Cyfrowy Senior

PORADNIK DLA SENIORÓW

BEZPIECZNY SENIOR W INTERNECIE

Broszura informacyjna

POZnań metropolia

Poznań 2021

Stowarzyszenie Aglomeracja Kalisko-Ostrowska

Broszura przygotowana przez zespół autorów na zlecenie:

Stowarzyszenie Metropolia Poznań
ul. Kościelna 37
60-537 Poznań
www.metropoliapoznan.pl
www.senior.metropoliapoznan.pl

1. Ogólnie o bezpieczeństwie w internecie

Internet to okno na świat. Świat wirtualny sposób szczególny właśnie dla seniorów może decydować o jakości życia i możliwościach realizacji swoich praw obywatelskich i społecznych. To właśnie internet pozwala nam korzystać z usług publicznych (w tym publicznych usług e-zdrowia), z mozliwości udziału w konsultacjach społecznych online oraz możliwości aktywizacji obywatelskiej w ramach budżetów obywatelskich, z bogatej oferty rozrywki i kultury w sieci, z platform komunikacji elektronicznej umożliwiających darmowy kontakt z rodziną i znajomymi itd.

Co więcej, internet jako taki jest **oknem na świat całkowicie dostępnym**, czyli pozbawionym barier architektonicznych. Możemy z zasobów sieci korzystać niemal niezależnie od naszego aktualnego stanu zdrowia, możliwości transportowych czy zasobów finansowych (duża część zasobów jest darmowa). Jedynym wymogiem jest posiadanie podłączenia do sieci internetowej za pośrednictwem oferty firm komercyjnych: telekomunikacyjnych lub też dostawców sygnału satelitarnego.

Jednak mimo swoich ogromnych zalet, środowisko internetu może być niebezpieczne a użytkowanie zasobów internetu niesie ze sobą także konkretne ryzyka dla seniorów.

W sieci możemy też spotkać tzw. **CYBERPRZESTĘPCÓW**.

Mają oni różne cele, jednak ogólnie możemy stwierdzić, że w większości przypadków **oszuści w internecie chcą wykraść**:

Nasze pieniądze

Prywatne informacje i dane na nasz temat

Dane naszych znajomych

Ryzyka w sieci – kiedy musimy uważać w internecie

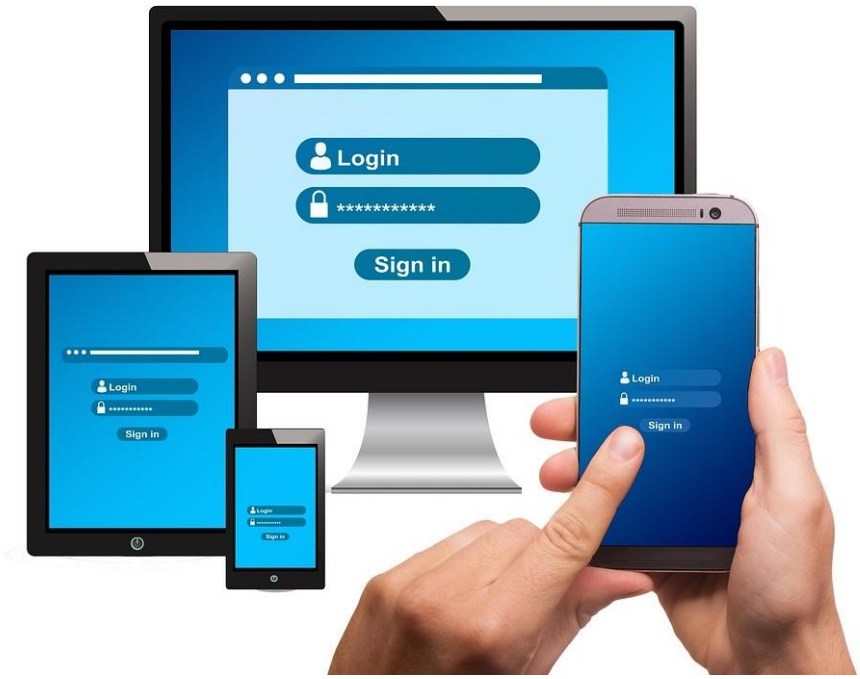
Odbierając pocztę elektroniczną e-mail	Kupując w sklepach internetowych	Korzystając z bankowości elektronicznej
Korzystając z mediów społecznościowych i dzieląc się swoją prywatnością	Korzystając z otwartych sieci WiFi	Wchodząc na nieznajome strony

Poniżej prezentujemy Państwu zestaw konkretnych zasad bezpiecznego korzystania z internetu. By czas spędzony w sieci był dla nas zarówno korzystny, jak i w pełni bezpieczny.

