STÓJ | POMYŚL | POŁĄCZ

## ZADBAJ O AKTUALNOŚĆ SYSTEMU OPERACYJNEGO I BEZPIECZEŃSTWO TWOICH URZĄDZEŃ

- **Korzystaj z aktualnego oprogramowania:** Regularnie aktualizuj program antywirusowy, przeglądarkę internetową i system operacyjny. Jest to jedna z podstawowych metod obrony przeciwko wirusom, złośliwemu oprogramowaniu i innym zagrożeniom obecnym w sieci.

- **Włącz aktualizacje automatyczne:** Wiele aplikacji oferuje możliwość automatycznego pobierania aktualizacji, w celu ochrony przed nowymi zagrożeniami. Aktywuj aktualizacje automatyczne wszędzie tam, gdzie jest to możliwe.

- **Chroń urządzenia podłączane do sieci:** Nie tylko komputery, ale także smartfony, tablety i inne urządzenia podłączane do Internetu potrzebują ochrony przed wirusami i złośliwym oprogramowaniem.

- **Skanuj przed użyciem:** Nie podłączaj do komputera nośników, których pochodzenie nie jest Ci znane. Urządzenia typu pendrive, dyski zewnętrzne i 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 Twoje 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 wykorzystującą dodatkowy składnik, np. kod SMS, token czy klucz sprzętowy.

- **Hasło w formie zdania:** Zadbaj o hasła posiadające przynajmniej 12 znaków. Chcesz zapamiętać je w prosty sposób? Układaj je w formie zdań, np.: *Białe kamienie leżą na ulicy, SlonceSwieciWMoimDomu!*.

- **Jedno hasło, jedno konto:** Jeżeli chcesz utrudnić działania przestępcom, dla każdego konta przygotuj oddzielne hasło. Niezbędne minimum, to rozdzielenie kont używanych w pracy i w celach prywatnych. Zadbaj o silne hasło do najistotniejszych serwisów (bankowość, poczta elektroniczna, portale społecznościowe).

- **Przechowuj bezpiecznie:** Każdy może zapomnieć hasła. Aby ułatwić nam życie, 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.

## 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 WiFi:** Ogranicz aktywność w publicznie dostępnych sieciach WiFi. Używając poza domem kluczowych serwisów (bankowość internetowa, poczta e-mail, portale społecznościowe) bezpieczniej będzie użyć własnego modemu 3G/LTE lub połączenia przez sieć VPN. Wyłączaj w urządzeniach transmisję Wi-Fi i Bluetooth, kiedy z nich nie korzystasz.

- **Chroń swoje finanse:** Korzystając z bankowości internetowej i sklepów online upewnij się, że połączenie jest objęte szyfrowaniem (*zielona kłódka* oraz prefiks "*https://*" lub "*shttp://*" 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 i 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.

## CHROŃ SWOJĄ PRYWATNOŚĆ

- **Informacje to cenna waluta:** 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://www.cert.pl/zglos-incydent (zgłaszanie incydentów naruszających bezpieczeństwo w sieci)

  https://dyzurnet.pl/ (przyjmowanie zgłoszeń dotyczących nielegalnych treści w Internecie)

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