Dzień Bezpiecznego Internetu

W każdy drugi wtorek lutego obchodzimy Dzień Bezpiecznego Internetu, którego celem jest promowanie bezpiecznego i odpowiedzialnego korzystania z Internetu. Dzień Bezpiecznego Internetu (DBI) został ustanowiony w 2004 roku z inicjatywy Komisji Europejskiej. W Polsce organizatorem tego wydarzenia jest Polskie Centrum Programu Safer Internet, które tworzą dwie organizacje – instytut badawczy NASK i Fundacja Dajemy Dzieciom Siłę.

Szanuj swoją prywatność

Większość odwiedzających stron, aplikacji i urządzeń zbiera nasze dane – to właśnie one sprawiają, że korzystanie z nich jest darmowe. Ceną jest nasza prywatność – nasze dane są sprzedawane i wykorzystywane np. do wyświetlania i spersonalizowania reklam. Coraz częściej możemy spotkać się z aplikacjami i rozwiązaniami, które mogą zwiększyć naszą prywatność. Osoby dbające o nią mogą korzystać z alternatywnych wyszukiwarek i aplikacji, które nie gromadzą danych użytkownika.

Chroń swoje dane

Nigdy nie podawaj w internecie swojego imienia i nazwiska – zamiast nich używaj nicku, którego nie będzie można w łatwy sposób z Tobą powiązać.

Nigdy też nie udostępniaj innym osobom poniższych danych:

- adresu
- numeru telefonu,
- PESEL – u
- danych z dowodu,
- osobistych informacji, np. imiona rodziców.

Wyszukiwarki

Wyszukiwarka Google, podobnie jak wiele innych wyszukiwarek internetowych, gromadzi dane użytkowników w celu personalizacji wyników wyszukiwania, poprawy jakości usług wyświetlania spersonalizowanych reklam. Chcąc zadbać o prywatność i nasze dane, możemy skorzystać z alternatywnych wyszukiwarek internetowych, które nie zbierają danych swoich użytkowników np. DuckDuckGo.

Tryb prywatny

Wiele przeglądarek ma wbudowany tryb prywatny lub incognito, który pozwala przeglądać Internet bez zostawiania „śladu” – niezapisywane są wtedy ciasteczka (cookies).Podczas użytkowania tego trybu nie zapisuje się także historia przeglądania. Tryb prywatny nie zapewnia prywatności ani większego bezpieczeństwa w sieci!. Dostawca Internetu wciąż otrzymuje pełną wiedzę o przeglądanych stronach. Tryb Incognito zapewnia jedynie prywatność przed innymi użytkownikami tego samego urządzenia!.

Szukaj kłódki

Przed wpisaniem swoich danych na stronie zawsze sprawdź „kłódki” przy adresie strony. Pokazuje ona, czy strona posiada certyfikat HTTPS, gwarantujący bezpieczne połączenie. Nawet przy certyfikacie HTTPS twoje dane wciąż mogą trafić w niepowołane ręce, jeżeli strona prowadzona jest przez przestępców.

Najlepszy antywirus

„Najlepszy antywirus znajduje się między klawiaturą a krzesłem”.
To popularne w środowisku cyberbezpieczeństwa powiedzenie odnosi się oczywiście do użytkownika urządzenia, który jest często najlepszym ogniwem bezpieczeństwa. Żadne oprogramowanie nie będzie w stanie uchronić naszego urządzenia, jeżeli będziemy korzystać z niego nierozważnie. Przeciętny użytkownik nie ma potrzeby instalowania antywirusa – wbudowane w system zabezpieczenia są wystarczające.

Silne hasła

Każdy użytkownik Internetu powinien stosować silne hasła. Zwiększają one bezpieczeństwo, jak i prywatność – chronią nasze konta przed przejęciem przez inne osoby. Cechami silnych haseł są:

- długość – im dłuższe, tym trudniejsze do złamania,
- różnorodność znaków – powinno zawierać kombinację liter, cyfr i symboli,
- brak oczywistych informacji – nie powinno być oparte na danych osobistych,
- unikalność – każde konto powinno mieć własne, niepowtarzalne hasło.

Weryfikacja dwuetapowa

Weryfikacja dwuetapowa jest dodatkowym zabezpieczeniem naszego konta. Zwiększa bezpieczeństwo poprzez wymóg potwierdzenia logowania na innych

urządzeniach lub koncie. Jeżeli strona lub aplikacja pozwala na użycie weryfikacji dwuetapowej, to zawsze powinniśmy z niej skorzystać! Znacząco zwiększa to bezpieczeństwo naszego konta – znajomość hasła nie pozwoli na przejęcie konta.

