

Poradnik dla seniorów o bezpieczeństwie w sieci



Capgemini 

Spis treści

1. Bezpieczeństwo w sieci	str. 4
2. Bezpieczne zakupy w Internecie	str. 5
3. Weryfikacja zbiórek charytatywnych	str. 7
4. Oszustwo na wnuczka - przykładowy scenariusz	str. 8
5. Jak można pomóc seniorom?	str. 10
6. Przeciwdziałanie oszustwom matrymonialnym	str. 11
7. Pozostałe formy pomocy	str. 12



Bezpieczeństwo w sieci



Podstawowe zabezpieczenia:

- Zainstaluj antywirusa
- Zwracaj uwagę na znaki bezpieczeństwa (kłódka)
- Włącz automatyczną aktualizację
- Używaj różnych haseł
- Używaj zaśleпки na kamerę



Korzystanie ze skrzynek e-mail i SMS:

- Nie klikaj w nieznane linki
- Sprawdzaj adresata
- Nie pobieraj załączników od nieznanymi adresatów
- Nie podawaj wrażliwych danych



Korzystanie z social mediów

- Nie publikuj poufnych informacji (np. o wyjazdach)

Bezpieczne zakupy w Internecie



Podstawowe zabezpieczenia:

- Poznaj zaufane platformy
- Używaj bezpiecznych form płatności
- Sprawdzaj opinie sklepów
- Bądź ostrożny przed fałszywymi linkami



Co zrobić, żeby nie paść ofiarą oszusta internetowego?

1. Zweryfikuj stronę sklepu internetowego, w którym zamierzasz dokonać zakupu: Zobacz czy sklep ma jakieś opinie, dane teleadresowe, NIP, regulamin itd.
2. Nie podawaj nigdy numeru dowodu, numeru PESEL, numeru karty (w przypadku gdy nie ma 100% pewności, że strona jest bezpieczna).
3. Porównaj ceny produktu z innymi sklepami – zbyt niska cena może być podejrzana.
4. Nie wchodź w podejrzane linki z ofertami od nieznanomych, nie klikaj w reklamy, nie klikaj w podejrzane maile.
5. Pamiętaj o ciągłej edukacji i oprogramowaniu antywirusowym.

Co zrobić, gdy zostałeś oszukany?

1. W przypadku wadliwego sprzętu lub w niespełniającego oczekiwań, masz prawo do zwrotu w ciągu od 14 do 30 dni.
2. Możesz zgłosić sprawę na policję, skontaktuj się z rzecznikiem praw konsumenta.
3. Informuj rodzinę i znajomych, aby uniknęli oszustwa.

Weryfikacja zbiorok charytatywnych



Podstawowe kroki

- Zweryfikuj, czy link prowadzi do strony o której mówi
- Zwróć uwagę na komunikaty o zagrożeniu z przeglądarki
- Sprawdzaj, czy organizacja istnieje i czy jest zarejestrowana (należy wpisać nazwę w Google oraz wyszukać rok założenia)
- Zwróć uwagę na różnicę między bezpiecznymi stronami, na przykład: siepomaga.pl a zbiórką, którą chcemy wesprzeć
- Zweryfikuj osobę zbierającą (imię i nazwisko, czy nie zakłada często różnych zbiorok)
- Nie wpłacaj pieniędzy na konta osób prywatnych, nie przesyłaj BLIKIEM
- Zwróć szczególną uwagę na płatności (sprawdzanie pośrednika; ilość przekazywanych danych: pesel, adres, dane bankowe, karta kredytowa)
- Nie dawaj upoważnień osobom trzecim

Oszustwa tzw. na wnuczka

METODY OSZUSTWA



TELEFONICZNE



NA ŻYWO

Przeciwdziałanie:

- Ustaw limity w banku – duże przelewy wykonuj tylko osobiście w banku
- Nie trzymaj gotówki w domu
- Ustaw w telefonie szybkie wybieranie numeru do rodziny
- Utrzymuj częsty kontakt z rodziną
- Miej ważne numery telefonów na kartce w domu
- Przecwicz testowy telefon
- Zweryfikuj poprzez zapytanie o informację niedostępną powszechnie, na przykład datę ostatniej wizyty, imię zwierząt
- Zgłaszaj próby (KAŻDA) oszustwa na policję
- Blokuj numerów w telefonie
- Zweryfikuj dane osobowe, które mogą być udostępnione w internecie

PRZYKŁADOWE METODY

- na wnuczka
- na policjanta
- na kolegę

Przykładowy scenariusz oszustwa

1. Nieznajomy numer dzwoni
2. Odbierasz
3. Osoba podaje się za kolegę wnuczka, informuje o wypadku i potrzebuje pieniędzy. Osoba zna imię wnuczka (najprawdopodobniej znalazła je na podstawie danych z postu na Facebooku) i mówi, że potrzebuje gotówki

CO ZROBIĆ?

- Nie podawaj wrażliwych danych!
- Rozłącz się i zadzwoń na zaufany numer – do wnuczka, syna, córki, aby poinformować o sytuacji i zweryfikować czy jest prawdziwa
- Zachowaj spokój i zadawaj pytania, na które znajomy wnuczka zna odpowiedź – jak się nazywa pies, gdzie mieszka w ramach weryfikacji

JAK ZABEZPIECZYĆ SIĘ PRZED TAKĄ SYTUACJĄ?

Utrzymuj kontakt z bliskimi osobami, miej zawsze aktualny numer telefonu

- Jeśli oszust podaje się za np. przedstawiciela banku – miej aktualny numer do infolinii banku i zadzwoń, aby poinformować/zweryfikować prawdziwość przedstawionych informacji
- Bądź ostrożny_a przy odbieraniu telefonów od nieznanymi numerów – zawsze zakładać, że to może być oszustwo

Capgemini 

Jak pomóc seniorom?

Potencjalne pomysły

Przeciwdziałanie oszustwom matrymonialnym

FORMA KONTAKTU	SPOSÓB PRZEKAZU	SPOSÓB PRZEKAZU
Ulotki w takich miejscach jak przychodnia, poczta	Wierszyki, rymowanki	Przykładowe historie
Czat Bot, Aplikacja	Automatycznie nawiązuje kontakt	Rozmowa i ostrzeżenie, scenariusze na trudne sprawy

Pozostałe formy pomocy



Przykłady

- Wyznacz osoby, z którą osoba starsza może się kontaktować w razie niepewności/pytań
- Znajdź grupy seniorów zainteresowanych tematyką Internetu, np. kluby seniorów w celu wspólnych spotkań towarzyskich i nauki
- Przedstaw typowe scenariusze oszustw, np. metoda na wnuczka, policjanta oraz instrukcja jak się zachować
- Reguły bezpieczeństwa – wymyśl hasła, dwuetapowa autoryzacja
- Pokaż bezpieczne strony internetowe
- Daj informację, kogo można zapytać / z kim można się skonsultować
- Akcja promocyjna metodą analogową, np. ulotki z informacjami na co uważać i co zweryfikować
- Prelekcje dotyczące bezpieczeństwa w sieci
- Znajdź punkt, gdzie specjaliści zweryfikują zabezpieczenia sprzętu elektronicznego (w przypadku zakupów w Internecie)
- Cenzurowanie przez operatorów złych treści zastawiających internetowe pułapki
- Infolinia
- Wtyczki do przeglądarki albo aplikacja na telefon