliście kartą, możecie łatwo odzyskać swoje pieniądze, korzystając z mechanizmu tzw. obciążenia zwrotnego (chargeback).

Szczegółowe porady, dzięki którym nie kupicie kota w worku, znajdziecie w aktualnościach na stronie ose.gov.pl: „Poradnik mikołajkowy – fałszywe sklepy online" oraz „Bezpieczni w sieci z OSE: uwaga na okazje w Black Friday".

W Święta warto zadać o higienę cyfrową – całą rodziną! Ustalcie zasady używania telefonów i internetu (np. nie korzystamy z telefonu przy stole, odkładamy urządzenia co najmniej godzinę przed snem) i wspólnie ich przestrzegajcie.

Każdy moment na zadbanie o równowagę online–offline jest dobry, jednak Gwiazdka wydaje się jedną z najlepszych okazji do wdrożenia zdrowych cyfrowych nawyków. Zupełne odłączenie się od naszych urządzeń jest niemożliwe (a nawet niewskazane, bo w sieci zaspokajamy przecież wiele swoich potrzeb), ale co powiecie na nieco odświeżone zasady korzystania z internetu? W końcu: nowy rok – nowi my!

Przede wszystkim reguły powinniście ustalić razem i dostosować je do wieku i potrzeb każdego z domowników. Mają one być pierwszym krokiem do zmiany, a nie trudnym, zniechęcającym doświadczeniem.

Na początek pomyślcie o określeniu limitu czasu, jaki można spędzać przed ekranem urządzenia. Wiedzieliście, że dzieci do drugiego roku życia w ogóle nie powinny mieć kontaktu z cyfrowymi sprzętami, a maluchy w wieku 2–5 lat mogą patrzeć w ekran maksymalnie godzinę dziennie?

Wyznaczcie też w domu jedno miejsce na odkładanie i ładowanie urządzeń. Umówcie się, że nie będziecie korzystać z ekranów zaraz po przebudzeniu, i spróbujecie wyzbyć się nawyku noszenia telefonu zawsze przy sobie. Postarajcie się odkładać urządzenia na czas posiłków, spotkań z bliskimi oraz co najmniej godzinę przed snem. Zaoszczędzony czas możecie spędzić całą rodziną np. na jakiejś aktywności na świeżym powietrzu lub zabawie offline!

O zaletach utrzymywania równowagi między aktywnościami w sieci i poza nią przeczytacie w aktualnościach na stronie ose.gov.pl: „Za dużo urządzeń? Wprowadź domowe zasady ekranowe”, „Kary i nagrody? Postaw na zasady”, „Cyfrowe nawyki u dzieci – to nasza wspólna sprawa”.

Kupując dziecku pod choinkę cyfrowy prezent, dobrze go przygotujcie. Przyda się aplikacja ochrony rodzicielskiej OSE mOchrona, która pomoże zadbać o bezpieczeństwo dziecka w sieci.

Po pierwsze – zastanówcie się, które urządzenie będzie dla dziecka najlepsze: jakie korzyści mu przyniesie oraz na co trzeba uważać. Po drugie – zadbajcie o odpowiednie zabezpieczenie sprzętu. Wybierzcie i zainstalujcie program antywirusowy, którego zadaniem będzie skanowanie, wykrywanie, rozpoznawanie oraz usuwanie z urządzenia złośliwego oprogramowania. Postawcie na narzędzie pochodzące od znanego producenta lub z zaufanego źródła! Nie zapomnijcie też o aktualizacjach systemowych, które pozwolą na sprawne korzystanie z telefonu, tabletu czy laptopa, a także na skuteczniejszą ochronę przed zagrożeniami w sieci.

Ostatnim (ale nie mniej ważnym!) elementem będzie też zainstalowanie naszej bezpłatnej aplikacji ochrony rodzicielskiej mOchrona. Dlaczego warto? Apka pomoże Wam zapewnić dzieciom bezpieczeństwo w internecie oraz szybko reagować na trudne sytuacje (za sprawą przycisku S.O.S.). mOchrona wspiera też w ustaleniu reguł dotyczących korzystania z urządzeń cyfrowych – dzięki niej możecie zobaczyć szczegółowe informacje na temat aktywności dziecka w internecie, sprawdzicie, ile czasu przeznacza np. na portale społecznościowe i gry, a także zablokujecie strony zawierające szkodliwe treści.

Aplikacja działa poprzez połączenie (sparowanie) urządzeń rodzica i dziecka, a co najważniejsze: jest intuicyjna i łatwa w obsłudze.

