

5 ZASAD CYBERBEZPIECZEŃSTWA

Cyberbezpieczeństwo to mądre i odpowiedzialne korzystanie z internetu oraz nowych technologii.

1. Korzystaj z bezpiecznych punktów dostępu i oprogramowania ochronnego.

Korzystanie z publicznych niezabezpieczonych sieci Wi-Fi może być ryzykowne. Cyberprzestępcy mogą wówczas śledzić Waszą aktywność online, a nawet przejąć Wasze dane czy hasła dostępu do Waszych kont.

Warto więc stosować oprogramowanie VPN (Virtual Private Network) szyfrujące ruch sieciowy. Ochronę przed atakami z wykorzystaniem złośliwego oprogramowania zapewni program antywirusowy, który warto zainstalować na wszystkich urządzeniach podłączonych do sieci. Korzystaj z systemów filtrujących oraz zapór sieciowych.

Korzystaj z szyfrowanych połączeń z witrynami internetowymi (zamknięta kłódeczka w pasku adresowym przeglądarki).

Pamiętaj:

- *Nie podłączaj do swojego sprzętu zewnętrznych nośników danych, co do których bezpieczeństwa nie masz pewności oraz sprawdzaj dokładnie adresy stron www, a także ich certyfikaty.*
- *Nie ściągaaj na urządzenia mobilne aplikacji, które nie pochodzą z oficjalnych sklepów np. Google, Apple, ponieważ mogą mieć ukryte funkcje narażające Twoje bezpieczeństwo lub prywatność.*

2. Nie otwieraj załączników z niepewnych źródeł i nie klikaj w podejrzaną linki.

Poczta elektroniczna to obecnie najpopularniejsze narzędzie cyberprzestępców i najprostszy sposób dystrybucji złośliwego oprogramowania: w linkach i załącznikach.

Jedną z metod, tzw. phishing* za pomocą linku odsyła do fałszywej strony banku, firmy czy urzędu, która po zalogowaniu przez użytkownika przejmuje jego dane uwierzytelniające lub infekuje samo urządzenie.

W sieci warto stosować się do zasady ograniczonego zaufania. Nigdy nie klikajmy w linki czy załączniki od nieznanego nadawcy i dokładnie przyglądamy się nazwie adresata oraz witryny, do której odsyła e-mail. Treść wiadomości wysłanej przez cyberprzestępcę często

zawiera błędy językowe, dlatego dobrze jest zwrócić na to uwagę podczas czytania. Wiadomości, których się nie spodziewaliśmy, zawsze należy traktować z ostrożnością. Warto najpierw skontaktować się bezpośrednio z nadawcą i zweryfikować, czy rzeczywiście wysłał do nas wiadomość.

***(Phishing** - to oszustwo internetowe, które atakuje swoją ofiarę, aby wyłudzić od niej poufne dane).

3. Twórz hasła skomplikowane i trudne do odgadnięcia przez postronne osoby.

Należy zawsze używać silnych, złożonych haseł zawierających małe, duże litery, liczby i znaki specjalne oraz dwuetapowego uwierzytelniania na wszystkich urządzeniach i kontach. To samo hasło nie powinno być używane na różnych kontach – zwłaszcza zawierających poufne informacje. Dzięki temu nawet, jeśli naruszone zostanie jedno z nich, cyberprzestępca nie będzie mógł wziąć na cel pozostałych.

Pamiętaj:

- „1234” i „hasło” – to nie hasła
- Wyloguj się po ukończonej sesji.
- Nie używaj tego samego hasła do różnych kont.
- Nie zapisuj haseł na kartkach oraz w plikach na komputerze.
- Regularnie zmieniaj hasła.
- Nie podawaj i nie wysyłaj swoich loginów i haseł innym osobom.

4. Regularnie aktualizuj system, aplikacje, przeglądarkę oraz oprogramowanie antywirusowe.

Często ignorujemy powiadomienia o aktualizacjach i przesuwamy je na później, tym samym ułatwiając hakerowi zadanie.

Absolutną podstawą bezpieczeństwa cyfrowego, jest korzystanie z oprogramowania antywirusowego na każdym urządzeniu podłączonym do internetu.

5. Dbaj o swoją prywatność

Wasze profile społecznościowe mówią wiele o naszej tożsamości.

Nie ma w tym nic złego, jeśli robicie to mądrze, świadomie decydując o tym jakie informacje i w jaki sposób chcemy o sobie udostępniać.

Pamiętaj:

- odpowiednio ustaw prywatność swoich profili w mediach społecznościowych,
- nie udostępniaj o sobie zbyt wiele spersonifikowanych informacji (np. adresu zamieszkania, nr telefonu),
- Unikaj kontaktów z osobami nieznanymi, które mogą podawać się za Twoich „przyjaciół” Często ich działanie polega na pozyskaniu Twojej sympatii, zależności od siebie co w konsekwencji może doprowadzić do działań niezgodnych z prawem.