

PIT jako przynęta. Oszuści polują na tożsamość

Kategoria: Styl życia

Opublikowano: czwartek, 24, kwiecień 2025 13:29

Katarzyna Sekuła

Odśłony: 832

Trwający okres rozliczeń podatkowych staje się nie tylko czasem intensywnej pracy dla urzędów skarbowych, ale również gorącym sezonem dla cyberprzestępców. W obliczu rekordowej liczby elektronicznych deklaracji PIT składanych przez Polaków, skala zagrożeń związanych z wyłudzeniem danych osobowych dramatycznie rośnie. Najcenniejszym łupem oszustów staje się numer PESEL, a sposób działania – choć znany od lat – nie traci na skuteczności.

Ponad pięć milionów podatników skorzystało w tym roku z e-usług fiskusa. To wygodne i szybkie rozwiązanie. Niestety, również wygodne dla tych, którzy czyhają na dane osobowe obywateli. Fałszywe e-maile, SMS-y czy strony internetowe podszywające się pod oficjalne instytucje – to tylko niektóre narzędzia, po które sięgają cyberprzestępcy, licząc na nieuwagę użytkowników. Ofiarami phishingu, czyli oszustwa polegającego na wyłudzeniu danych, mogą paść nawet ci ostrożni – jeśli chociaż przez moment stracą czujność.

Wystarczy kliknięcie

Mechanizm oszustwa jest prosty i sprytnie powiązany z oczekiwaniem na zwrot nadpłaty z PIT. W skrzynkach mailowych i telefonach pojawiają się wiadomości wyglądające jak oficjalne komunikaty urzędów – zawierają informację o przysługującym zwrocie podatku i link, który rzekomo prowadzi do formularza potwierdzającego dane bankowe. Kliknięcie w link i wprowadzenie danych może mieć dramatyczne konsekwencje: utratę środków z konta lub kradzież tożsamości. Oszuści zyskują wtedy dostęp do pełnych danych osobowych, w tym numeru PESEL, i mogą wykorzystać je do zaciągnięcia zobowiązań finansowych na dane ofiary.

Do arsenału przestępców dochodzą także fałszywe strony internetowe łudząco przypominające portale Ministerstwa Finansów, Krajowej Administracji Skarbowej czy e-Urzędu Skarbowego. Tego typu witryny bywają nie do odróżnienia na pierwszy rzut oka, szczególnie w sytuacji pośpiechu lub braku technicznej wiedzy. Oszuści doskonale wiedzą, jak wykorzystać moment nieuwagi.

Skala problemu

Z badania przeprowadzonego przez serwis ChronPESEL.pl oraz Krajowy Rejestr Długów wynika, że aż 30% Polaków doświadczyło kradzieży lub próby wyłudzenia danych osobowych. 18% respondentów spotkało się z próbą oszustwa, 5% padło jego ofiarą, a kolejne 7% zadeklarowało, że doświadczyło obu tych sytuacji. Liczby te obrazują skalę zjawiska, które – choć nagłaśniane przez media i instytucje – wciąż znajduje nowe ofiary.

Najbardziej niepokojące pozostaje jednak to, że tylko 11% osób, które miały styczność z próbą wyłudzenia danych, zgłosiło ten fakt odpowiednim służbom, takim jak policja czy CERT Polska. Brak reakcji ofiar tylko rozzuchwala cyberprzestępców i zwiększa ryzyko kolejnych ataków.

Jak się bronić?

Ochrona danych osobowych zaczyna się od czujności. Urzędy skarbowe i instytucje rządowe nie proszą podatników drogą mailową ani SMS-ową o potwierdzanie rachunków bankowych czy weryfikację danych osobowych. Każda tego typu wiadomość powinna wzbudzić podejrzenia. Kluczowe jest również dokładne sprawdzanie adresu strony internetowej – nawet drobna literówka może zdradzić fałszerstwo.

PIT jako przynęta. Oszuści polują na tożsamość

Kategoria: Styl życia

Opublikowano: czwartek, 24, kwiecień 2025 13:29

Katarzyna Sekuła

Odsłony: 832

W razie jakichkolwiek wątpliwości warto zweryfikować informacje bezpośrednio u źródła – kontaktując się z urzędem skarbowym lub korzystając z oficjalnych infolinii. Nigdy nie należy podawać numeru PESEL, loginów, haseł czy danych bankowych na stronach, do których prowadzą linki z niezweryfikowanych wiadomości.

Zagrożenie jest realne, a konsekwencje wycieku danych – bardzo poważne. W dobie cyfrowych usług finansowych i administracyjnych numer PESEL to jeden z najcenniejszych zasobów, jaki można utracić. Tym bardziej warto pamiętać, że złudna wygoda kliknięcia w link może kosztować znacznie więcej, niż przyniesie zysk.

Źródło: IP