2. Zadbaj o bezpieczne HASŁA

- Hasła powinny składać się z losowej kombinacji
  - ✓ Dużych i małych liter
  - ✓ Cyfr
  - ✓ Znaków specjalnych np. ! @ $ % &
- Nie wykorzystujmy informacji powiązany bezpośrednio z nami np. data urodzin, nazwa ulicy przy której mieszkamy, imię zwierzaka.
- Dbajmy o poufność swojego hasła.
- Używamy różnych haseł w różnych miejscach (np. inne w bankowości elektroniczne, inne w mediach społecznościowych).

PRZYKŁAD	
ŹLE	ImieNazwisko123!
DOBRZE	Pudelek6527@$*



3. Stosuj OPROGRAMOWANIE ANTYWIRUSOWE

- Dostępne są programy **płatne i bezpłatne**.
- Programy płatne są skuteczniejsze ponieważ: chronią przed większą liczbą zagrożeń a ich bazy wirusów są na bieżąco aktualizowane.
- Stosuj jednak co najmniej programy bezpłatne.
- Chronić można różne urządzenia: **komputer, laptop, tablet, smartfony.**

4. Uważaj na WIADOMOŚĆI OD NIEZNAJOMYCH

- Zwróć uwagę na wiadomości od nieznajomych Ci osób, szczególnie na te które **sprawiają wrażenie spersonalizowanych dla Ciebie**.
- **Nie otwieraj żadnych linków czy plików**. Nie przechodź na nieznane Ci strony poprzez odnośniki w podejrzanych wiadomościach.
- Jeśli masz wątpliwości:
  - ✓ **ZAWSZE sprawdź ADRES NADAWCY** (czy wygląda wiarygodnie)
  - ✓ **zadzwoń do osoby, która przesłała wiadomość** i potwierdź, że mail jest autentyczny.
- Szczególnie uważaj na wiadomość **od osób z zagranicy** lub o treści wskazującej na nieudolne tłumaczenie na język polski.

PRZYKŁADY

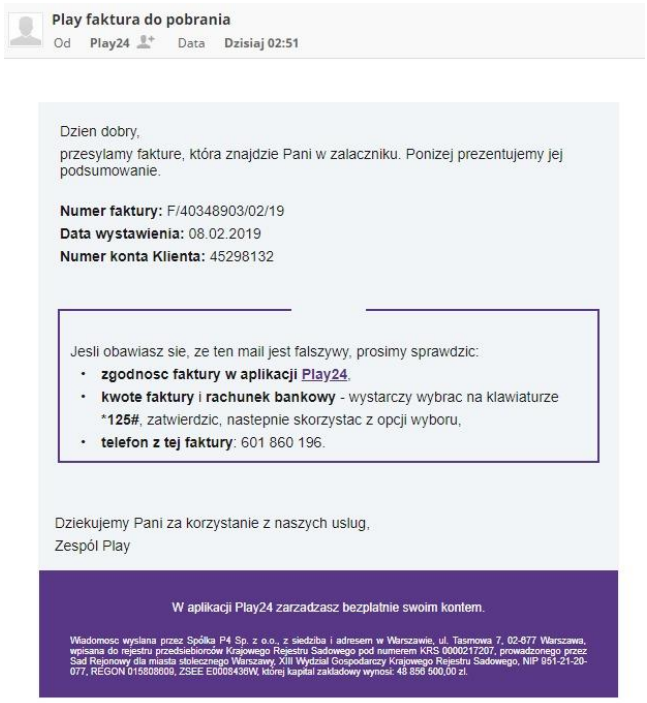
UWAŻAJ!

• Dostajesz maila od pracownika nieznanej Ci firmy informującego, że w załączeniu przesyła Ci korektę faktury.	✓ **Cel oszusta: otwarcie przez Ciebie pliku z wirusem**
• Otrzymujesz wiadomość z banku, że konieczna jest zmiana hasła do bankowości elektronicznej z linkiem do „strony banku”.	✓ **Cel oszusta: wpisanie przez Ciebie danych do logowania do konta po wejściu na fałszywą stronę banku**

PRZYKŁAD

UWAŻAJ!