Aplikacja mOchrona jest dostępna w oficjalnych sklepach z aplikacjami na urządzenia mobilne (Google Play, App Store, App Gallery), a także w wersji dla systemu Windows. Więcej informacji o naszej apce znajdziecie na stronie ose.gov.pl w zakładce mOchrona.

O cyfrowych prezentach choinkowych przeczytacie więcej w aktualnościach „Planujesz cyfrowy prezent? Zadbaj o jego bezpieczeństwo!” i „Smartzabawki i urządzenia cyfrowe dla dziecka. Jak mądrze wybrać prezent pod choinkę?” na stronie ose.gov.pl.

Podróżujecie do domu na święta? Uważajcie na otwarte sieci Wi-Fi na lotniskach i w hotelach. Traktujcie je zawsze jako niezaufane!

W przedświątecznym rozgardiaszu mamy sporo na głowie i niejednokrotnie ważne sprawy załatwiamy w ostatniej chwili. Być może w drodze do rodzinnego domu – na lotnisku, dworcu, w restauracji czy hotelu – przypomnimy sobie o niezapłaconych rachunkach czy ostatnim pilnym mailu… Na szczęście będziemy mieć ze sobą smartfon lub laptop, do szczęścia wystarczy więc już tylko połączenie z internetem. Czy możemy bez obaw skorzystać z publicznej sieci Wi-Fi? Niestety nie!

Za każdym razem, gdy korzystacie z niezabezpieczonego dostępu do internetu (a więc z otwartych sieci), musicie wzmóc czujność. Wybierajcie tylko przeznaczone do tego aplikacje i na zakończenie zawsze rozłączajcie się z siecią. Unikajcie też logowania się do swojej skrzynki pocztowej czy bankowości elektronicznej i pod żadnym pozorem nie podawajcie swoich danych, takich jak loginy i hasła. Jeżeli macie taką możliwość, korzystajcie wyłącznie z pakietu danych mobilnych dostarczanego przez Waszego operatora komórkowego.

Pamiętajcie też o zawsze aktualnych zasadach cyberhigieny: nie klikajcie w nieznane linki, nie otwierajcie niespodziewanych załączników, zwracajcie uwagę, czy znajdujecie się na prawdziwych stronach logowania.

Więcej porad opisaliśmy w aktualności „Bezpieczni w sieci z OSE na wakacje: korzystanie z Wi-Fi” na stronie ose.gov.pl.

Święta to czas, który warto spędzić offline – z bliskimi. Odłóżcie telefon, wyłączcie internet i cieszcie się świąteczną atmosferą!

Sianko pod białym obrusem, rozświetlona choinka, kolędy, 12 wigilijnych potraw: wszyscy znamy gwiazdkowe tradycje. Proponujemy – w tym i każdym kolejnym roku – dołączyć do nich jeszcze jeden zwyczaj, a mianowicie świąteczny offline challenge.

Zasada tego wyzwania jest jedna: odłączamy się od sieci na 48 godzin. Dwie dobry spędzone bez dostępu do internetu pomogą Wam pobyć ze sobą i swoimi bliskimi, a przecież o to tak naprawdę chodzi w świętach. Przyjrzycie się też swoim cyfrowym nawykom i sprawdzicie, jak bardzo na co dzień pochłania Was wirtualna rzeczywistość.

Być może nie będzie łatwo, zwłaszcza jeśli nie wyobrażacie sobie dnia bez zostawiania lajków, scrollowania mediów społecznościowych czy przeglądania filmików na TikToku. Postawcie na małe kroki. Zastanówcie się, co dało Wam odłączenie od internetu i smartfona. Może znaleźliście więcej czasu na swoje hobby, może lepiej spaliście, a może w pewnym momencie musieliście się poddać?

Cyfrowy detoks od czasu do czasu przyda się każdemu. Szybko przekonacie się, że można cieszyć się czasem spędzanym offline (JOMO, ang. Joy of Missing Out), zwłaszcza we wspaniałej, świątecznej aurze.

Jak podjąć wyzwanie? Przeczytajcie nasze aktualności na stronie ose.gov.pl: „Bezpieczni w sieci z OSE na wakacje: offline challenge” i „#offlinechallenge – czas na JOMO”.

Treść: Katarzyna Gańko
Projekt graficzny, skład: Aneta Witecka

NASK – Państwowy Instytut Badawczy
ul. Kolska 12
01-045 Warszawa

Rzeczpospolita Polska

OGÓLNOPOLSKA SIEĆ EDUKACYJNA

NASK