DLACZEGO WARTO DBAĆ O BEZPIECZEŃSTWO W SIECI

Internet to wspaniałe narzędzie – pomaga utrzymywać kontakt z rodziną, załatwiać sprawy urzędowe, robić zakupy i poznawać świat. Niestety, tam, gdzie są ludzie, pojawiają się też oszuści. Dlatego warto znać kilka prostych zasad, które pomogą Ci korzystać z sieci bez stresu i ryzyka.

Pamiętaj: cyberbezpieczeństwo to nie technologia, to zdrowy rozsądek w nowoczesnym wydaniu.

BROSZURA POWSTAŁA W RAMACH PROJEKTU "CYFROWY SENIOR"

CYFROWY SENIOR

Instytut Nowych Technologii

Finansowane przez Unię Europejską

Projekt "Cyfrowy Senior" o numerze 2024-3-PL01-ESC30-SOL-000276137 finansowany ze środków budżetu Unii Europejskiej w ramach Europejskiego Korpusu Solidarności.

BEZPIECZNY SENIOR W SIECI

Podstawowe zasady cyberbezpieczeństwa dla osób 60+

www.newtechlodz.com

ZAKUPY I BANKOWOŚĆ ONLINE – JAK NIE DAĆ SIĘ OSZUKAĆ

Zakupy przez internet są wygodne, ale wymagają ostrożności.

• Kupuj tylko w znanych, sprawdzonych sklepach.
• Sprawdź, czy adres strony zaczyna się od https:// (to znak, że połączenie jest bezpieczne).
• Nie podawaj danych karty na podejrzanych stronach.
• W bankowości internetowej nigdy nie klikaj w linki z e-maili – zawsze wpisuj adres banku samodzielnie.

Jeśli coś wygląda zbyt dobrze, by było prawdziwe – to pewnie oszustwo.

BEZPIECZNY E-MAIL I SMS

Wiadomości e-mail i SMS to ulubione narzędzia oszustów. Często udają bank, urząd lub znaną firmę.

Jak rozpoznać fałszywą wiadomość:
• Nadawca ma dziwny adres e-mail (np. zamiast bank.pl – bank123.biz).
• W treści są błędy, pośpiech lub groźby („Twoje konto zostanie zablokowane!”).
• Link prowadzi do nieznanej strony.

Zasada: nigdy nie klikaj w linki ani nie otwieraj załączników z niepewnego źródła. Lepiej usuń taką wiadomość lub zapytaj kogoś zaufanego, zanim coś zrobisz.

SILNE HASŁA I LOGOWANIE

Twoje hasło to klucz do Twojego cyfrowego domu. Jeśli ktoś je pozna, może wejść tam bez Twojej zgody.

Jak tworzyć dobre hasła:
• Używaj minimum 8 znaków (litery, cyfry i symbole).
• Nie używaj imion ani dat urodzenia
• Dla ważnych kont używaj innych haseł • Zapisz je w notesie lub menedżerze haseł, ale nie na kartce przy komputerze.

Przykład: „MójPies!45Dom”.

Jeśli to możliwe, włącz tzw. dwustopniowe logowanie (2FA) – to dodatkowa ochrona, która wymaga potwierdzenia logowania np. kodem SMS.

10 ZŁOTYCH ZASAD CYBERBEZPIECZEŃSTWA

1. Nigdy nie podawaj swoich haseł innym.
2. Nie klikaj w podejrzane linki.
3. Sprawdzaj adresy stron i nadawców.
4. Używaj silnych i różnych haseł.
5. Aktualizuj komputer i telefon.
6. Nie daj się ponaglać – oszuści działają na emocjach.
7. Nie wysyłaj pieniędzy osobom poznanym w sieci.
8. W razie wątpliwości – zapytaj rodzinę lub znajomych.
9. Dbaj o prywatność – mniej znaczy bezpieczniej.
10. Ufaj, ale sprawdzaj.

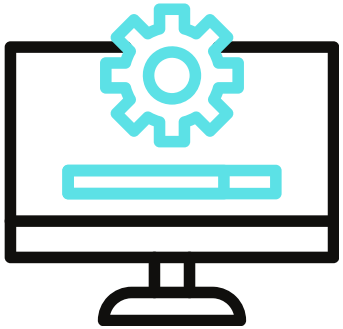
Pamiętaj: bezpieczeństwo w sieci to codzienny nawyk, który chroni Ciebie i Twoich bliskich.

TELEFON, KOMPUTER I AKTUALIZACJE

Bezpieczny sprzęt to podstawa. Nawet najlepsze hasło nie pomoże, jeśli komputer jest zainfekowany.

- Regularnie aktualizuj system i programy (to naprawia błędy, które mogą wykorzystać oszuści).
- Zainstaluj darmowy program antywirusowy.
- Zawsze blokuj ekran, gdy odchodzisz od urządzenia.
- Nie podłączaj przypadkowych pendrive'ów – mogą zawierać wirusy.

Drobne nawyki potrafią uchronić przed dużymi problemami.



MEDIA SPOŁECZNOŚCIOWE

Facebook, WhatsApp, Messenger – to świetne sposoby, by być w kontakcie. Ale pamiętaj, że nie każdy, kto pisze w internecie, jest tym, za kogo się podaje.

- Nie udostępniaj publicznie danych osobowych, adresu ani numeru telefonu.
- Uważaj na osoby, które szybko proszą o pieniądze lub zbyt osobiste informacje.
- Nie klikaj w linki wysyłane przez nieznajomych.

Zasada: jeśli coś wzbudza wątpliwość – nie reaguj od razu, zapytaj kogoś bliskiego.