STÓJ | POMYŚL | POŁĄCZ

DOBRE PRAKTYKI

ZADBAJ O AKTUALIZACJE I BEZPIECZEŃSTWO URZĄDZEŃ

- **Korzystaj z aktualnego oprogramowania:** Regularnie aktualizuj system operacyjny, program antywirusowy, przeglądarkę internetową. Dzięki aktualizacjom łatwiej ustrzeżesz się przed szkodliwym oprogramowaniem i innymi zagrożeniami obecnymi w sieci.
- **Włącz aktualizacje automatyczne:** Wiele aplikacji oferuje możliwość automatycznego pobierania aktualizacji, w celu ochrony przed nowymi zagrożeniami. Skorzystaj z tego rozwiązania wszędzie tam, gdzie to możliwe.
- **Chroń urządzenia podłączane do sieci:** Nie tylko komputery, ale także smartfony, tablety i inne podłączane do Internetu urządzenia, potrzebują ochrony przed wirusami i złośliwym oprogramowaniem.
- **Skanuj przed użyciem:** Nie podłączaj do komputera nośników, których pochodzenie nie jest Ci znane. Dyski zewnętrzne, pendrive'y, czy inne nośniki danych mogą być niebezpieczne (zainfekowane przez szkodliwe oprogramowanie). Zanim otworzysz ich zawartość skorzystaj ze skanera antywirusowego.

ZABEZPIECZ DOSTĘP DO POSIADANYCH INFORMACJI

- **Dwuskładnikowe uwierzytelnianie:** Zadbaj o swoje konta w sieci. Logowanie oparte wyłącznie o nazwę użytkownika i hasło nie jest wystarczająco bezpieczne (szczególnie w przypadku konta e-mail, portalu społecznościowego czy bankowości internetowej). Aktywuj weryfikację tożsamości opartą o dodatkowy składnik, np. kod SMS, token, czy klucz sprzętowy.
- **Stwórz mocne hasło:** Dobre hasło składa się przynajmniej z 12 znaków. Skup się na pozytywnych zdaniach lub zwrotach o których lubisz myśleć i które łatwo zapamiętasz (np. „Kocham miasto muzyki"). Na wielu stronach internetowych, możesz przy wprowadzaniu hasła używać spacji.
- **Jedno hasło, jedno konto:** Jeżeli chcesz utrudnić działania przestępcom, dla każdego konta przypisz oddzielne hasło. Niezbędne minimum, to rozdzielenie kont używanych do pracy i celów prywatnych. Zadbaj o silne hasło do najistotniejszych serwisów (bankowość, poczta elektroniczna, portale społecznościowe).
- **Przechowuj bezpiecznie:** Każdy może zapomnieć swojego hasła. W celu ułatwienia nam życia stworzono aplikacje zwane menadżerami haseł. Służą do bezpiecznego przechowywania danych dostępowych. Możesz z nich korzystać. Jeżeli zapisałeś hasło na kartce (lepiej tego nie rób), postaraj się umieścić ją w bezpiecznym miejscu, z dala od komputera.

STÓJ | POMYŚL | POŁĄCZ

DOBRE PRAKTYKI

KORZYSTAJ ROZWAŻNIE

Zatrzymaj się, jeśli masz wątpliwości: Linki i załączniki w wiadomościach e-mail, spreparowane posty w mediach społecznościowych oraz reklamy - to częste metody używane przez przestępców w celu kradzieży danych. Jeżeli wydają Ci się podejrzane, po prostu je zignoruj. Nawet, jeżeli źródło wygląda na zaufane.

Uważaj na hotspoty Wi-Fi: Ogranicz aktywność w publicznie dostępnych sieciach Wi-Fi. Używając poza domem kluczowych serwisów (poczta e-mail, bankowość internetowa, portale społecznościowe) bezpieczniej będzie użyć własnego modemu LTE lub połączenia VPN. Pamiętaj o wyłączaniu transmisji Wi-Fi i Bluetooth, kiedy z niej nie korzystasz.

Chroń swoje finanse: Korzystając z bankowości internetowej i sklepów online, upewnij się, że połączenie jest objęte szyfrowaniem (zielona kłódka oraz prefiks „https://" w pasku adresu). Odczytując kod SMS uwierzytelniający transakcję, zweryfikuj kwotę przelewu i numer rachunku odbiorcy!

BĄDŹ ŚWIADOMYM UŻYTKOWNIKIEM

Pozostań na bieżąco: Nie lekceważ informacji ze świata bezpieczeństwa IT. Jeśli coś podawane jest do publicznej wiadomości, najczęściej dotyczy także Ciebie.

Pomyśl, zanim zadziałasz: Bądź ostrożny wobec korespondencji zachęcającej do natychmiastowych działań. Szczególnie, jeśli ktoś oferuje Ci łatwy zysk lub próbuje nakłonić do podania prywatnych danych. Robiąc zakupy w sieci, weryfikuj reputacje sklepów. Dziel się wiedzą z rodziną i znajomymi.

Zadbaj o kopie zapasowe: Zabezpiecz efekty swojej pracy, muzykę, zdjęcia, cenne dokumenty. Twórz kopie zapasowe i przechowuj je w bezpiecznym miejscu.

STÓJ | POMYŚL | POŁĄCZ

DOBRE PRAKTYKI

CHROŃ SWOJĄ PRYWATNOŚĆ

Informacje mają wartość: Dane na Twój temat, takie jak historia zakupów czy historia lokalizacji są cenne. Zwracaj uwagę kto i co (aplikacje, strony internetowe) próbuje uzyskać do nich dostęp.

Dostosuj ustawienia prywatności w serwisach online i na urządzeniach: Dzięki nim, możesz lepiej chronić Twoje dane. Sam decyduj, jak wiele informacji na swój temat chcesz udostępnić innym.

Pomyśl, zanim udostępnisz: Zwracaj uwagę na przesyłaną do sieci treść, zasięg komunikatu, a także sposób, w jaki może zostać odebrany.

TWÓRZ KULTURĘ BEZPIECZNEJ SIECI

Twoje zachowanie w sieci ma znaczenie: Stosowanie dobrych praktyk buduje kulturę bezpiecznej sieci. To, co robisz, ma znaczenie (w domu, w pracy, gdziekolwiek jesteś).

Traktuj innych tak, jak sam chciałbyś być traktowany.

Wspieraj walkę z cyberprzestępczością: Jeżeli zaobserwujesz niepokojące zjawiska, nie wahaj się o tym poinformować: https://incydent.cert.pl (zgłaszanie incydentów naruszających bezpieczeństwo w sieci) https://dyzurnet.pl (przyjmowanie zgłoszeń dotyczących nielegalnych treści w Internecie).

Odwiedź https://stojpomyslpolacz.pl i dowiedz się więcej.