- e-mail imitujący fakturę od operatora komórkowego Play
- Na pierwszy rzut oka mail wygląda wiarygodnie (bardzo dobra imitacja)
- Oszustwo zdradził w tym przypadku adres nadawcy: ***bimemetirez1997@o2.pl***



Play faktura do pobrania
Od **Play24** Data **Dzisiaj 02:51**

Dzien dobry,
przesylamy fakture, która znajdzie Pani w zalaczniku. Ponizej prezentujemy jej podsumowanie.

Numer faktury: F/40348903/02/19
Data wystawienia: 08.02.2019
Numer konta Klienta: 45298132

Jesli obawiasz sie, ze ten mail jest falszywy, prosimy sprawdzic:
- **zgodnosc faktury w aplikacji** Play24,
- **kwote faktury** i **rachunek bankowy** - wystarczy wybrac na klawiaturze ***125#**, zatwierdzic, nastepnie skorzystac z opcji wyboru,
- **telefon z tej faktury**: 601 860 196.

Dziekujemy Pani za korzystanie z naszych uslug,
Zespól Play

W aplikacji Play24 zarzadzasz bezplatnie swoim kontem.

Wiadomosc wyslana przez Spółka P4 Sp. z o.o., z siedziba i adresem w Warszawie, ul. Tasmowa 7, 02-677 Warszawa, wpisana do rejestru przedsiebiorców Krajowego Rejestru Sadowego pod numerem KRS 0000217207, prowadzonego przez Sad Rejonowy dla miasta stolecznego Warszawy, XIII Wydzial Gospodarczy Krajowego Rejestru Sadowego, NIP 951-21-20-077, REGON 015808609, ZSEE E0008436W, której kapital zakladowy wynosi: 48 856 500,00 zl.

UWAŻAJ!

PRZYKŁAD

- e-mail imitujący informację z platformy NETFLIX
- W żadnym wypadku nie należy klikać na przycisk w tym mailu i nie podejmować żadnych akcji.
- Ponownie oszusta zdradził adres nadawcy: ***test@33srz.com***

Twoje powiadomienie o zawieszeniu

Nie udało nam się autoryzować płatności za kolejny cykl rozliczeniowy abonamentu, dlatego zawiesiliśmy Twoje członkostwo. Twoja obecna subskrypcja jest jednak aktywna do momentu jej wygaśnięcia.

Oczywiście chcielibyśmy, abyś wrócił do nas. Dlatego wystarczy kliknąć przycisk zrestartuj swoje członkostwo, aby zaktualizować swoje dane i kontynuować oglądanie wszystkich najlepszych filmów z programów telewizyjnych.

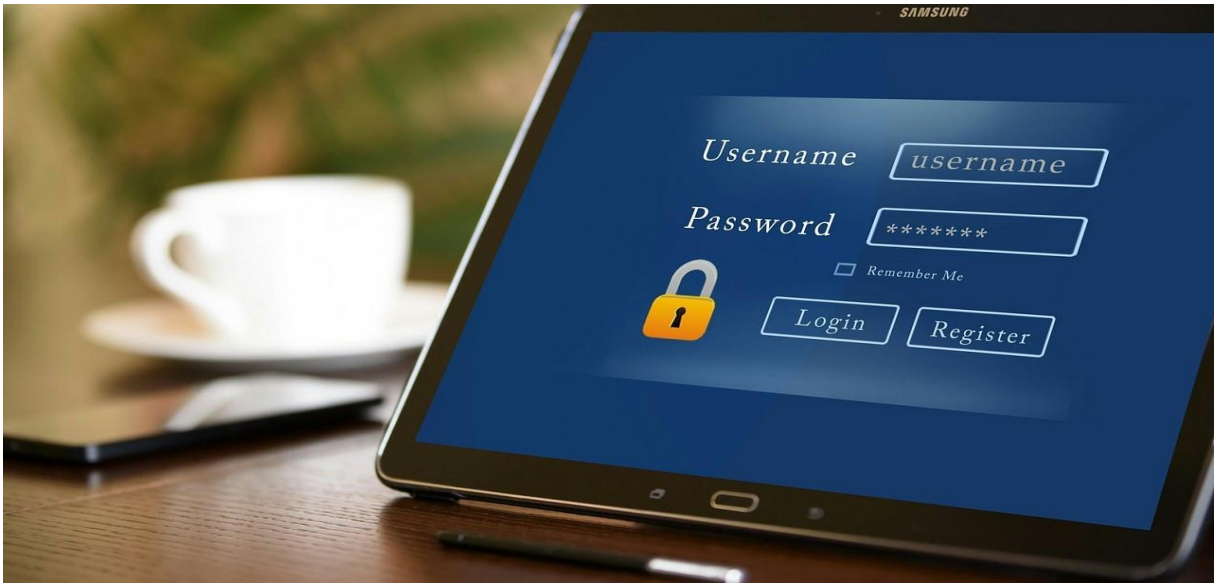
Zrestartuj swoje członkostwo.

