Czego boją się Polacy w sieci?

Kategoria: Styl życia
Opublikowano: środa, 22, październik 2025 08:06
Tomasz Smaś
Odsłony: 853

Najnowsza, 6. edycja badania „Postawy Polaków wobec cyberbezpieczeństwa”, przygotowana przez Warszawski Instytut Bankowości we współpracy ze Związkiem Banków Polskich, ujawnia dwoistość w podejściu Polaków do cyfrowego świata. Blisko dwie trzecie mieszkańców kraju deklaruje, że czuje się bezpiecznie w sieci. Jednocześnie Polacy nie lekceważą zagrożeń, wskazując na phishing, kradzież tożsamości, fake newsy i dezinformację jako najczęściej obawiane niebezpieczeństwa.

Raport, zaprezentowany z udziałem przedstawiciela Ministerstwa Cyfryzacji, podkreśla, że cyberbezpieczeństwo to wspólna odpowiedzialność. Wicepremier i minister cyfryzacji wskazał, że choć państwo buduje systemy ochrony i inwestuje w edukację, żadne rozwiązanie technologiczne nie zastąpi zdrowego rozsądku i czujności każdego użytkownika internetu. Podkreślił, że realne zagrożenia, takie jak phishing czy dezinformacja, dotykają Polaków każdego dnia, co wymusza szybsze działania zarówno ze strony instytucji, jak i samych obywateli.

Wzrost zagrożeń i alarmujące braki w weryfikacji informacji

Pomimo deklarowanego rosnącego poczucia bezpieczeństwa, Polacy dostrzegają szereg zagrożeń w codziennym korzystaniu z e-usług, mediów społecznościowych i internetu.

Aż 88% badanych obawia się phishingu (wyłudzenia danych osobowych czy pieniędzy), 38% boi się kradzieży tożsamości, a co trzeci respondent (32%) obawia się fake newsów i dezinformacji.

Badanie ujawnia jednak, że Polacy nadal przywiązują zbyt małą wagę do krytycznej analizy i sprawdzania źródeł informacji. Tylko 38% badanych uważa, że wiadomości w mediach społecznościowych nie są ich głównym źródłem wiedzy. Zaledwie 32% czyta całą informację, a 31% weryfikuje ją w kilku źródłach. Jeszcze bardziej niepokojący jest fakt, że tylko co czwarty badany przyznaje, że nie udostępnia treści, których pochodzenia nie sprawdził. Aktywna postawa wobec dezinformacji jest słaba – zaledwie 17% deklaruje zgłaszanie fałszywych treści.

Nowe technologie: AI szansą, ale i zagrożeniem deep fake

W kontekście dynamicznego rozwoju narzędzi opartych na sztucznej inteligencji (AI), Polacy stają się coraz bardziej otwarci na tę technologię. Już 28% badanych widzi w AI szansę (dwukrotnie więcej niż w 2024 r.), choć połowa społeczeństwa nadal podchodzi do niej z dystansem. Dostrzegane są zarówno zalety, jak i realne zagrożenia, w tym ryzyko związane z technologią deep fake.

W odniesieniu do usług finansowych, świadomość współodpowiedzialności za bezpieczeństwo rośnie. Zaledwie 29% respondentów ma świadomość, że bezpieczeństwo e-usług finansowych to wspólna odpowiedzialność państwa, instytucji finansowych i klientów. Niemniej jednak, badani coraz częściej zauważają swój wpływ na cyberbezpieczeństwo, stawiając siebie w hierarchii odpowiedzialności za bezpieczeństwo usług finansowych już na trzecim miejscu (awans z piątego miejsca w poprzedniej edycji).

Prezes Związku Banków Polskich zaznaczył, że banki konsekwentnie edukują klientów w zakresie rozpoznawania prób phishingu, spoofingu czy vishingu, podkreślając, że wiedza i czujność są pierwszą linią obrony przed cyberprzestępcami.

Luka między deklaracją a praktyką: słabe punkty w nawykach

Mimo ogólnej znajomości zasad cyberbezpieczeństwa, w codziennych nawykach Polaków wciąż widoczne są luki:

- 63% deklaruje, że nie podaje nikomu swoich haseł, danych kart ani numeru PESEL.
- 62% nie otwiera załączników ani nie klika w linki od nieznanych nadawców.
- Mniej niż połowa dba o swoją prywatność w mediach społecznościowych (47%) czy stosuje dwuskładnikowe uwierzytelnianie (45%).

Najsłabiej wygląda sytuacja w przypadku korzystania z publicznych sieci wi-fi. Tylko 29% respondentów nie loguje się na strony wymagające podania loginu i hasła, korzystając z takich sieci np. na lotnisku czy w kawiarni.

Wiceprezes Warszawskiego Instytutu Bankowości podkreślił, że właściwe postawy i bezpieczne zachowania w cyberświecie są kluczowymi kompetencjami XXI wieku. Zaproponował rozważenie włączenia tych zagadnień do procesu edukacji formalnej od najmłodszych lat, wskazując na przykłady innych krajów, jak Finlandia, gdzie uczniowie od dawna uczą się rozpoznawać dezinformację.

Inwestycje i nowelizacja ustawy

W odpowiedzi na rosnącą skalę zagrożeń w sieci, Polska znacząco wzmacnia krajowy system cyberbezpieczeństwa. Tylko w 2025 roku na budowanie cyberodporności w sferze cywilnej zaplanowano rekordowe wydatki przekraczające 3,1 mld zł. Jest to największa w historii inwestycja w zwiększanie cyberodporności kraju.

Ponadto, wkrótce pod obrady Rady Ministrów ma trafić projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa. Ma on na celu wprowadzenie nowych obowiązków dla podmiotów z kilkunastu sektorów gospodarki, co zwiększy ochronę systemów informacyjnych i odporność na incydenty. Trwają również prace nad nową Strategią Cyberbezpieczeństwa RP, kluczowym dokumentem określającym strategiczne cele na najbliższe lata.

Działania państwa obejmują także programy edukacyjne i profilaktyczne. W tym roku szkolnym Ministerstwo Cyfryzacji, we współpracy z NASK i ABW, realizuje program wsparcia szkół, rodziców i uczniów w walce z cyberprzemocą pod hasłem „Włącz szacunek. Wyłącz hejt”, który obejmuje szkolenia, webinary i cyberlekcje promujące higienę cyfrową.

Pełna treść raportu znajduje się w załączeniu.

Źródło: MC