BNP PARIBAS

10 ZASAD
CYBERBEZPIECZNEGO SENIORA

czyli jak zadbać o:
#bezpieczny komputer
#bezpieczny internet
#bezpieczne finanse

W erze cyfrowej kontakt online jest ważny. Ważne jest także, aby podjąć odpowiednie kroki w celu ochrony przed zagrożeniami cybernetycznymi.
Oto dziesięć podstawowych wskazówek, jak samodzielnie zadbać o bezpieczne korzystanie z internetu.

1. UŻYWAJ SILNYCH HASEŁ – minimum 15 znaków

Silne hasła to pierwsza linia obrony przed cyberatakami:

- używaj kombinacji liter, cyfr i symboli
- unikaj łatwych do odgadnięcia informacji, takich jak daty urodzenia czy imiona
- używaj różnych loginów i haseł dla bankowości elektronicznej, mediów społecznościowych czy poczty elektronicznej
- rozważ użycie menedżera haseł, aby bezpiecznie zarządzać swoimi hasłami.

2. ZACHOWAJ OSTROŻNOŚĆ W MEDIACH SPOŁECZNOŚCIOWYCH

Media społecznościowe mogą być świetnym sposobem na kontakt z przyjaciółmi i rodziną. Niestety mogą również zawierać wiele fałszywych ofert inwestycyjnych, informacji i linków prowadzących do stron przygotowanych przez oszustów. Uważaj, jakie informacje osobiste udostępniasz publicznie. Rozważ ustawienie konta jako prywatne lub ogranicz jego widoczność dla nieznajomych.

3. SPRAWDZAJ WIARYGODNOŚĆ WIADOMOŚCI E-MAIL

Uważaj na e-maile, szczególnie te, których nadawca prosi o dane osobowe, dane do logowania oraz zachęca do klikania w linki. Zawsze sprawdzaj nadawcę zanim podejmiesz działania.
Phishing to powszechna metoda, w której przestępcy podszywają się pod legalne firmy lub instytucje aby ukraść wrażliwe informacje.

4. AKTUALIZUJ OPROGRAMOWANIE

Regularnie aktualizuj system operacyjny Twojego komputera, telefonu, aplikacji i oprogramowania antywirusowego. Jest to kluczowe dla Twojego bezpieczeństwa. Aktualizacje często zawierają poprawki zabezpieczeń, które chronią przed lukami w systemie. Włącz automatyczne aktualizacje, aby nie przegapić ważnych uaktualnień.

5. REGULARNIE MONIOTRUJ KONTA BANKOWE

Regularnie sprawdzaj wyciągi bankowe i karty kredytowe. Natychmiast zgłaszaj podejrzane transakcje. Ustaw powiadomienia o transakcjach, co może pomóc wcześnie wykryć potencjalne oszustwa.

6. UŻYWAJ BEZPIECZNYCH POŁĄCZEŃ WI-FI

W miejscach publicznych takich jak lotniska, hotele, kawiarnie nie korzystaj z ogólnodostępnej sieci Wi-Fi do logowania się w bankowości internetowej. W domu upewnij się, że Twoje Wi-Fi jest zabezpieczone silnym hasłem.

7. TWÓRZ KOPIE ZAPASOWE WAŻNYCH DANYCH

Regularnie twórz kopie zapasowe danych komputera lub telefonu, najlepiej na zewnętrznym dysku twardym lub w chmurze.
Jeśli Twój komputer padnie ofiarą wirusa lub awarii, dzięki kopiom zapasowym, nie stracisz ważnych dokumentów i zdjęć.

8. WŁĄCZ DWUETAPOWE LOGOWANIE

Uwierzytelnianie dwuskładnikowe daje dodatkową opcję zabezpieczenia kont, szczególnie e-mailowych i bankowych.
Jak to działa? W większości wypadków będziesz otrzymywać jednorazowy kod na telefon, tablet lub e-mail. Kod ten trzeba wpisać w trakcie logowania po tym, jak wpiszesz hasło, zmniejsza to ryzyko włamania na konta.

9. EDUKUJ SIĘ NA TEMAT NOWYCH ZAGROŻEŃ I OSZUSTW

Bądź na bieżąco i poszerzaj swoją wiedzę o najnowszych oszustwach skierowanych do seniorów. Mogą to być:

- fałszywe powiadomienia o wygranych w loteriach
- oszukańcze telefony z pomocą techniczną
- "zbyt dobre, by były prawdziwe" oferty inwestycyjne.

Wiedza na temat cyberzagrożeń zwiększy Twoją świadomość i bezpieczeństwo.
Dobre źródła wiedzy:
www.bnpparibas.pl/bezpieczenstwo
Materiały Edukacyjne Cyberbezpieczeństwo
www.nask.pl

10. FAŁSZYWE POŁĄCZENIA TELEFONICZNE

Fałszywe połączenie telefoniczne, czyli Vishing polega na tym, że przestępca podszywa się pod pracownika banku. Wykorzystuje przy tym prawdziwy numer telefonu banku. Klient jest przekonywany, że rozmawia z pracownikiem banku.

Pracownicy banku nigdy nie proszą, aby:

- podać im login lub hasło do bankowości internetowej.
- zainstalować dodatkowe oprogramowanie lub uzyskać zdalny dostęp do komputerów/telefonów klientów.
- podać im pełny numer karty i kod CVV.
- Podać im kod BLIK, zrobić przelew, wpłatę lub wypłatę pieniędzy w bankomacie czy oddziale banku.

Nie wahaj się zwrócić o pomoc do członków rodziny lub przyjaciół, jeśli nie rozumiesz jakiegoś zagadnienia związanego z technologią. Niezależnie od tego, czy nie wiesz, jak ustawić funkcje bezpieczeństwa, czy jak rozpoznać podejrzane e-maile pomoc bliskiej osoby, może zapewnić spokój i zwiększyć Twoje bezpieczeństwo w sieci.