–Twoi przyjaciele z Netflix

5. Jeśli to możliwe korzystaj z WERYFIKACJI DWUSTOPNIOWEJ

- Dwustopniowa weryfikacja znacząco zwiększa nasze bezpieczeństwo czyli np.
  - ✓ Logowanie z podaniem **LOGINU** i **HASŁA** a następnie…
  - ✓ Podanie **kodu przesłanego SMS-em**.

Metoda nr 1		**Metoda nr 2**		**WEJŚCIE NA KONTO**
HASŁO		**KOD SMS**		



6. Staraj się tworzyć KOPIE ZAPASOWE

- Kopie zapasowe to kopiowanie zawartości dysku, biblioteki zdjęć czy filmów z urządzenia, które używamy na co dzień na jakieś inne alternatywne urządzenie (np. dysk zewnętrzny lub pen drive o większej pojemności) lub na dysk wirtualny (chmura).
- Ma to szczególne znaczenie w przypadku np. zdjęć czy dokumentów.
- W sytuacji gdy doszłoby do utraty danych na komputerze np. ze względu na atak hackerski lub defekt sprzętowy – będziesz zabezpieczony i nie utracisz swoich plików.

7. Zachowaj ostrożność korzystając z OTWARTYCH SIECI WiFi

Wi-Fi to lokalna bezprzewodowa sieć komputerowa (oparta na łączności radiowej), kojarzona z bezprzewodowym dostępem do Internetu w miejscach publicznych, zwykle zabezpieczona hasłem dostępu

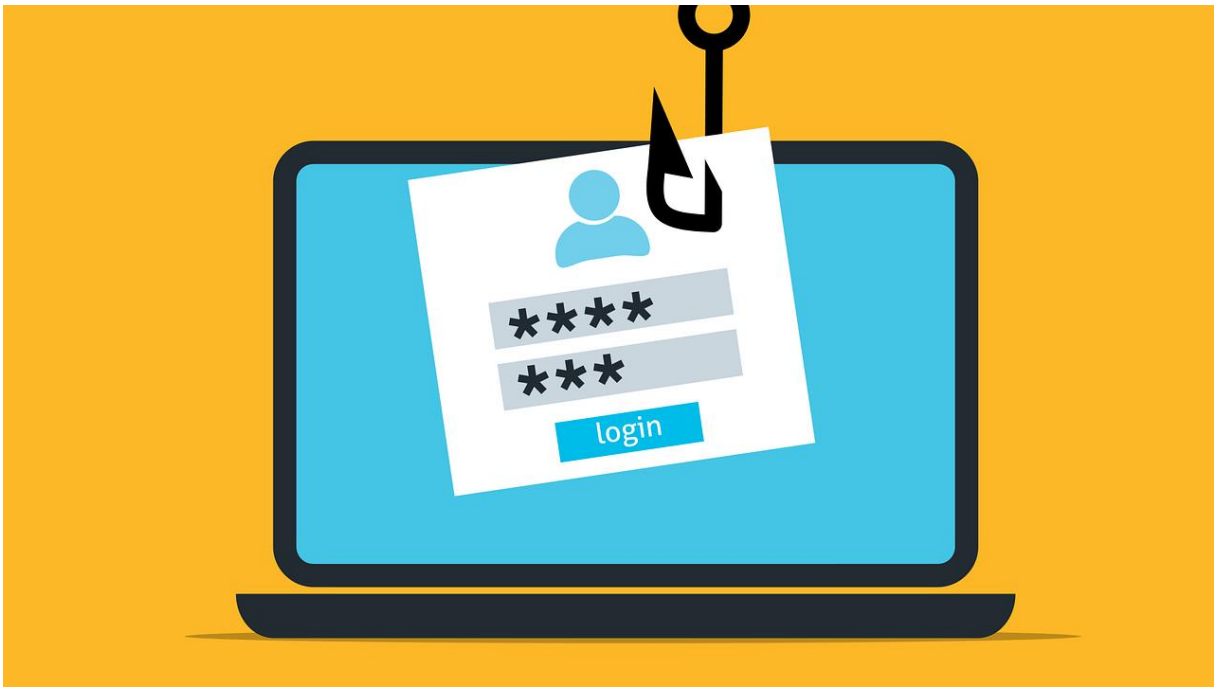
- Z sieci WiFi korzystamy zazwyczaj dlatego, że oferują **BEZPŁATNY** dostęp do internetu.
- Korzystając z internetu w miejsach publicznych i używając WiFi **nie wykonuj poprzez takie sieci płatności przez internet!**
- Unikaj także wkorzystywania swoich danych wrażliwych oraz nie wyrażaj zgody na dostęp do Twoich danych innych użytkowników.
- Zachowaj ostrożność korzystając z WiFi szczególnie w takich miejscach publicznych jak:
    - ✓ centrum handlowe,
    - ✓ restauracja,
    - ✓ kawiarnia,
    - ✓ skwer publiczny.
- Nawet jeśli dostawcą internetu w danej lokalizacji jest placówka publiczna, to sieć ta może być bardziej narażona na ataki hakerskie.

