POLSKA PARTIA PIRATÓW

ZACHOWAJ BEZPIECZEŃSTWO W SIECI!

Istnieje kilka ważnych kroków, które warto podjąć aby zachować bezpieczeństwo w sieci. Przedstawiamy kilka podstawowych zasad.:

AKTUALIZACJE OPROGRAMOWANIA

Regularnie aktualizuj system operacyjny i wszystkie zainstalowane programy, w tym przeglądarkę internetową.

Aktualizacje zawierają poprawki zabezpieczeń, które pomagają chronić Twoje urządzenie przed zagrożeniami.

BEZPIECZNE HASŁA

Używaj silnych, unikalnych haseł do swoich kont online. Hasła powinny zawierać kombinację liter, cyfr i znaków specjalnych. Unikaj prostych haseł, takich jak „123456” czy „password”.

Dodatkowo, warto korzystać z menedżera haseł, który pomoże Ci zarządzać i generować bezpieczne hasła.

ANTYWIRUS I FIREWALL

Zainstaluj i regularnie aktualizuj oprogramowanie antywirusowe na Swoim urządzeniu oraz zapory sieciowe (firewall). To pomoże w blokowaniu niebezpiecznych plików i prób nieautoryzowanego dostępu do Twojego sprzętu.

OSTROŻNOŚĆ W MEDIACH SPOŁECZNOŚCIOWYCH

Uważaj, co udostępniasz na portalach społecznościowych. Nie publikuj prywatnych informacji, takich jak adres zamieszkania czy numer telefonu. Ustaw również odpowiednie ustawienia prywatności, aby kontrolować, kto może widzieć Twoje dane.

Nie chwal się w mediach społecznościowych o tym, że nie ma Ciebie w domu – to pozwoli również ochronić Twój majątek od kradzieży.

VPN

Ostrożnie korzystaj z publicznych sieci Wi-Fi. Unikaj przesyłania poufnych informacji, takich jak hasła do kont bankowych, gdy korzystasz z niezabezpieczonej sieci.

W tym pomoże Tobie VPN, czyli wirtualna sieć prywatna, to bezpieczny tunel, za pomocą którego Twoje urządzenie ustanawia połączenie z Internetem.

KOPIA ZAPASOWA

Robienie kopii zapasowych jest kluczowym elementem praktyk bezpieczeństwa w sieci.

Twoich danych przed przypadkową utratą lub uszkodzeniem. W przypadku awarii sprzętu, ataku hakerskiego, błędu użytkownika lub innego nieprzewidzianego zdarzenia, możesz stracić cenne pliki i informacje. Wykonując regularne kopie zapasowe, masz możliwość przywrócenia utraconych danych i minimalizowania strat.

Fajną opcją jest usługa One Drive dla systemu Windows 11 – gdzie kopia zapasowa jest tworzona automatycznie i daje dobrą ochronę przed oprogramowaniem wymuszającym okup.

Kolejną ciekawą opcją jest icloud dla urządzeń od Apple jako usługa do tworzenia kopii zapasowej w celu ochrony naszych danych.

Wiele urządzeń pozwala na tworzenie kopii zapasowych na fizycznych dyskach zewnętrznych.

NIEZNANE LINKI I ZAŁĄCZNIKI

Nie otwieraj podejrzanych linków ani nie pobieraj nieznanych załączników. Mogą one zawierać złośliwe oprogramowanie, które zagraża Twojemu komputerowi i prywatności.

MONITOROWANIE SWOJEGO KONTA

Regularnie sprawdzaj swoje konta online, takie jak poczta e-mail, konta bankowe czy media społecznościowe. W przypadku wykrycia podejrzanej aktywności lub nieautoryzowanego dostępu, natychmiast podjęcie odpowiednich kroków, takich jak zmiana hasła i powiadomienie odpowiednich służb.

EDUKACJA

Pozostań na bieżąco z najnowszymi zagrożeniami w sieci i zwiększaj swoją świadomość na temat bezpieczeństwa online. Czytaj wiarygodne źródła informacji na ten temat jak: niebezpiecznik.pl

Pamiętaj, że bezpieczeństwo w sieci to nie tylko kwestia techniczna, ale także świadomość i odpowiednie zachowanie. Bądź ostrożny podczas udostępniania swoich danych osobowych, korzystaj z silnych haseł, nie klikaj na podejrzane linki i dbaj o ochronę swojego urządzenia przed złośliwym oprogramowaniem.