"BEZPIECZNY INTERNET: 10 KROKÓW DO OCHRONY PRZED CYBERZAGROŻENIAMI"

1. **Używaj silnych haseł**
   Twórz hasła składające się z co najmniej 12 znaków, zawierających wielkie i małe litery, cyfry oraz znaki specjalne.

2. **Bądź ostrożny z e-mailami i wiadomościami**
   Nie otwieraj podejrzanych e-maili i wiadomości oraz nie klikaj w linki ani załączniki z nieznanych źródeł.

3. **Zabezpiecz urządzenia mobilne**
   Włącz blokady ekranu, szyfrowanie danych

4. **Ogranicz dostęp do danych**
   Ustal, kto ma dostęp do Twoich danych osobowych

5. **Sprawdzaj ustawienia prywatności**
   Sprawdź swoje ustawienia prywatności w aplikacjach i serwisach społecznościowych

6. **Unikaj udostępniania zbyt wielu informacji**
   Bądź ostrożny z tym, co publikujesz w Internecie, szczególnie na platformach społecznościowych.

7. **Aktualizuj oprogramowanie**
   Regularnie instaluj aktualizacje systemu operacyjnego, aplikacji oraz oprogramowania zabezpieczającego. Używaj wyłącznie oficjalnych źródeł do pobierania oprogramowania, unikaj pirackich wersji.

8. **Zwracaj uwagę na oprogramowanie**
   Zainstaluj oprogramowanie antywirusowe. Używaj renomowanych programów antywirusowych i regularnie aktualizuj ich bazy danych.

9. **Używaj zapory sieciowej**
   Włącz zaporę systemową lub zainstaluj zaporę sprzętową, aby kontrolować ruch sieciowy.

10. **Rozważnie korzystaj z publicznych Wi-Fi**
    Nie wykorzystuj publicznych Wi-Fi do logowania się do kont osobistych i bankowych.

"ZAGROŻENIA W CYBERPRZESTRZENI: 10 NIEBEZPIECZEŃSTW, KTÓRE POWINIENEŚ ZNAĆ !"

1. **Phishing**
   Ataki mające na celu wyłudzenie danych logowania i informacji osobowych poprzez fałszywe e-maile lub strony internetowe.

2. **Malware**
   Oprogramowanie złośliwe, które może infekować urządzenia, prowadząc do utraty danych, kradzieży informacji lub uszkodzenia systemów.

3. **Ransomware**
   Złośliwe oprogramowanie, które szyfruje pliki na urządzeniu i żąda okupu za ich odszyfrowanie.

4. **Keyloggery**
   Oprogramowanie rejestrujące naciśnięcia klawiszy, co może prowadzić do kradzieży haseł i danych osobowych.

5. **Spyware**
   Programy szpiegowskie, które zbierają dane o użytkownikach bez ich wiedzy, często monitorując ich działania w Internecie.

6. **Adware**
   Oprogramowanie, które wyświetla niechciane reklamy, często spowalniając działanie urządzenia i zbierając dane o preferencjach użytkownika.

7. **Browser Hijacker (porywacz przeglądarek)**
   To rodzaj złośliwego oprogramowania, które zmienia ustawienia przeglądarki internetowej bez zgody użytkownika. Instalują złośliwe oprogramowanie lub śledzą działania użytkownika w Internecie.

8. **Fałszywe aplikacje**
   Aplikacje, które wyglądają jak oryginalne, ale zawierają złośliwe oprogramowanie lub wyłudzają dane użytkownika.

9. **Ataki socjotechniczne**
   Manipulacja użytkownikami wykorzystując rozmaite techniki wywierania wpływu i manipulowanie drugim człowiekiem.

10. **Spoofing**
    Oszustwo polegające na podawaniu się za inną osobę lub źródło, aby wprowadzić w błąd użytkownika np. podszywanie się pod czyjś numer telefonu.