BĄDŹ BEZPIECZNY

Bezpieczeństwo seniorów ma wielowymiarowe znaczenie. Kluczem jest eliminowanie potencjalnych zagrożeń, między innymi w tak ważnych obszarach, jak ruch drogowy i przestrzeń cyfrowa. Bezpieczeństwa nie osiąga się zakazami, ale budowaniem świadomości ryzyka. Na drodze ważna jest zasada widoczności i obiektywna ocena własnych możliwości fizycznych. Z kolei w świecie cyfrowym najważniejsze jest wdrożenie zasady ograniczonego zaufania do komunikatów. Tylko w taki świadomy sposób senior nie będzie narażony na działania oszustów, które niestety wciąż są powszechne. Zatem bądźmy czujni i przezorni. Czasem tylko to wystarczy, aby być bezpiecznym.



Wojciech Saługa
Marszałek Województwa Śląskiego

BĄDŹ ROZWAŻNY

PHISHING (FISZING)

Phishing to próba wyłudzenia danych, pieniędzy lub dostępu do konta poprzez fałszywe wiadomości, e-maile, SMS-y lub rozmowy telefoniczne. **Oszuści często podszywają się pod bank, urząd, sklep, firmę kurierską czy członka rodziny**, aby wzbudzić zaufanie i skłonić do szybkiego działania.

Aby się chronić, nie klikaj w podejrzane linki i nie otwieraj nieoczekiwanych załączników. Nigdy nie podawaj przez telefon, e-mail lub SMS swoich haseł, kodów SMS, kodów BLIK ani danych do logowania. Jeśli wiadomość lub telefon budzą wątpliwości, przerwij kontakt i samodzielnie skontaktuj się z daną instytucją, korzystając z oficjalnego numeru telefonu lub strony internetowej.

Pamiętaj: oszuści liczą na pośpiech i emocje.
Zatrzymaj się, sprawdź i dopiero potem działaj.

Oszustwa komputerowe stanowią

94%

wszystkich rejestrowanych incydentów.

Najczęściej oszuści podszywają się pod wiadomości z **popularnych serwisów zakupowych.**

BEZPIECZNY SENIOR

NA DRODZE I W SIECI

Śląskie.
DLA SENIORA



BEZPIECZNIE NA DRODZE

- **Zawsze zatrzymuj się przed przejściem**
- **Upewnij się, że jadące pojazdy zamierzają ci ustąpić**
- **Kiedy będzie to możliwe, zacznij przechodzenie, idź prosto w poprzek drogi**
- **Nie przekraczaj jezdni w pobliżu zaparkowanych samochodów,** nadjeżdżający kierowcy nie będą cię zza nich mogli zobaczyć
- **Przechodź w takim miejscu aby kierowcy samochodów i rowerzyści mogli widzieć cię z daleka i bez utrudnień**
- **Unikaj przechodzenia w pobliżu zakrętów i wzniesień**
- **Po zmroku bezwzględnie noś odblaski**

BEZPIECZNIE W SIECI

- ✓ **Regularnie aktualizuj systemy i aplikacje**
  Aktualizacje zawierają poprawki bezpieczeństwa.
- ✓ **Włącz uwierzytelnianie dwuskładnikowe (2FA)**
  Dodatkowe potwierdzenie logowania zwiększa bezpieczeństwo.
- ✓ **Używaj długich haseł i menedżera haseł**
  Stosuj silne, unikalne hasła.
- ✓ **Sprawdzaj adres strony przed wpisaniem danych**
  Zwracaj uwagę na fałszywe strony.
- ✓ **Weryfikuj informacje innymi kanałami**
  Sprawdzaj nietypowe prośby.

- ✗ **Nie używaj tych samych haseł w różnych miejscach**
  Każda usługa powinna mieć własne hasło.
- ✗ **Zachowaj ostrożność korzystając z publicznego Wi-Fi**
  Sprawdzaj z jaką siecią się łączysz i nie ignoruj ostrzeżeń o bezpieczeństwie połączenia.
- ✗ **Uważaj na zbyt dobre oferty inwestycyjne**
  To często oszustwo.
- ✗ **Nie działaj pod presją rozmówcy**
  Jeśli rozmowa budzi podejrzenia rozłącz się. Samodzielnie zadzwoń na numer z oficjalnej strony instytucji lub znany ci numer bliskiej osoby - nie na numer podany przez rozmówcę.
- ✗ **Nie pozostawiaj odblokowanego telefonu lub komputera bez nadzoru**
  Zawsze blokuj urządzenie, nawet na chwilę.

Jeśli coś wzbudza Twoją wątpliwość, daj znać zespołowi CERT Polska.

Formularz online: incydent.cert.pl
SMS na numer: 8080
Aplikacja mObywatel – zakładka „Bezpiecznie w sieci".