Wirtualna sieć prywatna

VPN, czyli wirtualna sieć prywatna, jest często polecana w celu ochrony naszej prywatności. Jej użycie sprawia, że nasz dostawca Internetu nie wie jakie strony odwiedzamy. VPN szyfruje dane, co może zwiększyć bezpieczeństwo użytkownika. Komercyjne VPN nie gwarantuje pełnej prywatności!. Ukrywa nasze dane tylko przed dostawcą Internetu – lecz dostawca VPN otrzymuje informację o odwiedzanych przez nasz stronach.

Nie ufaj bezgraniczne

Influencerzy, youtuberzy i streamerzy nie są Twoimi przyjaciółmi!. Polecane przez nie aplikacje, urządzenia lub usługi mogą być szkodliwe – zarówno dla Twojej prywatności, jak i niekiedy zdrowia. Wiele osób w Internecie poleca produkty bez ich sprawdzenia lub pomijając ich wady. Często otrzymują za to pieniądze od sponsora, więc wypowiadają się o nich wyłącznie pozytywnie.

Nic za darmo

Nie wszystko w życiu można otrzymać za darmo – szczególnie w Internecie. Jeżeli coś jest darmowe, to najczęściej płaci się swoim czasem lub danymi. Coraz częściej można spotkać się także z oszustwami, związanymi z obietnicą bezpłatnego dostępu do normalnie płatnych usług. Jedną z popularniejszych oszustw są te dotyczące walut premium. Najczęściej oszustwo polega na zalogowaniu się na fałszywą stronę lub wypełnianiu ankiet – zarabia na nich oszust, a poszkodowany nigdy nie otrzymuje waluty premium.

Sprawdź dwa razy

Jednym z częstych oszustw w Internecie jest podszywanie się, wykorzystując przejęte konta lub adresy e – mail. Jeżeli znana ci osoba prosi o coś nietypowego – pożyczenie pieniędzy, dostęp do konta – zweryfikuj prośbę inną metodą komunikacji. Administratorzy, moderatorzy lub właściciele stron banków NIGDY nie będą prosić o Twoje dane do logowania. Taka prośba jest próbą przejęcia Twojego konta. Nie próbuj także logować się na strony używając linków w wiadomościach – zawsze ręcznie wpisuj adresy z witryny.

Dezinformacja

W ostatnich latach coraz częściej spotykamy się z dezinformacją (tzw. *fake news*). Są to informacje, które nie pochodzą ze sprawdzonych źródeł lub w ogóle nie są oparte na faktach!. Mają one na celu wprowadzenie czytelnika w błąd lub wywołanie kontrowersji.
Dezinformacja często wywołuje nienawiść do danej grupy osób. Zawsze powinniśmy weryfikować informacje, korzystając z kilku niezależnych od siebie źródeł.

Mowa nienawiści

Bezpieczeństwo w sieci nie dotyczy tylko naszych kont, ale także naszego zdrowia. Coraz częściej w Internecie możemy spotkać się z cyberprzemocą i mową nienawiści. Osoby, które są jej celem niekiedy doświadczają długotrwałych skutków – wywołany stres wpływa negatywnie na zdrowie psychiczne i obniża samoocenę. W 2023 roku aż 38 procent polskich uczniów doświadczyło przemocy internetowej.

Szanuj innych

Nie musimy się zgadzać z każdą opinią i na nią odpowiadać. Odmienne zdanie nie jest także przyzwoleniem na atakowanie drugiej osoby – rozmówcę zawsze powinniśmy traktować z szacunkiem. Nie odpowiadaj na wiadomości i posty nawołujące do nienawiści, hejtu lub agresji – autorom tych treści zależy na uwadze i interakcji. Zgłoś te treści administratorowi!.

Nie ignoruj!

Każdy z nas może przyczynić się do bezpiecznego Internetu – wystarczy reagować i zgłaszać przypadki oszustw, niebezpieczeństw i cyberprzemocy. Obecnie prawie w każdej witrynie, mediach społecznościowych i komunikatorach istnieje opcja zgłaszania wiadomości lub postu. Pozwala to usuwać niewłaściwe treści, które mogą wprowadzić innych w błąd lub doprowadzić do utraty danych.