8. Aktualizuj OPROGRAMOWANIE

- Staraj się aktualizować wszystkie swoje urządzenia elektroniczne tj.: komputer, laptop, tablet, telefon.
- Aktualizacja sprawia, że nasze urządzenia są mniej podatne na niebezpieczeństwa w sieci – **aktualizacje eliminują luki bezpieczeństwa.**
- Gdy Twoje urządzenie poprosi się o zgodę na aktualizację **NIE OBAWIAJ SIĘ** kliknąć TAK lub AKTUALIZUJ.
- **Aktualizacja może zająć kilka lub kilkanaście minut.** Zazwyczaj urządzenie pozwoli Ci wybrać odpowiedni czas, gdy akurat nie będziesz potrzebować internetu i gdy będzie można swobodnie przeprowadzić aktualizację.

9. NIE ZAPAMIĘTUJ haseł i danych w przeglądarce internetowej

- Staraj się nie zgadzać się gdy urządzenie zapyta czy zapamiętać Twoje hasło. W takiej sytuacji Twoje hasła i dane są bardziej zagrożone atakiem.
- Pod żadnym pozorem nie korzystaj z tej funkcji poza domem wykorzystując urządzenia w pracy czy w klubie seniora.



10. Zwróć uwagę na ADRESY i BEZPIECZNE STRONY

- Gdy otrzymałeś od kogoś adres internetowy **zwróć uwagę czy nazwa strony jest poprawna** (czy nie posiada błędu i nie prowadzi do fałszywej strony).
- Czasem oszuści **zmieniają tylko jedną literę** by adres strony przypominał adres strony internetowej Twojego banku czy firmy telekomunikacyjnej. Mają wówczas nadzieję, że ich ofiary nie zauważą podstępu.
- Czasem też stosują inne sztuczki:
  - ✓ gdy w adresie jest literka **„S”** wpisują cyfrę **„5”**
  - ✓ gdy w adresie jest litera **„O”** (jak „olbrzym”) wpisują cyfrę **„0”** (zero)
- Fałszywe strony banków, systemów płatniczych czy innych instytucji finansowych stanowią poważne zagrożenie. Twoja przygoda z nimi może rozpocząć się od otrzymania zaskakującego lub niepokojącego e-maila informującego, że zarejestrowano podejrzaną transakcję na Twoim koncie itp. Zazwyczaj taka wiadomość nie zawiera zbyt wielu szczegółów, a by uzyskać więcej informacji, musisz kliknąć link, podać swoje dane, hasło oraz numer karty. Jednak, istnieje mały, ale dość istotny szczegół. Link

podany w wiadomości przekierowuje Cię na podrobioną stronę. Wygląda ona niemal tak samo jak prawdziwa lub jest do niej bardzo podobna. Jednak informacje, które tam wpiszesz, zostaną przesłane nie do banku, a prosto do cyberprzestępców. Ten rodzaj oszustwa nazywany jest **phishingiem** (czyt. „fiszingiem”) i jest bardzo powszechną metodą wyłudzania pieniędzy w sieci. Internetowi złodzieje tworzą także fałszywe strony popularnych sklepów internetowych, księgarni oraz popularnych serwisów (Facebook, Gmail, Allegro itp.).

- Warto też zawsze sprawdzić czy strona na którą wchodzimy ma tzw. **certyfikat SSL (kłódka)**

SSL (ang. Secure Sockets Layer) - to protokół sieciowy zabezpieczający komunikację pomiędzy przeglądarką internetową a serwerem.

