Dobre praktyki w zakresie bezpieczeństwa teleinformatycznego

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).

Zabezpiecz dostęp do posiadanych danych

· **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").

· **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 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) bezpieczniej będzie użyć własnego modemu LTE lub połączenia VPN. Pamiętaj o wyłączaniu transmisji Wi-Fi i Bluetooth, kiedy z niej nie korzystasz.

Bądź świadomym użytkownikiem

· **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, kliknięcia w link czy pobrania załącznika.

Gdy pracujesz zdalnie

· **Korzystaj tylko z zaufanego połączenia z siecią:** Jeśli wraz z laptopem zapewniono Ci także dodatkowe urządzenie umożliwiające połączenie z Internetem lub wyposażono 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.

· **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.

· **Dbaj 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.

Poniżej znajduje się ogólna lista zasad, o których warto pamiętać wynikająca z dobrych praktyk:

· **Sprawdzaj adres strony Banku – szyfrowane połączenie https**

- **Sprawdzaj certyfikat strony przed każdą próbą logowania do systemu (autentyczność serwera)**

- **Uważaj na e-maile z prośbą o podanie lub weryfikację poufnych danych, np. haseł do bankowości elektronicznej**

- **Weryfikuj dyspozycje przed zatwierdzeniem**

- **Dbaj o bezpieczeństwo swojego urządzenia i swoich haseł**

- **Sprawdzaj dane logowania**

- **Za każdym razem wyloguj się z serwisu, gdy już z niego nie korzystasz**