



NEWSLETTER "CZY WIESZ, ŻE..."

UWAGA NA FAŁSZYWY E-US!

Cyberprzestępcy rozpoczęli wysoce zorganizowaną kampanię phishingową wymierzoną w polskich podatników. Atak polega na podszywaniu się pod portal **podatki.gov.pl** w celu kradzieży danych osobowych oraz środków finansowych. Poniżej przedstawiamy szczegółową analizę wektora ataku.

1. Wiadomość początkowa (Wektor ataku)

Ofiara otrzymuje wiadomość e-mail informującą o rzekomej "nadpłacie podatku dochodowego". Wiadomość zawiera fałszywe logo i stylizację KAS.

Zwróć uwagę na **adres nadawcy**: **ooodptk@updates.i-pdtk.com** – to nie jest oficjalna domena administracji skarbowej!

Informacja o zleceniu przelewu z Urzędu Skarbowego

Elektroniczny System Podatkowy <ooodptk@updates.i-pdtk.com>
Do: Ty

PODATKI.GOV.PL PISMO URZĘDOW

Informacja o nadpłacie podatku dochodowego

Znak sprawy: LT 5/MB/2026/1725
Data wygenerowania: 20 sierpnia 2026 r.

Szanowny Podatniku,

Informujemy, że w wyniku automatycznej weryfikacji Państwa rocznego zeznania podatkowego za rok 2026, Krajowa Administracja Skarbowa odnotowała nadpłatę podatku dochodowego.

KWOTA ZWRÓTU
2 250,25 PLN
(słownie: dwa tysiące dwieście pięćdziesiąt złotych 25/100)

Potwierdzi dyspozycję zwrotu

Procedura zwrotu:

1. Przejdź pod bezpieczny link i uwierzysz się w systemie.
2. Zatwierdź transakcję zwrotu.
3. Oczekuj na zaksięgowanie środków (do 3 dni roboczych).

PODATKI.GOV.PL
Wspieranie techniczne: INFO@PODATKI.GOV.PL
Krajowa Informacja Skarbowa: 22 340 03 80

podatki.gov.pl

NAWIĄZANO BEZPIECZNE POŁĄCZENIE

Weryfikacja połączenia
To może potrwać chwilę. Proszę czekać, potwierdzamy Twoją sesję.

☐ Nie jestem robotem

To jest automatyczna kontrola bezpieczeństwa.
Privacy Terms

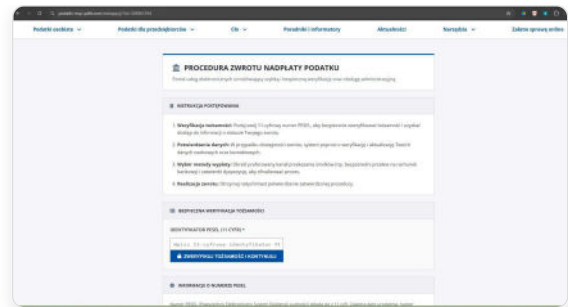
2. Przekierowanie i uwiarygodnienie

Po kliknięciu w link, ofiara trafia na stronę weryfikującą typu "CAPTCHA". Ma to na celu zbudowanie złudnego poczucia bezpieczeństwa oraz ominięcie automatycznych systemów skanujących filtry antyspamowe (tzw. cloaking).

3. Kradzież danych ewidencyjnych (PESEL)

Złośliwa strona (domena: **podatki-mq.i-pdtk.com**) wymusza podanie 11-cyfrowego numeru **PESEL** por pretekstem weryfikacji tożsamości. Jest to pierwszy etap kradzieży tożsamości, niezwykle groźny w kontekście zaciągania zobowiązań finansowych.

3



4. Zbieranie dodatkowych danych osobowych

W kolejnym kroku oszuści rozbudowują swój profil o ofierze, żądając podania imienia, nazwiska, adresu e-mail oraz numeru telefonu. Informacje te posłużą do dalszych ataków z użyciem inżynierii społecznej (np. vishing - spoofing telefoniczny).

4

5. Wyłudzenie danych karty płatniczej

Pod pretekstem "uznania na kartę" (zwrotu środków), ofiara proszona jest o podanie pełnych danych karty płatniczej (numer, data ważności, kod CVC/CVV). To pozwala przestępcom na natychmiastowe obciążenie rachunku z użyciem bramki płatniczej (tzw. carding).

5

Metoda uznania zwrotu

Wybierz preferowaną metodę otrzymania zwrotu.

Wybór metody

☒ **Przelew na rachunek bieżący**
Najczęstsze użycie na koncie bankowym. Średni czas to 1-3 dni robocze.

☐ **Uznanie na kartę (kredytową, debetową)**
Kwota zostanie zwrócona lub uznana bezpośrednio na wskazaną kartę.

Wybierz swój bank:

PKO Bank Polski Nowy PLN 2,000.00	Bank Pekao S.A. Nowy PLN 2,000.00	Santander Bank Polska Nowy PLN 2,000.00	mBank Nowy PLN 2,000.00	PKO Bank Śląski Nowy PLN 2,000.00
Bank Millennium Nowy PLN 2,000.00	Albo Bank Nowy PLN 2,000.00	BNP Paribas Bank Polska Nowy PLN 2,000.00	Credit Agricole Bank Polska Nowy PLN 2,000.00	Citi Handlowy Nowy PLN 2,000.00

Logowanie do banku

Odbiór wpłaty: 2 197,58 PLN

PKO Bank Polski Inteligo

Numer klienta albo przyjazny login

Dalej

6. Kradzież poświadczeń bankowych (np. PKO BP)

Jeżeli ofiara wybierze "Przelew na rachunek bieżący", zostaje poproszona o wybór swojego banku. Na zaprezentowanym ekranie logowania, podszywającym się pod **PKO Bank Polski**, przestępcy przejmują bezpośrednio login i hasło do bankowości elektronicznej, co daje im pełną kontrolę nad finansami poszkodowanego.

Rekomendacje z obszaru Bezpieczeństwa Informacji

Zawsze sprawdzaj adres URL witryny. Oficjalne usługi administracji rządowej znajdują się **wyłącznie w domenie .gov.pl**. Nigdy nie podawaj danych logowania do bankowości ani numerów kart płatniczych po kliknięciu w link z wiadomości e-mail. Wszelkie próby ataków należy bezzwłocznie zgłaszać do CERT Polska (incydent.cert.pl) zgodnie z właściwymi procedurami incydentów naruszeń w Twojej organizacji.

Infografika opracowana przez **MSVS i Cyber-JST**.

W trosce o cyfrowe bezpieczeństwo Twoje i Twojej organizacji.

Odwiedź nas na www.msvs.com.pl zadzwoń tel. 782-661-551 e-mail: lub napisz biuro@msvs.com.pl