

PORADNIK CYBERBEZPIECZEŃSTWA

Doniesienia o nowych atakach hakerskich, wyciekach danych i milionowych stratach ponoszonych przez firmy pojawiają się niemal codziennie. Myślisz, że w obliczu tych zjawisk nie jesteś w stanie opanować cyfrowego chaosu i zabezpieczyć swoich wrażliwych danych? Zastanawiasz się, jak chronić się przed zagrożeniami płynącymi z sieci? Zapoznaj się z naszymi poradami i sprawdź, jak bezpiecznie korzystać z internetu.

Co to jest cyberbezpieczeństwo?

Cyfryzacja to powszechne zjawisko – obecnie już **5 mld osób na świecie korzysta z internetu**. Cyberprzestrzeń stała się więc naszym drugim domem. O ile jednak w realnym świecie zabezpieczamy swoje mieszkanie, inwestujemy w nowoczesne drzwi i okna antywłamaniowe, wreszcie – chronimy swoje pieniądze i dane osobowe, o tyle w sieci często zapominamy o podobnych środkach ostrożności lub po prostu nie wiemy, jak bezpiecznie korzystać z internetu.

Dlatego też zarówno dla państw i firm, jak i dla zwykłych użytkowników priorytetem powinno stać się **cyberbezpieczeństwo**. Co to takiego jest? Pojęcie to dotyczy technologii, praktyk i procesów, które zostały stworzone, żeby **chronić sieci informatyczne, dane i programy przed uszkodzeniami, nieautoryzowanym dostępem, a także atakami hakerskimi**.

Na początku lutego obchodzimy **Dzień Bezpiecznego Internetu**, jednak nie tylko tego dnia powinniśmy dbać o bezpieczeństwo w sieci.

Warto o nim pamiętać stale i wypracować sobie pewne **dobre nawyki**. Stosowanie zasad bezpiecznego korzystania z internetu przedstawionych w naszym kompendium pozwoli Ci bowiem uniknąć najczęstszych zagrożeń w cyberprzestrzeni.

Jak tworzyć silne hasła, które zwiększą cyberbezpieczeństwo?

Przeciętny użytkownik posiada dziesiątki kont stworzonych w internecie, np. konto w banku, profile w mediach społecznościowych i na forach tematycznych czy kilka skrzynek pocztowych. Do wszystkich kont powinny być przypisane długie, skomplikowane hasła. Niestety, statystyki pokazują, że wciąż najpopularniejsze są słabe hasła, których odgadnięcie zajmuje hakerom kilka minut.

Najpopularniejsze hasła na świecie:

- 123456,
- 123456789,
- Qwerty,
- password,
- 111111.

Jak jednak pogodzić bezpieczeństwo informacyjne z wygodą? Odpowiedz sobie na pytanie, które konta są dla Ciebie najważniejsze i zasługują na silne hasła. **Długie i skomplikowane hasła** dadzą Ci pewność, że Twoje pieniądze są bezpieczne w banku i nikt nie wejdzie w posiadanie Twoich danych na Facebooku.

Pomocnym narzędziem przy tworzeniu haseł jest **manager haseł** – program pozwala zapisać wszystkie hasła w jednym miejscu. Wystarczy zapamiętać jedno długie hasło do tego programu.

Według badań przeprowadzonych przez firmę Hivesystems, zajmującej się cyberbezpieczeństwem, standardowe, **8-znakowe oraz złożone z cyfr, wielkich i małych liter oraz znaków specjalnych hasła** hakerzy **mogą złamać w ciągu zaledwie ok. 5 godzin!** To wystarczający powód, aby włączyć **dwustopniową weryfikację** praktycznie w każdym serwisie, w którym jest to możliwe – szczególnie w przypadku poczty lub Facebooka.

Uruchomienie tego rozwiązania kolejny krok w kierunku bezpiecznego internetu. Spowoduje on, że haker, któremu uda się poznać login i hasło, nie zaloguje się na Twoje konto, ponieważ zabraknie mu jednego bardzo ważnego elementu: kodu wysłanego SMS-em na Twój numer telefonu.

Bezpieczny smartfon – internet mobilny w telefonie

Niemal 97% Polaków używa smartfonów – wynika z „*Badania opinii publicznej w zakresie funkcjonowania rynku usług telekomunikacyjnych oraz preferencji konsumentów*” przeprowadzonego przez UKE w listopadzie 2021 roku. Obecnie telefony stanowią podstawową bazę danych o Tobie – również tych wrażliwych. Smartfony wykorzystuje się m.in. do:

- zarządzania finansami,
- komunikowania się z rodziną i przyjaciółmi,
- korzystania z mediów społecznościowych.

Smartfony można porównać do sejfów, w którym przechowujesz najważniejsze informacje oraz pieniądze. Problem w tym, że sejf jest wyposażony w szereg zaawansowanych zabezpieczeń, których większość smartfonów jest pozbawiona. Utrata takiego urządzenia to ogromne zagrożenie.

„Ludzki firewall”, czyli zasady bezpiecznego korzystania z internetu

Podczas korzystania z internetu warto kierować się brakiem zaufania i **wzmocną ostrożnością**. Nie traktuj tej przestrzeni jako w pełni przyjaznej. Bezpieczne poruszanie się w wirtualnej rzeczywistości można sprowadzić do kilku podstawowych zasad.

- Zainstaluj oprogramowanie antywirusowe.
- Twórz silne hasła do kont w internecie.
- Pamiętaj o aktualizacji oryginalnego oprogramowania.
- Nie klikaj w linki pochodzące od nieznanymi osób.

- Nie otwieraj załączników z e-maili pochodzących z niezweryfikowanych źródeł.
- Nie lekceważ komunikatów Google, że dana witryna może być niebezpieczna.
- Korzystaj z weryfikacji dwuetapowej, czyli dwukrotnego uwierzytelnienia najpierw hasłem, a następnie kodem otrzymanym w SMS-ie.

Bezpieczny internet – może być taki, jeśli będziesz przestrzegać tych prostych zasad.