Jego zadaniem jest szyfrowanie transmisji danych, czyli informacji poufnych, które najczęściej podajemy w formularzach (adresy e-mail, hasła, dane kontaktowe).

- certyfikat SSL – zwany jest „kłódką” lub „zieloną kłódką” i **zlokalizowany jest tuż przy adresie internetowym strony**, na którą wchodzisz.
- Po kliknięciu na „kłódkę” otrzymujemy informacje czy połączenie jest bezpieczne i szyfrowane, można też kliknąć w dany certyfikat bezpieczeństwa i znaleźć więcej informacji na jego temat.

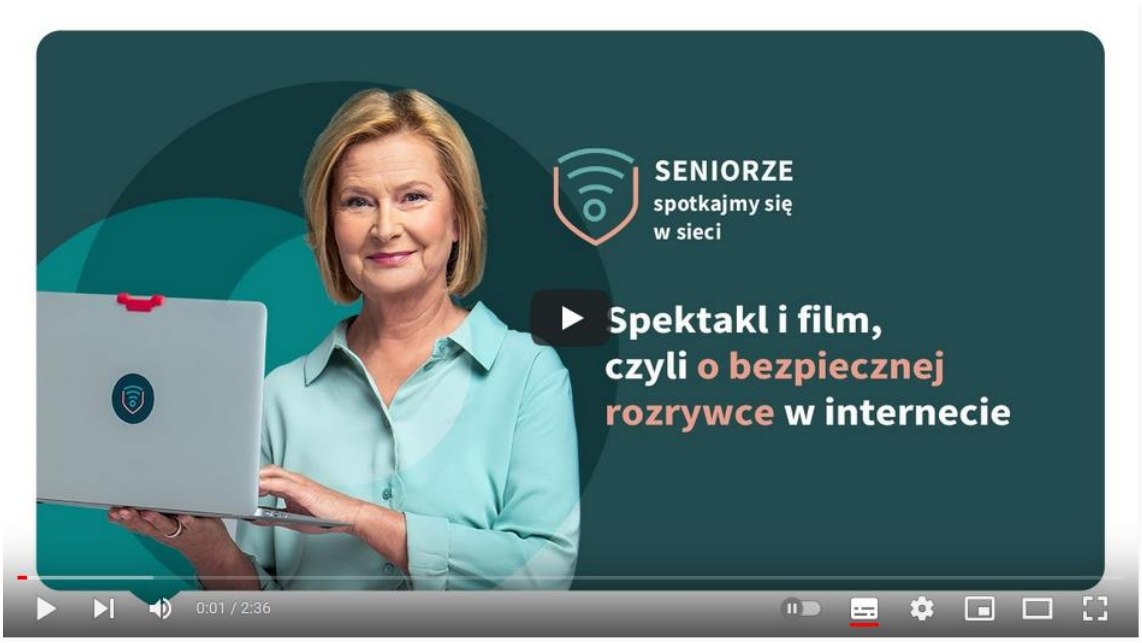
11. Dowiedz się więcej

Więcej informacji o bezpieczeństwie w internecie oraz film edukacyjny w tym temacie znajdziesz na stronach internetowych projektu:

www.senior.metropoliapoznan.pl (Stowarzyszenie Metropolia Poznań)

www.sako-info.pl/dla-seniorow (Stowarzyszenie Aglomeracja Kalisko-Ostrowska)

Zachęcamy także do zapoznania się z materiałami nt. bezpieczeństwa w internecie opracowanymi w ramach kampanii „Seniorze – spotkajmy się w sieci”: https://www.gov.pl/web/seniorze-spotkajmy-sie-w-sieci



Cyfrowy Senior

Broszura przygotowana w ramach projektu
„CYFROWY SENIOR – Program edukacji cyfrowej seniorów
w Metropolii Poznań i Aglomeracji Kalisko-Ostrowskiej”

POZnań metropolia

Stowarzyszenie Aglomeracja Kalisko-Ostrowska

www.senior.metropoliapoznan.pl **www.sako-info.pl/dla-seniorow**

Projekt finansowany ze środków Programu wieloletniego
na rzecz Osób Starszych „Aktywni+” na lata 2021-2025
oraz środków własnych Stowarzyszenia Metropolia Poznań
i Stowarzyszenia Aglomeracja Kalisko-Ostrowska

AKTYWNI+