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.
- **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. Zadbaj o silne hasło do najistotniejszych serwisów.
- **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.
- **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.
- **Pozostań na bieżąco:** Nie lekceważ informacji ze świata bezpieczeństwa IT. Jeśli coś podawane jest do publicznej wiadomości, najczęściej dotyczy także Ciebie.
- **Korzystaj tylko z zaufanego połączenia z siecią:** Jeśli wraz z laptopem zapewniono Ci także dodatkowe urządzenie umożliwiające połączenie z internetem lub Twój komputer jest wyposażony w kartę SIM, to do pracy korzystaj wyłącznie z takiego dostępu do sieci. 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).
- **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.
- **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.