# DOBRE PRAKTYKI W ZAKRESIE BEZPIECZEŃSTWA TELEINFORMATYCZNEGO

## Zadbaj o aktualizację 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 danych

- **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.

## 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.

## 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.

## Gdy pracujesz zdalnie

- **Korzystaj tylko z zaufanego połączenia z siecią:** Jeśli wraz z laptopem zapewniono Ci także dodatkowe urządzenie umożliwiające połączenie z internetem lub wyposażyła Twój komputer w kartę SIM, to do pracy korzystaj wyłącznie z takiego dostępu do sieci. Szczególnie w sytuacji, gdy Twoja sieć domowa jest współdzielona z innymi użytkownikami (np. z bloku lub osiedla). Nie łącz się z innymi otwartymi sieciami bezprzewodowymi, choćby ich zasięg w Twoim mieszkaniu był wyśmienity. Jeśli z jakiegoś powodu służbowy dostęp do internetu zawiedzie, to najbezpieczniej zastąpić go siecią udostępnioną z telefonu (tzw. hotspot).
- **Podczas pracy nie wychodź z tunelu VPN**: tunel VPN nie tylko szyfruje Twoje połączenie z siecią bankową, ale może zapewniać Ci także dodatkową ochronę przed zagrożeniami pochodzącymi z sieci, np. przed stronami internetowymi zaatakowanymi przez malware. Dlatego w czasie pracy zdalnej nie wyłączaj tunelu VPN, nawet jeśli zechcesz sprawdzić coś niezwiązanego z Twoimi obowiązkami.
- **Daj o bezpieczeństwo danych podczas ich przesyłania:** Pamiętaj o tym, aby nigdy nie wysyłać wrażliwych danych bez szyfrowania. Jeśli przekazujesz komuś cenne dane jako załącznik do wiadomości email, to dodatkowo zabezpiecz taki plik hasłem. Jeśli program, którego używasz nie ma takiej funkcjonalności, to zawsze możesz spakować plik np. programem ZIP z użyciem hasła i dopiero w takiej postaci dołączyć go do wiadomości. Hasło do pliku przekaż odbiorcy najlepiej w inny sposób, np. za pomocą SMS. I – co najważniejsze – przed wysłaniem pliku upewnij się, czy adres odbiorcy jest poprawnie wpisany. Nie wysyłaj plików „na skróty", czyli z Twojego prywatnego konta czy też z pominięciem poczty bankowej. Jeśli Twój bank udostępniła specjalną platformę do bezpiecznej wymiany plików, to korzystaj wyłącznie z tej metody i zrezygnuj z wysyłania plików mailem.

## 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.